Penetration Testing Report

By: TerminalTinker

Report Issued: May 3, 2024

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to Carl Acme - Acme Widgets Co. Nor facilitate attacks against Carl Acme - Acme Widgets Co. HurstSec Cyber LLC shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on Carl Acme - Acme Widgets Co.'s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

1.1 Executive Summary

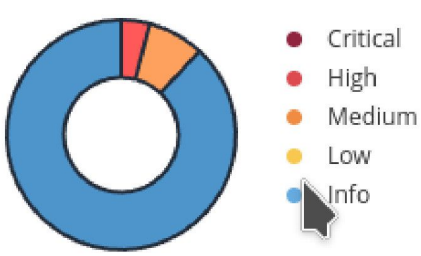
HurstSec Cyber LLC was granted permission to perform a security assessment of the internal corporate network of Acme Widgets Co. from 4/22/2024 to 5/03/2024 midnight. HurstSec Cyber LLC ’s penetration test acts just as close to an attack from an external threat actor attempting to gain access to systems within the Acme Widgets Co. corporate network. The purpose of this report is to find and identify vulnerabilities in Acme Widgets Co.’s infrastructure and recommend remediation strategies to those vulnerabilities. HurstSec Cyber LLC identified a total of 12 critical vulnerabilities and 8 high severity vulnerabilities within the scope of the engagement which are broken down by severity in the table below. This report will focus on analyzing the critical and high severity vulnerabilities within the provided scope.

1.2 Graphical Summary

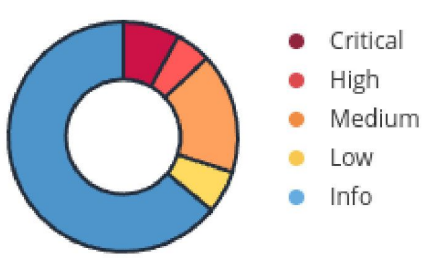
CRITICAL	HIGH	MEDIUM	LOW
12	**8**	**As needed**	**As needed**

- As needed = if company requests for vulnerability.

Machine1_ip



Machine2_ip



The critical and highest severity vulnerabilities give potential attackers the opportunity to get access or command line access to harm Acme Widgets Co. 's infrastructure. In order to ensure data confidentiality, integrity, and availability, security remediations stated in this report should be implemented as described.

*** Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

2.0 SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Networks

Network	Note
Machine2_ip	Metasploitable2
Machine1_ip	VulnHub Box

3.0 High Level Assessment Overview

In this penetration test, I was assigned the task to stimulate real-world threat actors that would take actions against the specified ip addresses within my scope: Machine1_ip and Machine2_ip . My overall goal was to evaluate both of the host ip addresses, identify any vulnerable services, and exploit those vulnerabilities for Acme Widgets Co.

3.1 Short Term Recommendations

HurstSec Cyber LLC recommends Acme Widgets Co. to take the following actions as soon as possible to minimize business risk.

Short Term Remediations:

- Reset Passwords/use passwords that don't come default.
- Upgrade software and services labeled as Vulnerabilitiable in this report.
- Place appropriate restrictions to make sure services are only accessible to authorized users.

3.2 Long Term Recommendations

HurstSec Cyber LLC recommends the following actions be taken over the next 12 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

Long Term Remediations:

- If updates/upgrades can’t be run, then invest in software and machines that would support the latest security patches.

4.0 Vulnerability scanning and analysis

4.1 Information Gathering

During the information gathering phase, I gathered information about specified ip addresses within my scope: Machine1_ip and Machine2_ip in Acme Widgets Co. 's network systems. I scanned for open ports and other enumeration methods against the targets to discover open ports and services. Then, I ran a basic network scan on the specified ip addresses within my scope: Machine1_ip and Machine2_ip using Nessus and NMAP vuln script to see what are known vulnerabilities.

4.2 Penetration Testing

After using NMAP and Nessus to gain more information about the targets, I used the knowledge gained to launch attacks that exploited the vulnerabilities in the Acme Widgets Co. network. I took into consideration my restrictions and scope along with making sure that my actions do not impact the day to day operations of the Client's business (Acme Widgets) at all times.

The following are graphical representations of scans looking for open ports using NMAP:

```
$ nmap -sC -sV -Pn Machine2_ip

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 3.0.20-Debian (workgroup:
WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

$ nmap -p- -sV Machine2_ip

```
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  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
```

```
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5

3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu
4.2.4-1ubuntu4))

5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp  open  vnc         VNC (protocol 3.3)

6000/tcp  open  X11         (access denied)

6667/tcp  open  irc         UnrealIRCd

6697/tcp  open  irc         UnrealIRCd

8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)

8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1

8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path
/usr/lib/ruby/1.8/drb)

39034/tcp open  nlockmgr    1-4 (RPC #100021)

39500/tcp open  status      1 (RPC #100024)

50152/tcp open  java-rmi    GNU Classpath grmiregistry

58882/tcp open  mountd      1-3 (RPC #100005)
```

5.0 CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

6.0 Identified vulnerabilities

IP Address: Machine1_ip

Number	Finding	CVSS v2.0 Base Score	Risk	Page
1	ProFTPD Compromised Source Packages Trojaned Distribution	**10.0**	**High**	14
1.1	Apache Service Privilege Escalation	**N/a**	**N/a**	18
2	ICMP Timestamp Request Remote Date Disclosure	**2.1**	**Medium**	27

IP Address: Machine2_ip

Number	Finding	CVSS v2.0 Base Score	Risk	Page
3	UnrealIRCd Backdoor Detection	**10.0**	**Critical**	28
4	VNC Server 'password' Password	**10.0**	**Critical**	29
5	NFS Exported Share Information Disclosure	**10.0**	**Critical**	32
6	SSL Version 2 and 3 Protocol Detection	**10.0**	**Critical**	33
7	Bind Shell Backdoor Detection	**10.0**	**Critical**	35
8	Unix Operating System Unsupported Version Detection	**10.0**	**Critical**	36
9	Apache Tomcat SEoL (<= 5.5.x)	**10.0**	**Critical**	37

10	Apache Tomcat AJP Connector Request Injection (Ghostcat)	**9.8**	**Critical**	38
11	NFS Shares World Readable	**8.8**	**High**	39
12	rlogin Service Detection	**7.5**	**High**	40
13	rsh Service Detection	**7.5**	**High**	41
14	Samba Badlock Vulnerability	**7.5**	**High**	42
15	SSL Medium Strength Cipher Suites Supported (SWEET32)	**7.5**	**High**	43
16	ISC BIND Service Downgrade / Reflected DoS	**5.0**	**High**	44

1 - ProFTPD Compromised Source Packages Trojaned Distribution

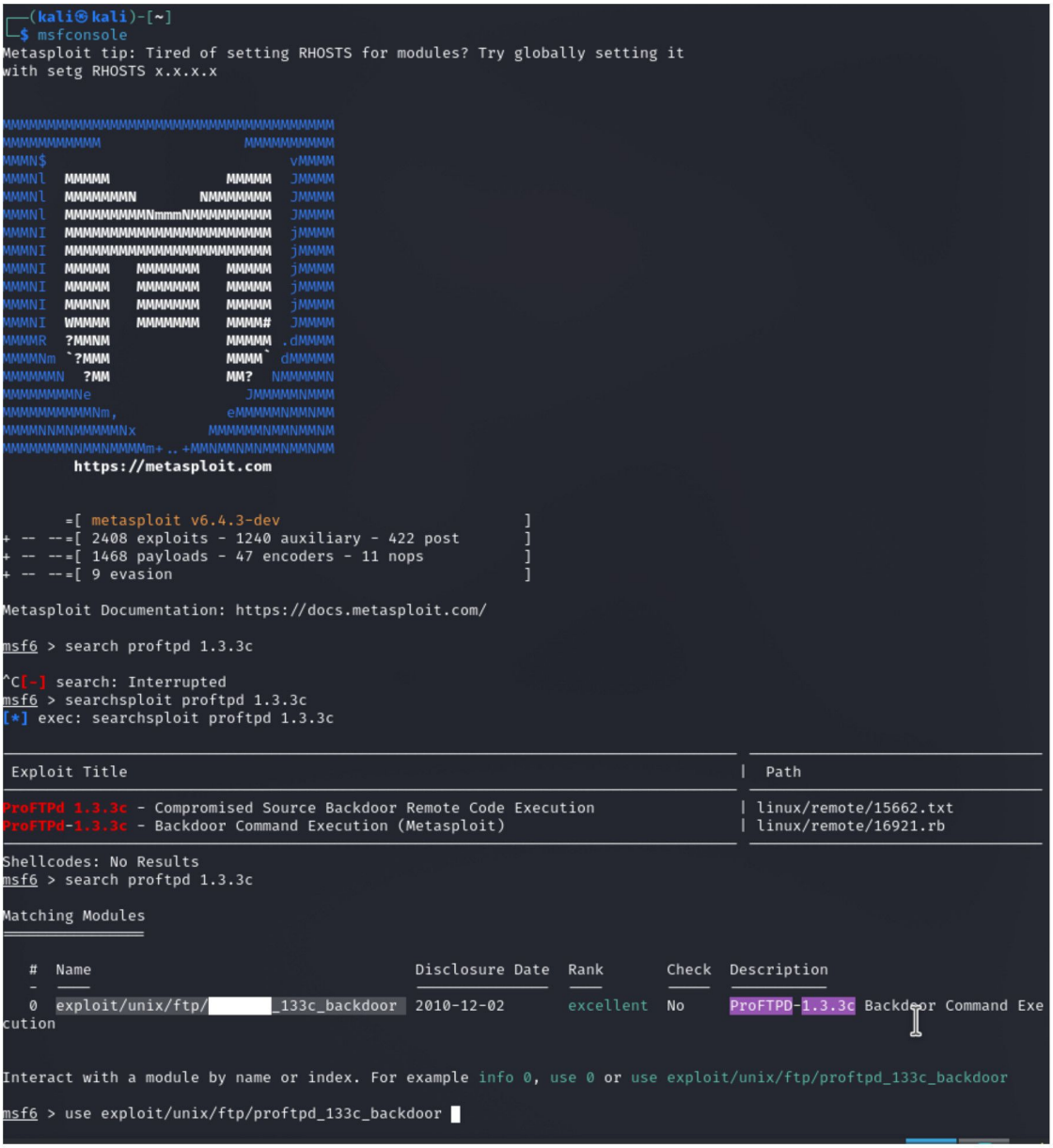
HIGH Severity (10.0/10)	
IP Address Impacted	Machine1_ip

Security Implications

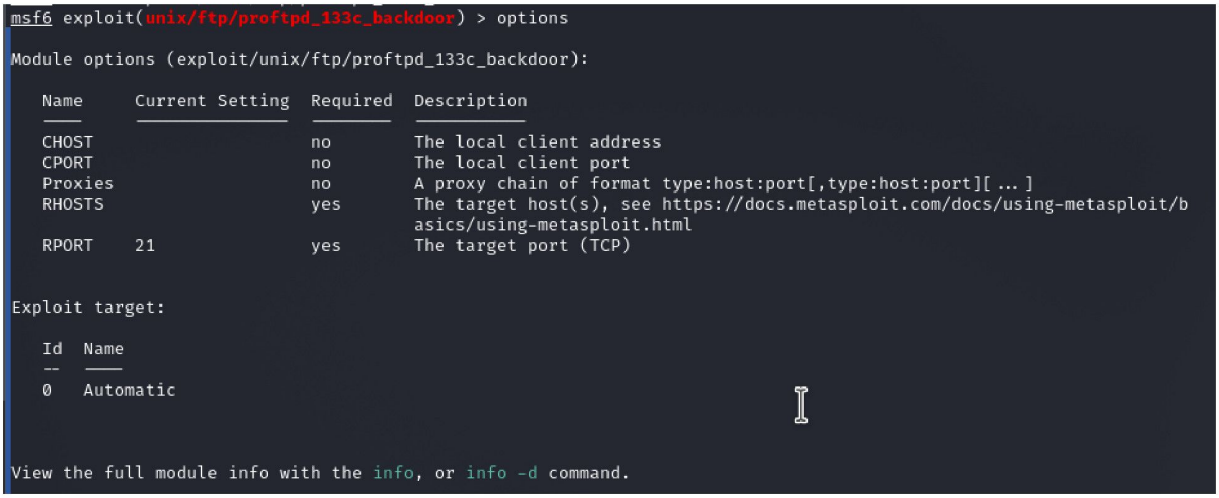
The ProFTPD software, which is an FTP server used on Unix and Linux systems, had a security issue. Specifically, the version of ProFTPD installed on the remote host was compiled with a backdoor in a file called 'src/help.c'. This backdoor was related to a compromise of the main distribution server for the ProFTPD project. By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute unjustifiable commands with system privileges.

Analysis

This part goes through a possible method that a real-world threat actor can use to exploit this version of ProFTPD 1.3.3c. I started by searching for exploits related to “proftpd 1.3.3c”:



exploit/unix/ftp/proftpd_133c_backdoor suggests that there is a known backdoor exploit for ProFTPD version 1.3.3c to gain unauthorized access.



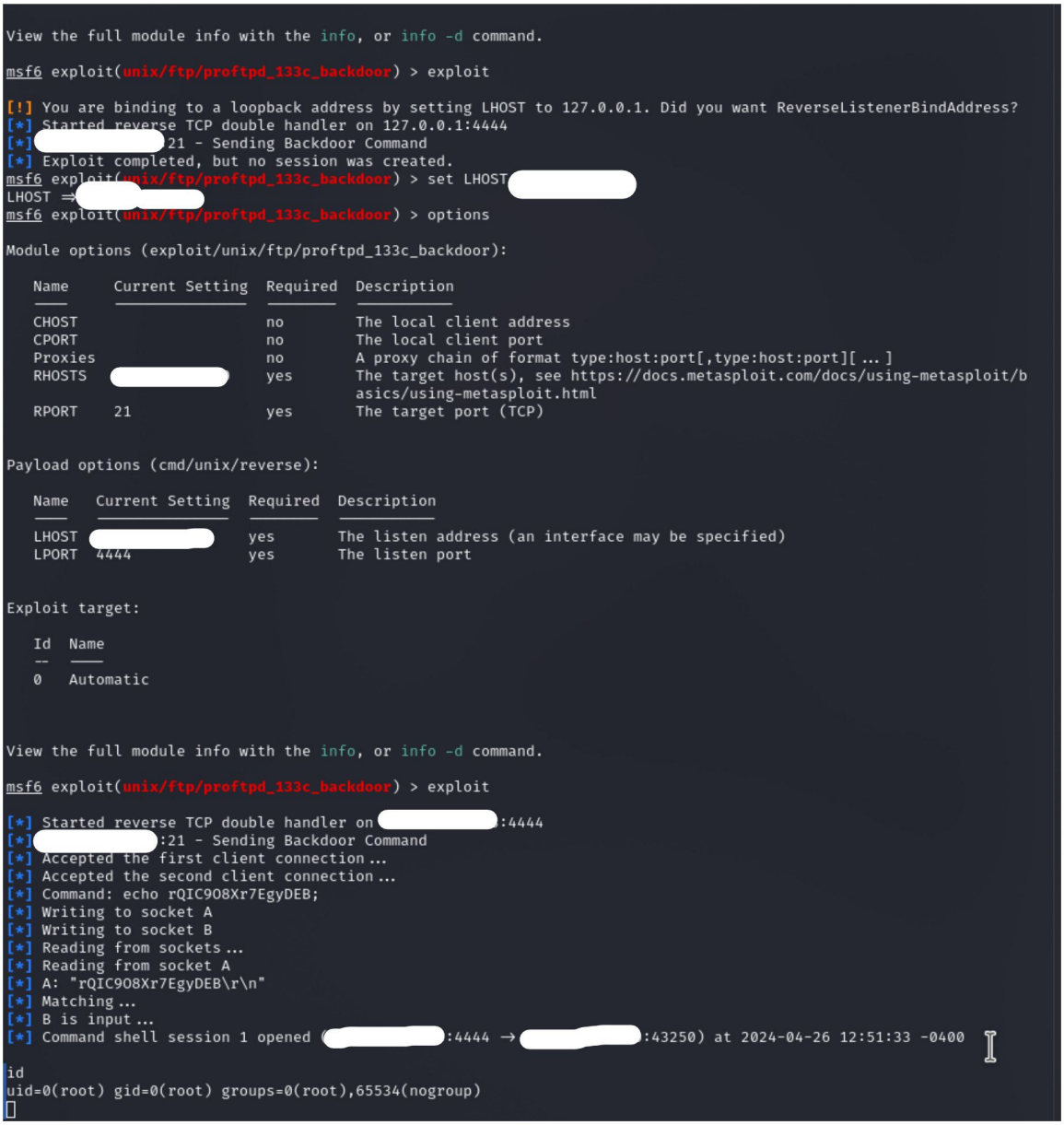
Need to set payload to cmd/unix/reverse to setting up a reverse shell. A reverse shell allows an attacker to gain access to a vulnerable system by establishing a connection from the target system back to the attacker's machine. The following commands ran the **unix/ftp/proftpd_133c_backdoor** exploit to gain access to the shell:

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[-]              :21 - Exploit failed: A payload has not been
selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD
cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

The screenshot includes specific module options and payload settings, such as LHOST and LPORT, which are used to define the IP address and port for the reverse connection. The

commands shown in the screenshot are an attempt to exploit a system by executing a payload that would open a command shell session, indicating successful exploitation.



Once the unix/ftp/proftpd_133c_backdoor exploit is executed, I was able to type “whoami” to confirm that I have root access to the host.

Recommendations

- Reinstall the host from known, good sources.

References (opt)

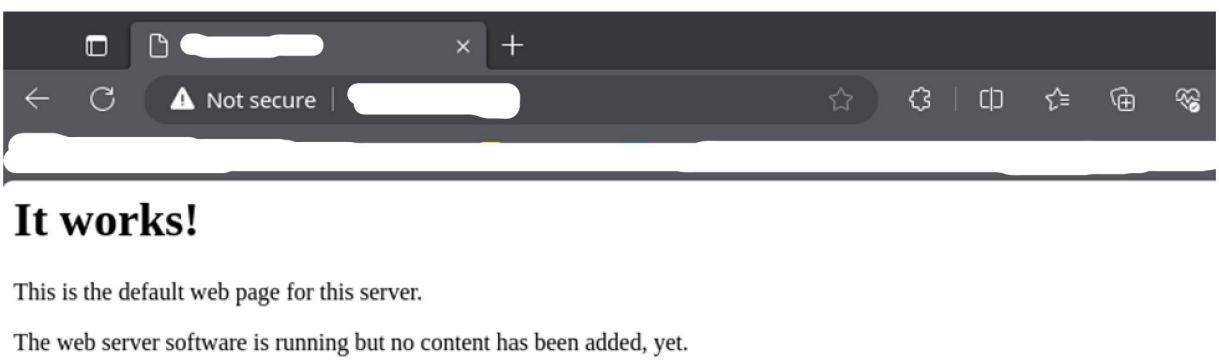
- https://www.theregister.co.uk/2010/12/02/proftpd_backdoored/
- https://xorl.wordpress.com/2010/12/02/news-proftpd-owned-and-backdoored/

- http://www.nessus.org/u?74de525d

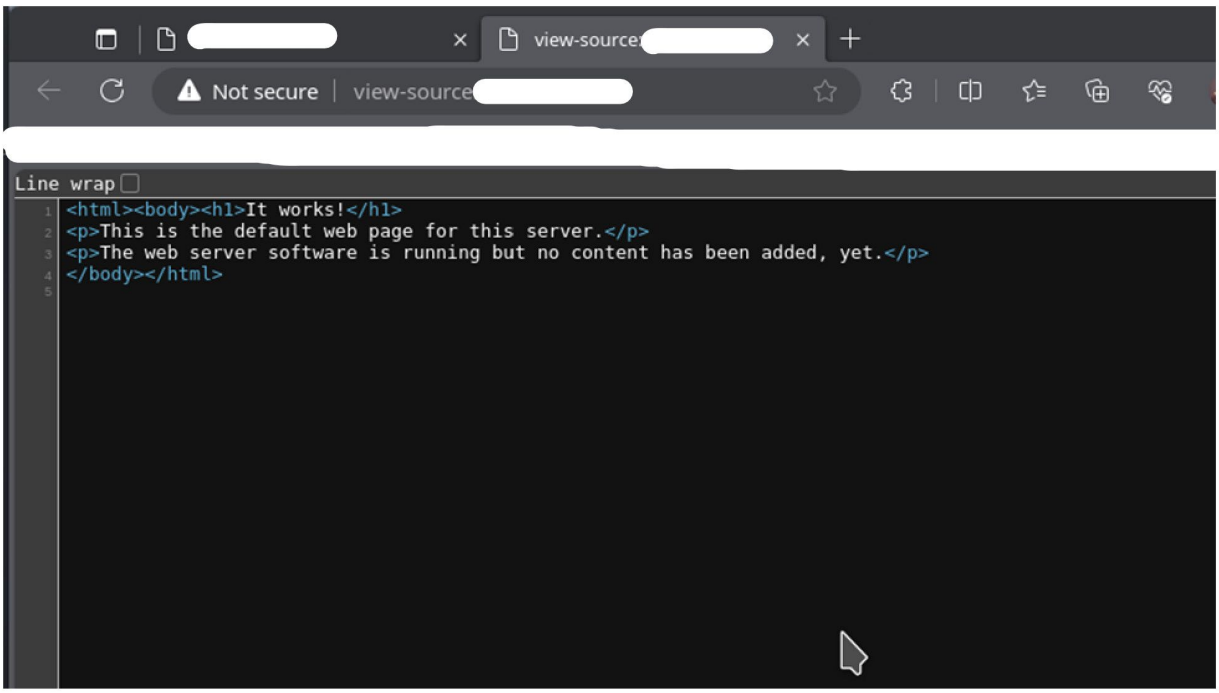
1.1 - Apache Service Privilege Escalation

IP Address Impacted	Machine1_ip

This part goes through a possible method that a real-world threat actor can use privilege escalation to gain admin access to vtc secret wordpress. The screenshot below is of a web browser displaying a default webpage, typically seen when a new server is set up and no content has been added yet.



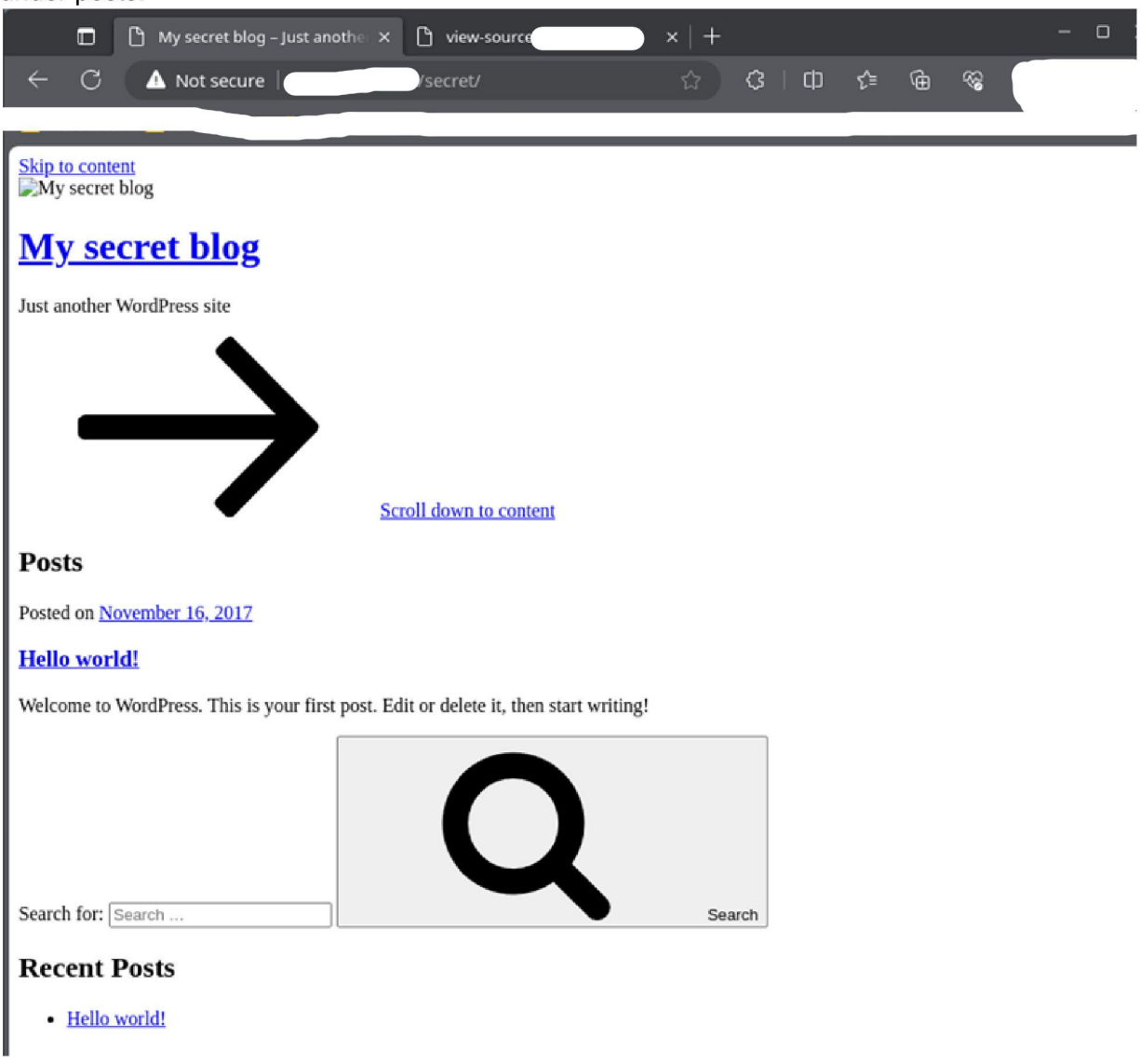
When viewing the page source, I noticed that there is no robots.txt file available to indicate any potential folders or sitemap.



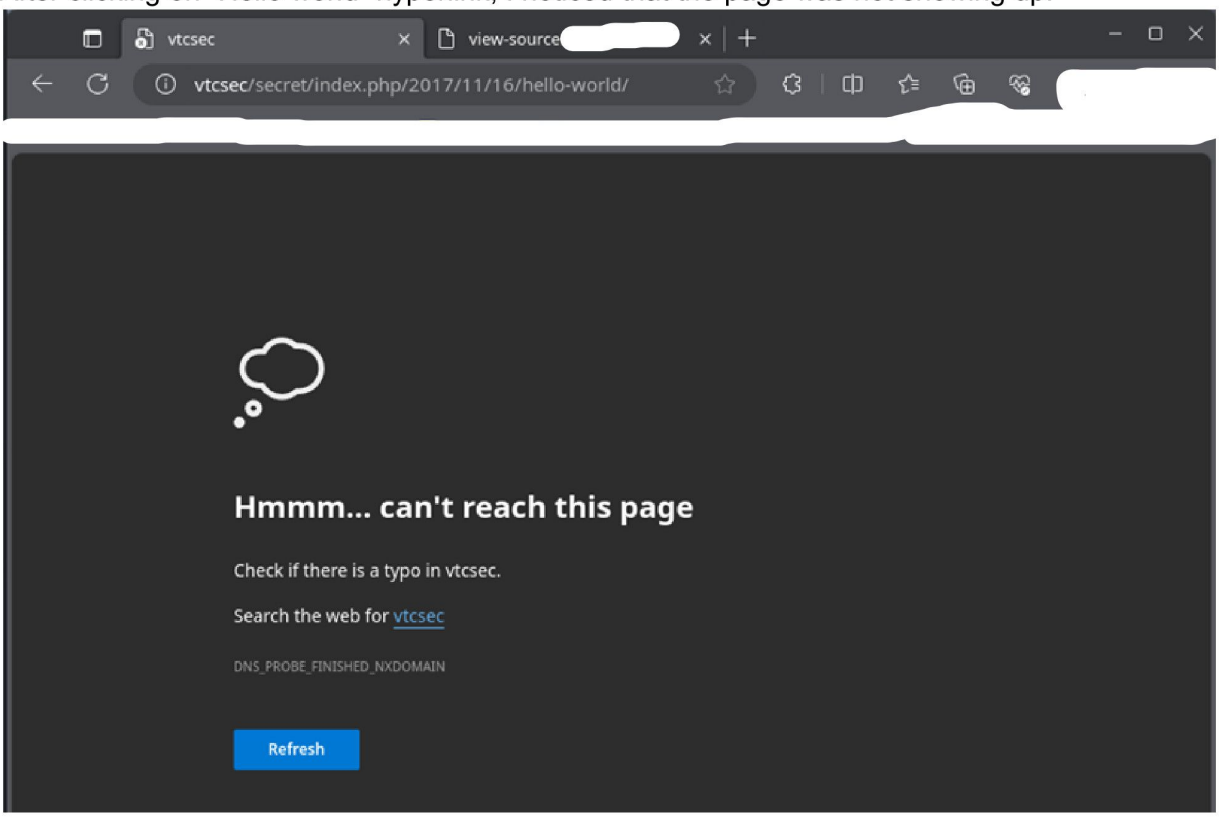
I then ran a dirb scan, a useful tool for scanning HTTP-based webservers to search for directories and files. It revealed an interesting URL http:// /secret.

```
dirb http://Machine1_ip /usr/share/wordlists/dirb/common.txt
-o dirb.txt
---- Scanning URL: http://  Machine1_ip  / ----
+ http://  Machine1_ip  /index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://  Machine1_ip  /secret/
```

I put the interesting URL http:// Machine1_ip secret into my browser and clicked “Hello world!” under posts.



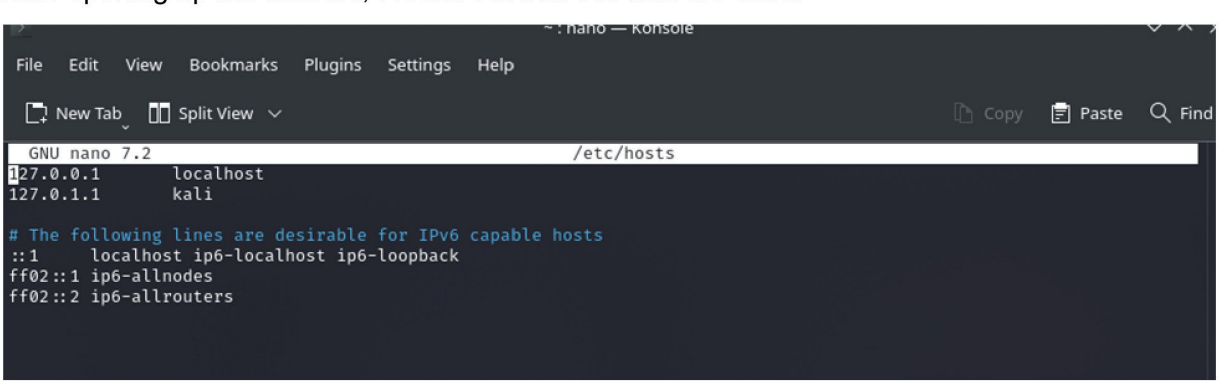
After clicking on “Hello world” hyperlink, I noticed that the page was not showing up.



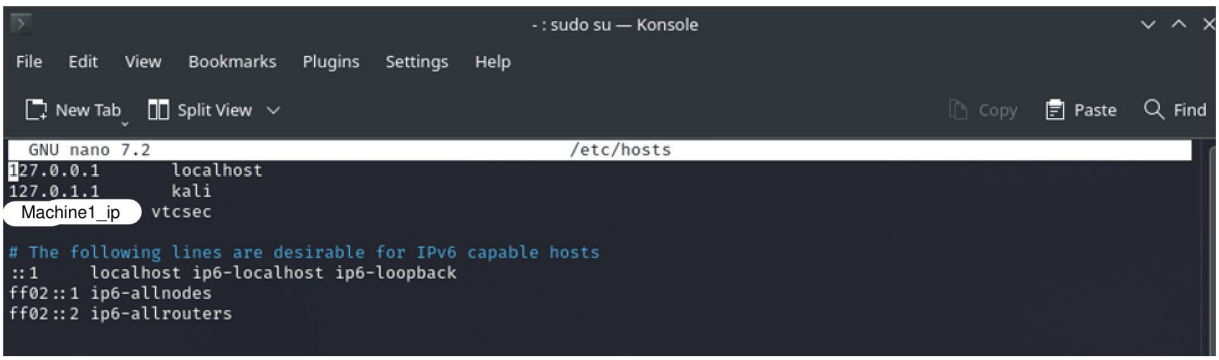
I determined that this link was referring to a domain named "vtcsec" instead of an IP address. I corrected this by manually adding my computer’s ip address to the host file.

`nano /etc/hosts`

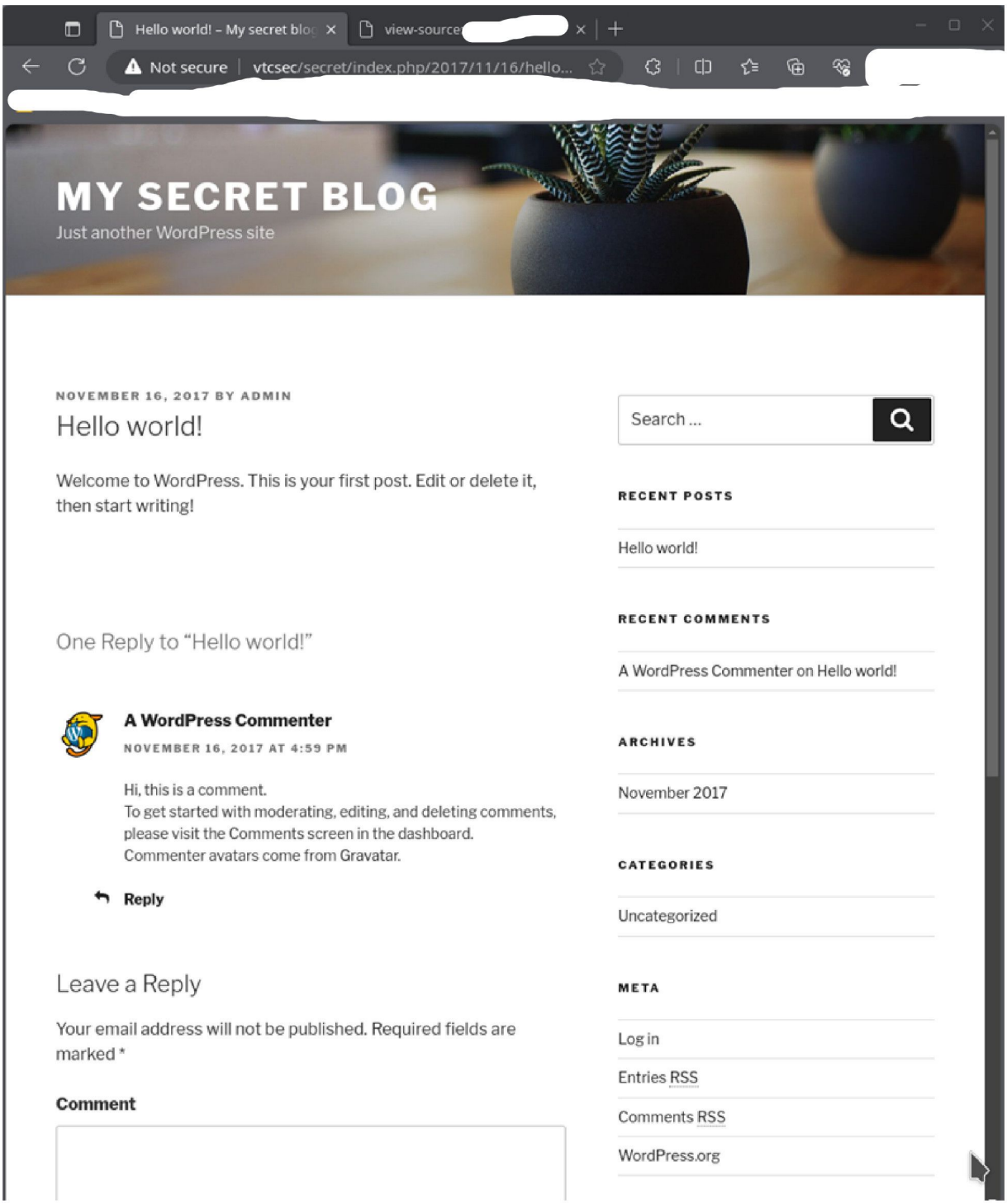
After opening up the host file, I found out that this was the case.



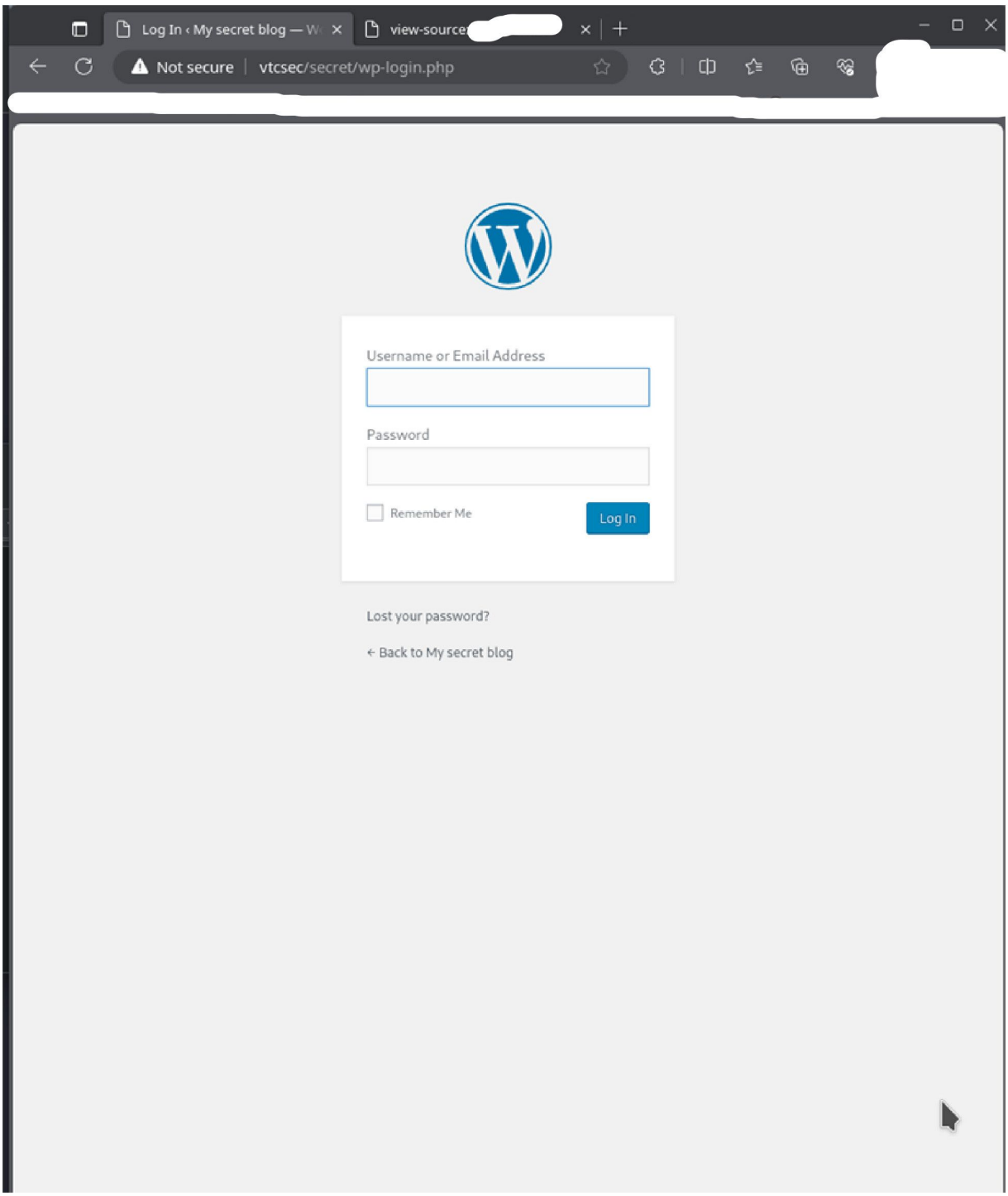
I added in my computer’s ip address to the host file..



After saving this file, I refreshed the webpage and saw a page titled “MY SECRET BLOG”.



I proceeded to link to the log in panel that can then be found on the right-hand side under the meta sublist.



I ran a scan to search for valid users and vulnerabilities on the site and found a user identified as admin.

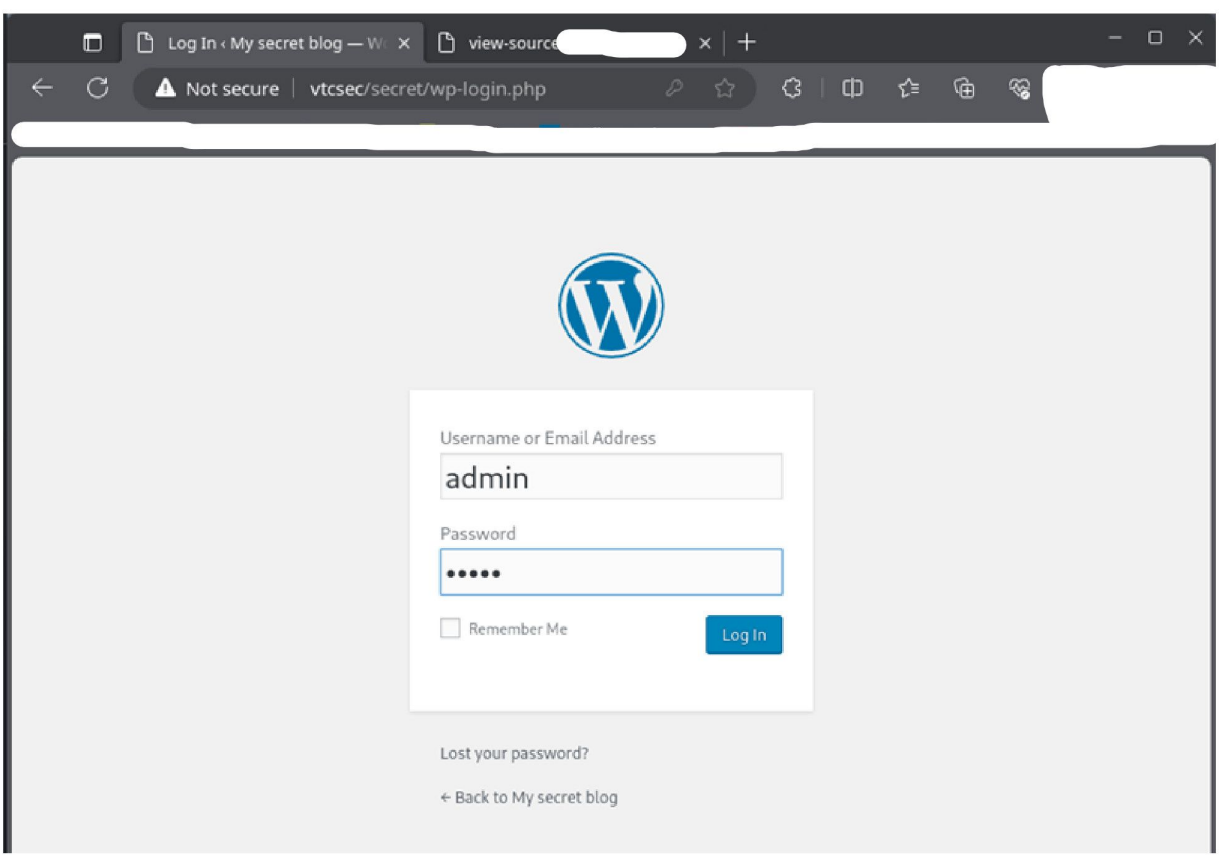
```
wpscan --url http:// Machine1_ip          /secret/ --enumerate
```

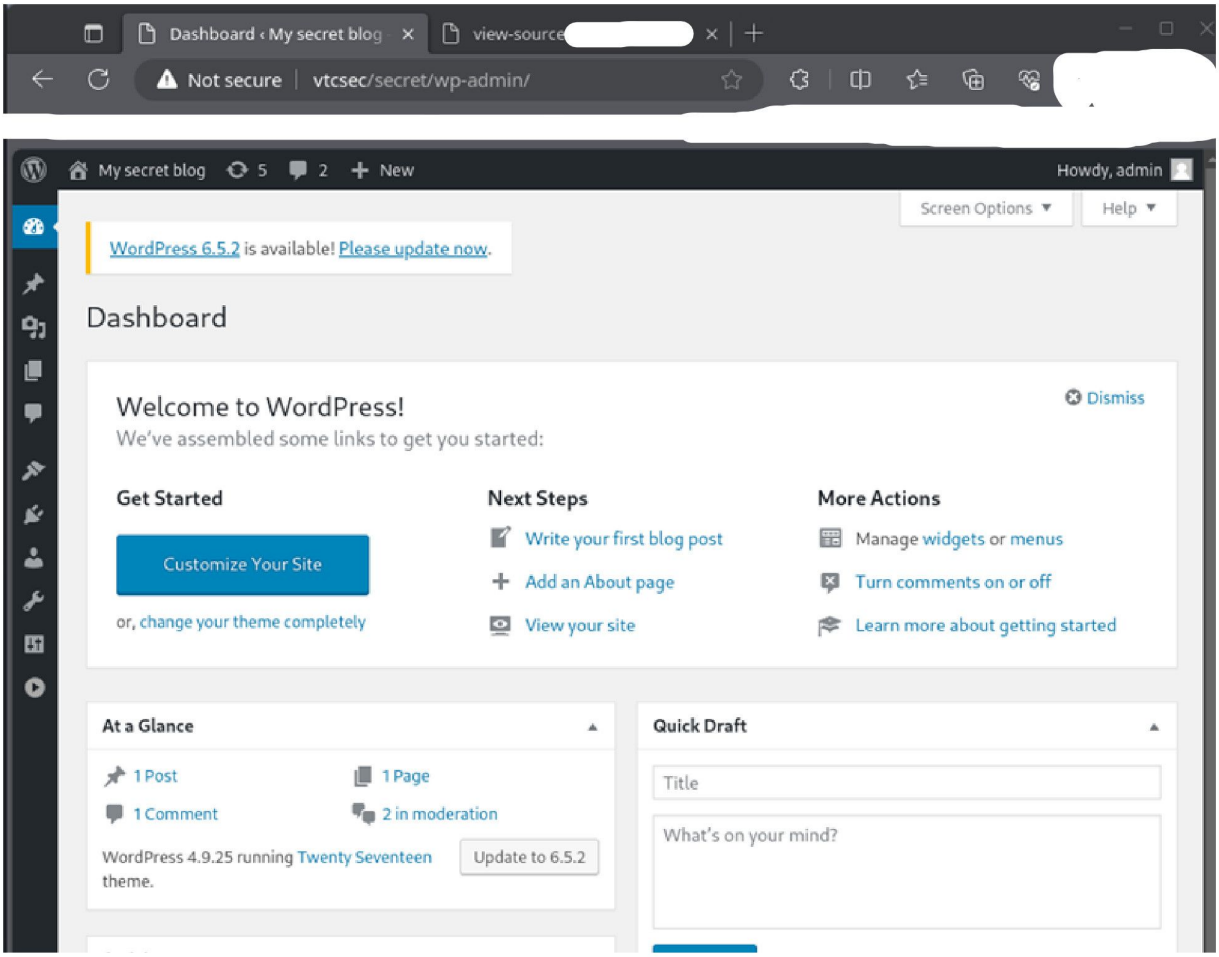
```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
<=======================================> (10 / 10) 100.00% Time:
00:00:00

[i] User(s) Identified:

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

After confirming the user identified as admin from the wp scan, I decided to first use the default password to wordpress which is also admin. I found the default password to work and gained admin access to the wordpress dashboard.




Dashboard ‹ My secret blog
view-source
Not secure
vtcsec/secret/wp-admin/
My secret blog
5
2
New
Howdy, admin
Screen Options
Help
WordPress 6.5.2 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
Get Started
Customize Your Site
or, change your theme completely
Next Steps
Write your first blog post
Add an About page
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started
At a Glance
1 Post
1 Page
1 Comment
2 in moderation
WordPress 4.9.25 running Twenty Seventeen theme.
Update to 6.5.2
Quick Draft
Title
What's on your mind?

2 - ICMP Timestamp Request Remote Date Disclosure

MEDIUM SEVERITY (2.1/10)	
IP Address Impacted	Machine1_ip

Security Implications

When a remote host receives an ICMP timestamp request, it responds by revealing the current date and time set on the targeted machine. This allows an attacker to know the date that is set on the targeted machine. By knowing the system's time, the attacker gains an advantage in their attempts to bypass security measures that rely on timing or time-based tokens.

Analysis

The attacker that performs this exploitation may:

- Authentication Bypass: An attacker can manipulate their own system time to bypass these mechanisms.
- Session Take Over: By accurately determining the target system's date, an attacker can synchronize their actions with specific events (e.g., session timeouts) to take control of active sessions.
- Forensic Manipulation: Malicious actors can alter timestamps on logs, files, or other system artifacts to cover their tracks during an attack.
- Replay Attacks: Accurate timestamps allow attackers to replay captured network traffic at the exact moment when validation of authentication tokens take place.
- Password Reset Attacks: If a password reset token is time-based, knowing the system date enables an attacker to generate valid tokens for unauthorized password resets.

Recommendations

- Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
- Regularly monitor and audit system logs for suspicious activity related to time manipulation.
- Implement additional authentication factors beyond time-based mechanisms.

References (opt)

- **N/a**

3 - UnrealIRCd Backdoor Detection

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to unauthorized access to servers running the affected versions from November 2009 through June 2010.

Analysis

The attacker that performs this exploitation may:

- Unauthorized Access - presence of the backdoor allows attackers to gain unauthorized access to the Metasploitable2.
- Data Theft and Manipulation - Attackers take sensitive data from the compromised system.
    - May access confidential files, databases, or user credentials stored on the server.
    - Additionally, they can alter or delete critical data, disrupting normal operations.
- Service Disruption - backdoor allows attackers to disrupt services such as injecting malicious code.
- Risk to Connected Clients - By an attacker gaining control of the Metasploitable2, they can go on to attacking other vulnerable systems on the network.

Recommendations

- Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
- Change passwords and review logs for suspicious activity.
- Inform users about the incident and encourage them to update their IRC clients.

References (opt)

- https://seclists.org/fulldisclosure/2010/Jun/277
- https://seclists.org/fulldisclosure/2010/Jun/284
- http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

4 - VNC Server 'password' Password

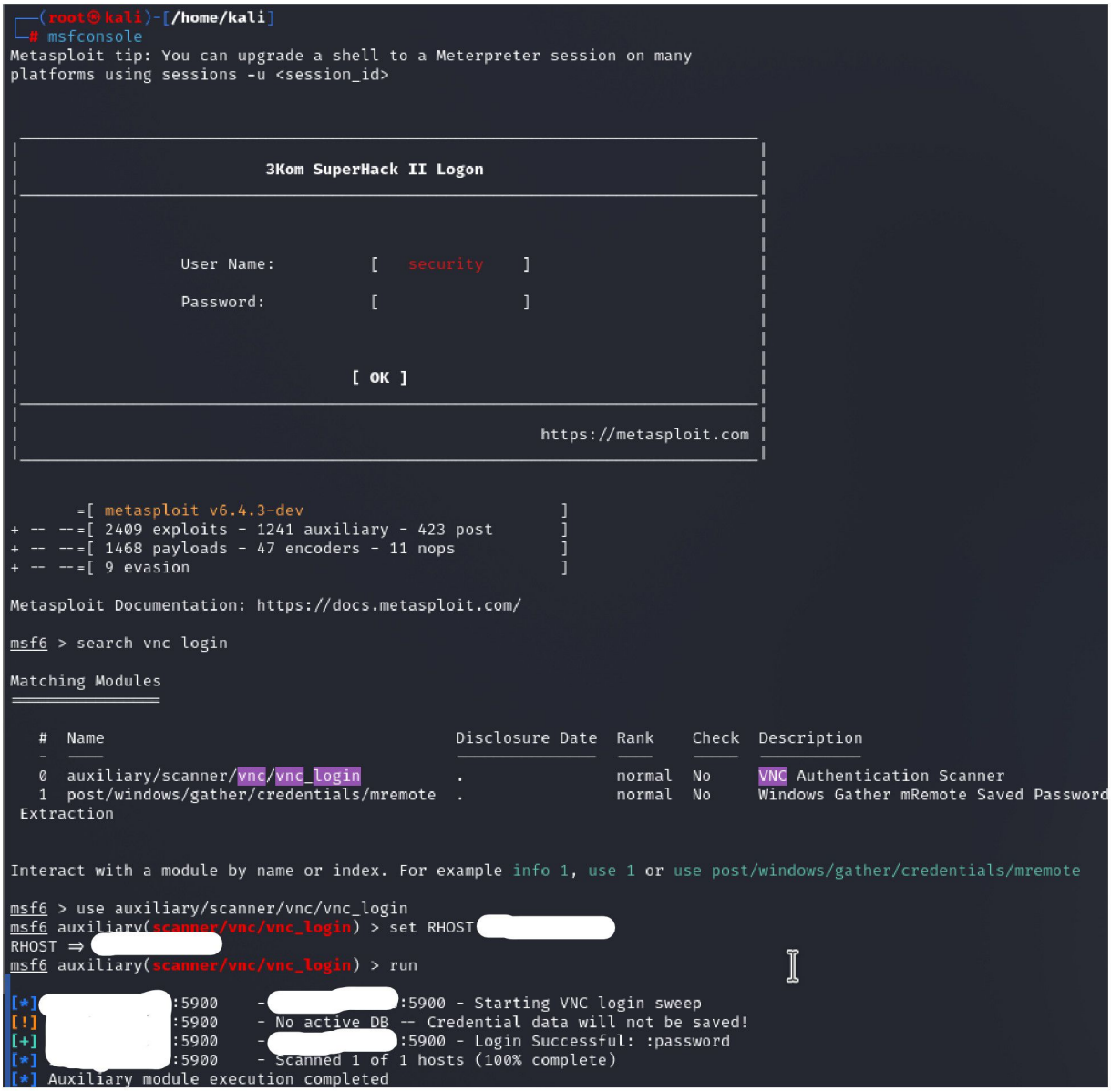
CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

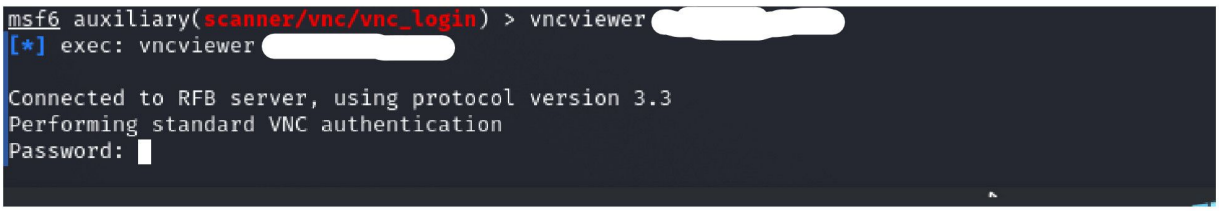
VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Analysis

This part goes through a possible method that a real-world threat actor can use to exploit this VNC Server.The terminal shows a successful login attempt using the VNC login module, which suggests that it is possible to gain unauthorized access to a system through the VNC protocol.

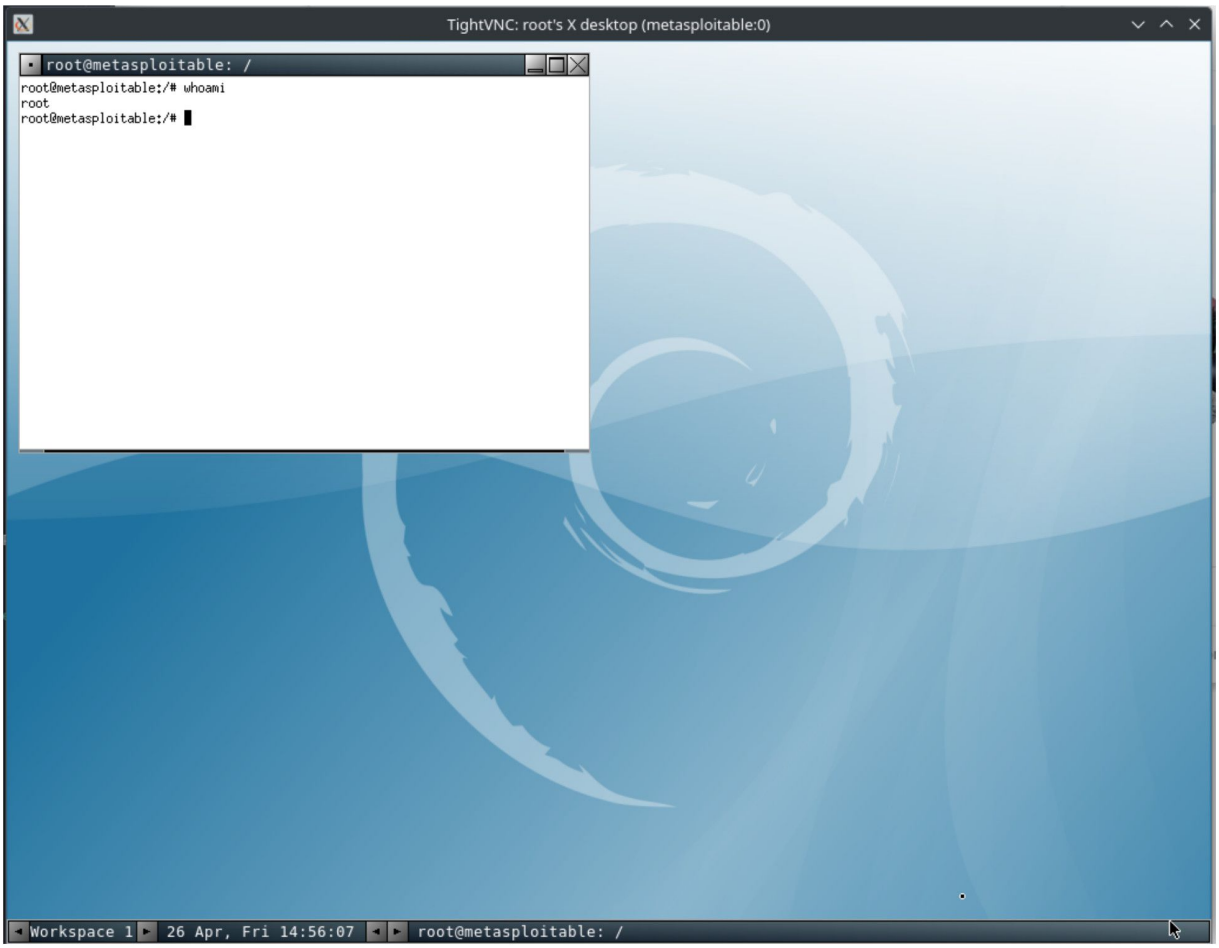


auxiliary/scanner/vnc/vnc_login suggests that there is a known backdoor exploit for ProFTPD version 1.3.3c to gain unauthorized access to the VNC Server.



Logged in with only using a password which is not secure and should be changed. The next screenshot is of a desktop environment with an open terminal window. The terminal shows a command whoami being executed, which is used to display the current system user. The output

root indicates that I was able to be logged in as the root user, which has administrative privileges.



Recommendations

- Secure the VNC service with a strong password.

References (opt)

- N/a

5 - NFS Exported Share Information Disclosure

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read and possibly write files on remote hosts.

Analysis

The attacker that performs this exploitation may:

- Exploiting a weakly configured NFS share can lead to unauthorized access to files or even obtaining a shell on the ip address impacted..

Recommendations

- Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
- Restrict IP Addresses: Limit the IP addresses that can mount exposed shares.
- Read-Only Access: Allow read-only access to exported shares if possible.

References (opt)

- N/a

6 - SSL Version 2 and 3 Protocol Detection

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Analysis

The attacker that performs this exploitation may:

- Attackers can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between affected service and clients.

Recommendations

- Consult the application's documentation to disable SSL 2.0 and 3.0.
- Use TLS 1.2 (with approved cipher suites) or higher instead.

References (opt)

- https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
- http://www.nessus.org/u?b06c7e95
- http://www.nessus.org/u?247c4540
- https://www.openssl.org/~bodo/ssl-poodle.pdf
- http://www.nessus.org/u?5d15ba70
- https://www.imperialviolet.org/2014/10/14/poodle.html

- https://tools.ietf.org/html/rfc7507
- https://tools.ietf.org/html/rfc7568

7 - Bind Shell Backdoor Detection

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

A shell is listening on the remote port without any authentication being required. An attacker may use shell by connecting to the remote port and sending commands directly.

Analysis

The attacker that performs this exploitation may:

- This situation poses a security risk because unauthorized users can potentially connect to Metasploitable 2 shell is listening on port 1524 (based from the output of the NMAP Scan) and gain access to the system.
- Tools like netcat(using the TCP/IP protocol to read and write data across network connections to connect to port 1524 from their Kali machine.

Recommendations

- Verify if the remote host has been compromised, and reinstall the system if necessary.

References (opt)

- N/a

8 - Unix Operating System Unsupported Version Detection

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

This indicates that the Unix operating system running on the remote host is no longer supported. Lack of support means that the vendor no longer releases new security patches for this specific version.

Analysis

The attacker that performs this exploitation may:

- Unsupported versions are more susceptible to security risks because they do not receive critical updates.
- Attackers can exploit known vulnerabilities found in the past to compromise this system.

Recommendations

- Upgrade to a version of the Unix operating system that is currently supported.
- Regularly check for updates and apply security patches to keep the system secure.

References (opt)

- N/a

9 - Apache Tomcat SEoL (<= 5.5.x)

CRITICAL SEVERITY (10.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Analysis

The attacker that performs this exploitation may:

- Attackers can exploit known vulnerabilities in unsupported versions to compromise the Tomcat server.
- The risk of not upgrading can lead to unauthorized access, data leakage, or even remote code execution.

Recommendations

- Upgrade to a version of Apache Tomcat that is currently supported.
- Continuously monitor for security updates and apply patches promptly.

References (opt)

- https://tomcat.apache.org/tomcat-55-eol.html

10 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

CRITICAL SEVERITY (7.5/10)	
IP Address Impacted	Machine2_ip

Security Implications

A file read/inclusion vulnerability was found in the AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server.

Analysis

The attacker that performs this exploitation may:

- In instances where the vulnerable server allows file uploads, attackers could upload malicious JavaServer Pages (JSP) code within various file types and potentially achieve remote code execution (RCE).

Recommendations

- Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
- Update the AJP configuration to require authorization.

References (opt)

- http://www.nessus.org/u?8ebe6246
- http://www.nessus.org/u?4e287adb
- http://www.nessus.org/u?cbc3d54e
- https://access.redhat.com/security/cve/CVE-2020-1745
- https://access.redhat.com/solutions/4851251
- http://www.nessus.org/u?dd218234
- http://www.nessus.org/u?dd772531
- http://www.nessus.org/u?2a01d6bf
- http://www.nessus.org/u?3b5af27e
- http://www.nessus.org/u?9dab109f
- http://www.nessus.org/u?5eafcf70

11 - NFS Shares World Readable

HIGH SEVERITY (5.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Analysis

The attacker that performs this exploitation may:

- This error on the remote NFS server configuration poses a security risk because sensitive data may be accessible to unauthorized users.

Recommendations

- Place the appropriate restrictions on all NFS shares (limit access based on hostname, IP, or IP range).

References (opt)

- http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

12 - rlogin Service Detection

HIGH SEVERITY 7.5/10)	
IP Address Impacted	Machine2_ip

Security Implications

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Analysis

The attacker that performs this exploitation may:

- Eavesdropping: Attacker can listen to the communication and capture login credentials.
- Man-in-the-Middle: A bad actor can position themselves between the client and server, intercepting and manipulating the data.
- Authentication Bypass: Misconfigured rlogin services may allow unauthorized access without proper authentication.

Recommendations

- Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

References (opt)

- N/a

13 - rsh Service Detection

HIGH SEVERITY (7.5/10)	
IP Address Impacted	Machine2_ip

Security Implications

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Analysis

The attacker that performs this exploitation may:

- Unauthorized users may gain access to the system due to weak authentication.

Recommendations

- Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

References (opt)

- N/a

14 - Samba Badlock Vulnerability

HIGH SEVERITY (6.8/10)	
IP Address Impacted	Machine2_ip

Security Implications

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Analysis

The attacker that performs this exploitation may:

- Attackers can abuse this vulnerability to execute code in the root context even without authentication.
- Sensitive security data in the Active Directory (AD) database may be at risk.

Recommendations

- Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- Follow security guidelines for Samba configurations.

References (opt)

- http://badlock.org
- https://www.samba.org/samba/security/CVE-2016-2118.html

15 - SSL Medium Strength Cipher Suites Supported (SWEET32)

HIGH SEVERITY (5.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

* Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Analysis

The attacker that performs this exploitation may:

- The attack takes advantage of the design weakness in these 64-bit block ciphers.
- An attacker has the possibility of recovering small portions of plaintext when encrypted with these weak ciphers.

Recommendations

- Reconfigure the affected application if possible to avoid use of medium strength ciphers.
- Disable the use of 3DES (Triple Data Encryption Standard) cipher suites.
- Prefer stronger encryption algorithms like AES (Advanced Encryption Standard) with larger block sizes.

References (opt)

- https://www.openssl.org/blog/blog/2016/08/24/sweet32/
- https://sweet32.info

16 - ISC BIND Service Downgrade / Reflected DoS

HIGH SEVERITY (5.0/10)	
IP Address Impacted	Machine2_ip

Security Implications

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Analysis

The attacker that performs this exploitation may:

- Degrade the performance of the DNS server.
- Use the affected server as a reflector in a reflection attack.

Recommendations

- Upgrade to the ISC BIND version referenced in the vendor advisory.
- Follow security guidelines for BIND configurations.

References (opt)

- https://kb.isc.org/docs/cve-2020-8616

APPENDIX A- TOOLS USED AND VERSION

TOOL	DESCRIPTION
Hydra	Used for password cracking.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
Nessus	Used to scan the networks for vulnerabilities.
Wireshark	Used to analyze the packets coming through the network.

Table A.1: *Tools used during assessment*

Version Information

Version	Date	Description
1.0	5/1/24	Initial report to client

APPENDIX B- CONTACT

Contact Information

Name	TerminalTinker
Address	
Phone	
Email	