VAJA: Poizvedovanje (ang. Reconnaissance)

Namen

Namen te naloge je učenje uporabe različnih tehnik in orodij za pridobivanje informacij o ciljnih sistemih. S pomočjo tehnik »reconnaissance« boste poizvedovali po DNS naslovu »recon.cybersec.ltfe.org«, da razkrijete ključne informacije o ciljnem omrežju. Te informacije vključujejo IP naslove, konfiguracijo omrežja, razpoložljive storitve in potencialne ranljivosti. Ta proces omogoča razumevanje, kako napadalci zbirajo predhodne informacije, ki so uporabne za uspešno izvedbo kibernetskih napadov ali za ustrezno obrambno strategijo.

Uvod

Poizvedovanje je prvi korak v procesu etičnega hekanja ali kibernetske obrambe. Ta korak vključuje pasivno in aktivno zbiranje informacij o cilju brez povzročanja škoda ali prekoračitve etičnih meja. Pasivno izvidništvo se osredotoča na zbiranje javno dostopnih informacij brez neposredne interakcije s ciljnim sistemom. To vključuje analizo spletnih mest, iskanje podatkov v javnih bazah ali uporabo storitev, kot je WHOIS, za pridobivanje informacij o domenah.

Aktivno izvidništvo vključuje neposredno interakcijo s ciljnim sistemom z uporabo različnih tehnik in orodij, kot so skeniranje vrat, analiza DNS zapisov in preizkušanje povezljivosti s sistemom.

Naloge:

S pomočjo tehnike »reconnaissance« poizveduj po DNS naslovu »recon.cybersec.ltfe.org«. Nalogo izvajajte v operacijskem sistemu Kali Linux.

1. Ker smo v nalogi napoteni preko DNS, si seveda ogledamo DNS zapis:

```
~# dig recon.cybersec.ltfe.org

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> recon.cybersec.ltfe.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45784
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;recon.cybersec.ltfe.org.       IN      A

;; ANSWER SECTION:
recon.cybersec.ltfe.org. 3600   IN      CNAME   net-212-101-137-92-
29.cybersec.ltfe.org.
net-212-101-137-92-29.cybersec.ltfe.org. 3600 IN A 212.101.137.92

;; Query time: 34 msec
;; SERVER: 193.189.160.13#53(193.189.160.13)
;; WHEN: Sun Mar 31 20:16:17 2024
;; MSG SIZE  rcvd: 93
```

1.1. DNS zapis »recon.cybersec.ltfe.org.« je alias, ki kaže na »net-212-101-137-92-29.cybersec.ltfe.org.«
1.2. »net-212-101-137-92-29.cybersec.ltfe.org.« ima A zapis »212.101.137.92«, kar pomeni da je končni IP naslov v katerega se razrešuje »recon.cybersec.ltfe.org« »212.101.137.92«.

2. Za nadaljevanje bi se lahko zapičili samo na IP naslov »212.101.137.92«, lahko pa sliko gledamo širše. Nam CNAME zapis, ki je zapisan na dolgo in široko sporoča kaj več?

net-212-101-137-92-29.cybersec.ltfe.org.

V njem vidimo zapisan IP naslov »212.101.137.92«, kaj bi lahko pomenil »net-» spredaj in »-29«? Morda je ta računalnik v omrežju z masko »/29«?

Če je tako, potem najprej ugotovimo za katero IP omrežje gre. Logična AND operacija med »212.101.137.92« in »255.255.255.248« nam pove, da je network ID »212.101.137.88/29«.

2.1. Poiščimo vse žive hoste v tem omrežju:

```
~# nmap -sP 212.101.137.88/29

Starting Nmap 6.00 ( http://nmap.org ) at 2024-03-31 20:25 CEST
Nmap scan report for 212.101.137.90
Host is up (0.0066s latency).
Nmap scan report for 212.101.137.91
Host is up (0.0041s latency).
Nmap scan report for 212.101.137.92
Host is up (0.0050s latency).
Nmap scan report for 212.101.137.94
Host is up (0.0072s latency).
Nmap done: 8 IP addresses (4 hosts up) scanned in 1.81 seconds
```

3. Še vedno ne vemo ali je ta ping scan zanesljiv (obstaja verjetnost, da kakšen računalnik na odgovarja na ping). Odločimo se za SYN stealth portscan v tem omrežju:

```
nmap -sS 212.101.137.88/29
```

3.1. Če iščemo bolj natančne informacije, torej tudi verzije strežniških programov (servisov / daemonov) uporabimo portscan z –A opcijo:

```
nmap -A 212.101.137.88/29
```

Če bomo pridobili podatke o različicah strežnikih programov, lahko potem na podlagi njih ugotovimo ali gre za posodobljeno različico strežniškega programa, ali pa ima le-ta že znane ranljivosti.

4. Nadaljevanje reconnaissance-a bi lahko bilo skeniranje subneta oz. na subnetu odkritih daemonov z OpenVAS-om, vendar to ni predmet te demonstracije in tega tečaja.
4.1. Če najdemo kje teči FTP strežnik se lahko nanj povežemo in zahtevamo anonimni FTP. Morda pa na njem najdemo kaj zanimivega?

```
# ftp 212.101.137.92
Connected to 212.101.137.92.
220 Welcome to CyberOps-LTFE FTP service.
```

```
Name (212.101.137.92:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> @
?Invalid command
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              16 Mar 28 18:16 txt.txt
226 Directory send OK.
ftp> get txt.txt
local: txt.txt remote: txt.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for txt.txt (16 bytes).
226 Transfer complete.
16 bytes received in 0.00 secs (58.1 kB/s)
ftp> bye
221 Goodbye.
~# cat txt.txt
Tukaj ni nic!!!
~#
```

V zgornjem primeru smo se povezali na FTP strežnik na “212.101.137.92”, tam našli datoteko “txt.txt”, si jo prenesli na svoj računalnik in si ogledali njeno vsebino.

Ostale opcije glede poizvedovanja po domeni

Napadalec bi seveda lahko pogledal Whois podatke o domeni “ltfe.org”, potem pa začel iskati Whois podatke o IP naslovu, ki pripada organizaciji, kjer gostuje domena “ltfe.org”.

Napadalec bi se lahko tudi fokusiral na poddomeno “cybersec.ltfe.org”, v kolikor le-ta gostuje na drugih DNS strežnikih, kakor domena “ltfe.org”. To ugotovimo z ukazom:

```
dig ns cybersec.ltfe.org
```

Če nam ukaz ne vrne NS zapisov, so DNS strežniki enaki kakor za domeno “ltfe.org”.

Drug način kako to ugotovimo je:

```
dig +trace cybersec.ltfe.org
```

Vprašanja

1. Kaj ugotovimo o dani domeni?
2. Katere naprave smo odkrili v omrežju?
3. Kakšne storitve smo odkrili na napravah?
4. Zapišite ukaze, ki ste jih uporabili in namen ukazov.
5. Opišite ranljivosti sistemov.
6. Opišite predloge za izboljšanje varnosti sistemov.