VAJA: L2 napadi

Namen

Namen te naloge je podrobno raziskati in praktično izvesti različne L2 napade, s posebnim poudarkom na ARP in DHCP protokolih

Uvod

V omrežnem okolju, kjer je varnost pogosto spregledana ali nezadostno izvajana, L2 napadi predstavljajo resno grožnjo integriteti in zaupnosti podatkov. Protokoli kot so ARP in DHCP, ki ne vključujejo avtentikacije sporočil, so še posebej ranljivi, kar omogoča napadalcem, da izkoristijo te pomanjkljivosti za izvajanje napadov kot so ARP cache poisoning in rogue DHCP server setup.

Naloge:

1. Napadi na ARP tabelo
   Protokol ARP je zelo enostavno zlorabiti ker ne avtenticira poslanih ARP Request sporočil. V kratkem vse napade na ARP tabelo označim z izrazom »ARP Cache Poisoning«. V preteklosti so bili napadi na ARP tabele zelo uničujoči saj so omogočali prisluškovanje nešifriranemu http prometu. Danes te napadi niso več tako zelo uničujoči saj uporabljamo https, vendar so še vedno zelo pogosti saj so zelo enostavni za izvedbo.

   1.1 Ponarejevanje ARP zapisov
   Ponarejevanje zapisov temelji na posredovanju nezaželenih (angl. Gratuitous) ARP odgovorov, kjer tarči posredujemo ponarejene IP -> MAC zapise. Samo ponarejevanje ni tko efektivno saj bo tarča hitro odkrila, da ne komunicira z namenjeno napravo.

   Ker želimo neovirano zajemanje paketov, moramo vklopiti posredovanje ip paketov. Postavimo se v vlogo super uporabnika `Kali@kali: sudo su`. In nato izvedemo ukaz

```
 echo 1> /proc/sys/net/ipv4/ip_forward
```

   Zaženemo program Wireshark, da lahko opazujemo promet in nato sosedu pošljemo svoj MAC ter IP naslov.

```
arpspoof -i <oznaka vmesnika> -r -t [ip_tarče] [naš_ip]
```

   1.2 Man in the Middle napad
   Man in the middle je bolj sofisticiran napad kot klasično ponarejevanje ARP zapisov saj je ponarejevanje ARP tabele dvosmerno. V praksi se tako kot ime že pove, postavimo med našo tarčo in poljubno napravo. Uporabili bomo enak ukaz kot v prejšnjem primeru, vendar bomo tokrat namesto našega IP naslova, uporabili IP naslov privzetega prehoda.

```
arpspoof -i <oznaka vmesnika> -r -t [ip_tarče] [ip_privzeti_prehod]
```

   IP naslov privzetega prehoda lahko izvemo s pomočjo ukaza `arp -a` oziroma `netstat – r`.

2. DHCP Napadi

Enako kot protokol ARP, DHCP ne uporablja avtentikacije vira, zato se je zelo preprosto predstavljati kot »rogue« DHCP strežnik in pošiljati napačne informacije. Alternativno lahko izsušimo bazen uporabnih IP naslovov in tako legitimnim strankam onemogočimo dostop do interneta.

2.1 DHCP Starvation

Posodobimo Kali Linux z ukazom `apt-get update` in nato namestimo eno izmed orodji za izvajanje napadov na nivoju DHCP-ja.

- Yersinia
- DHCPig

Namestimo orodje DHCPig z ukazom `apt-get install dhcpig`. Vse možnosti, ki jih omogoča DHCPig si lahko ogledamo z ukazom dhcpig -h. Za izvedbo napada je dovolj, da uporabimo ukaz `dhcpig <vmesnik>`. Za bolj detajlni odziv lahko ukazu dodamo dodatne zastavice `dhcpig -c -v3 -l -a -i -o <vmesnik>`.

2.2 Rogue DHCP Server

Za postavitev rogue dhcp strežnikov imamo več opcij, najlažje je uporabiti orodje Metasploit. Orodje metasploit zaženemo tako, da v konzolo napišemo ukaz `msfconsole`. Ko se orodje zažene moramo poiskati ustrezni modul, ki omogoča postavitev rogue dhcp strežnik. Vse module lahko preverimo z ukazom `show auxiliary`**.** Željen modul aktiviramo z ukazom `use <cela_pot>` in nato lahko preverimo katere parametre moramo obvezno nastaviti z ukazom `show options`. Kljub temu da sta samo 2 parametra označena kot obvezna, moramo nastaviti naslednje parametre.

- StartIP
- EndIP
- Netmask
- Router
- Srvhost

Glede na parametre izvedemo različne napade. Če dodeljujemo prave nastavitve vendar sami sebe označimo kot usmerjevalnik, izvedemo MITM napad. Če posredujemo čisto napačne informacije smo izvedli DOS napad.

Parametre nastavimo z ukazom `set option <parameter>` in zaženemo z `run`.

3. IPv6 Napadi
   Najbolj popularno orodje za izvršitev napadov na protokolu IPv6 je IPv6Toolkit, ki je zbirka odprtokodnih orodji za testiranje IPv6 omrežji. Orodje namestimo z ukazom `apt install ipv6toolkit`.

   - Primer pošiljanja NS sporočil: `ns6 -i eth0 -s 2001:db8::/32 -t 2001:db8::1 -F 10 -l -z 10 -e -v`

   Drugo zelo uporabno in veliko bolj enostavno orodje za uporabo se imenuje thc-ipv6 in je že inštaliran na Kali sistemih.

   - Primer DAD DOS napada: atk6-dos-new-ip6 -S <vmesnik>
   - Primer NMAP napada: atk6-alive6 <vmesnik>
   - Primer Router Info: atk6-dump_router6 <vmesnik>
   - Primer DHCP info: atk6-dump_dhcp6 <vmesnik>
   - Primer DHCP Spoof: atk6-fake_router26 <vmesnik>
   - Primer DHCP kill: atk6-kill_router6 <vmesnik>