Threats and Countermeasures

Lecture 08:
Technical Writing

COMP-5830/-6830
Spring 2025

PenTests are Technical Writing

Purpose of Technical Writing

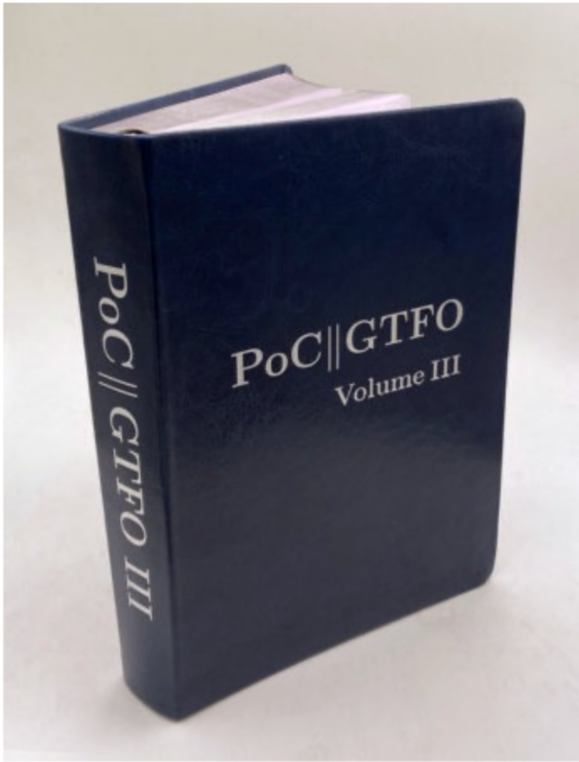
The purpose of writing technical documents is to **archive** and **communicate** information.

Purpose of Technical Writing

The purpose of writing technical documents is to archive **and** communicate information.

Purpose of Technical Writing

The purpose of writing technical documents is to **archive** and **communicate** information.



Purpose of Technical Writing

The purpose of writing technical documents is to **archive** and **communicate** information.

- Archive-only: PoCs, code, screenshots, diagrams, log files, etc

Purpose of Technical Writing

The purpose of writing technical documents is to **archive** and **communicate** information.

- Archive-only: PoCs, code, screenshots, diagrams, log files, etc
- Communicate-only: 30-day embargo alert, buying ”put” options, tweeting “Tango Down” 🤡

PenTests are Technical Writing

- Identify vulnerabilities you found
  - Whether used or not on the main-path

PenTests are Technical Writing

- Identify vulnerabilities you found
  - Whether used or not on the main-path
- Provide enough detail to be useful

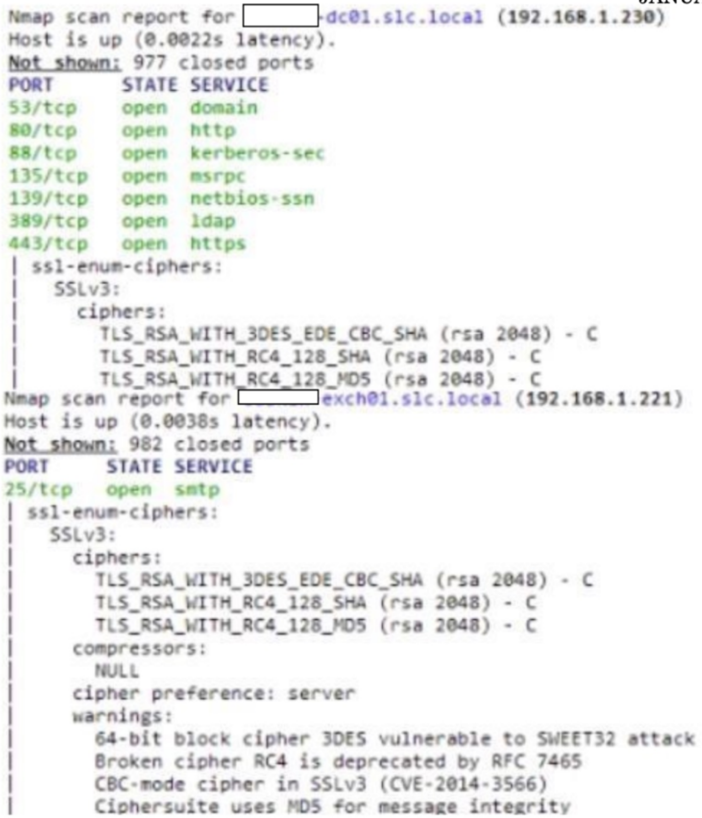
PenTests are Technical Writing

- Identify vulnerabilities you found
  - Whether used or not on the main-path
- Provide enough detail to be useful
- Be concise enough to avoid the infamous "forest vs. trees" situation

PenTests are Technical Writing

- Identify vulnerabilities you found
  - Whether used or not on the main-path
- Provide enough detail to be useful
- Be concise enough to avoid the infamous “forest vs. trees” situation
- Explain what it means for your audience
  - Scare enough to not ignore
  - Not scare to the point of nihilism or panic*

*unless panic is warranted



```
Nmap scan report for [redacted]-dc01.slc.local (192.168.1.230)
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
Nmap scan report for [redacted]exch01.slc.local (192.168.1.221)
Host is up (0.0038s latency).
Not shown: 982 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
```

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)(WINSHOCK)

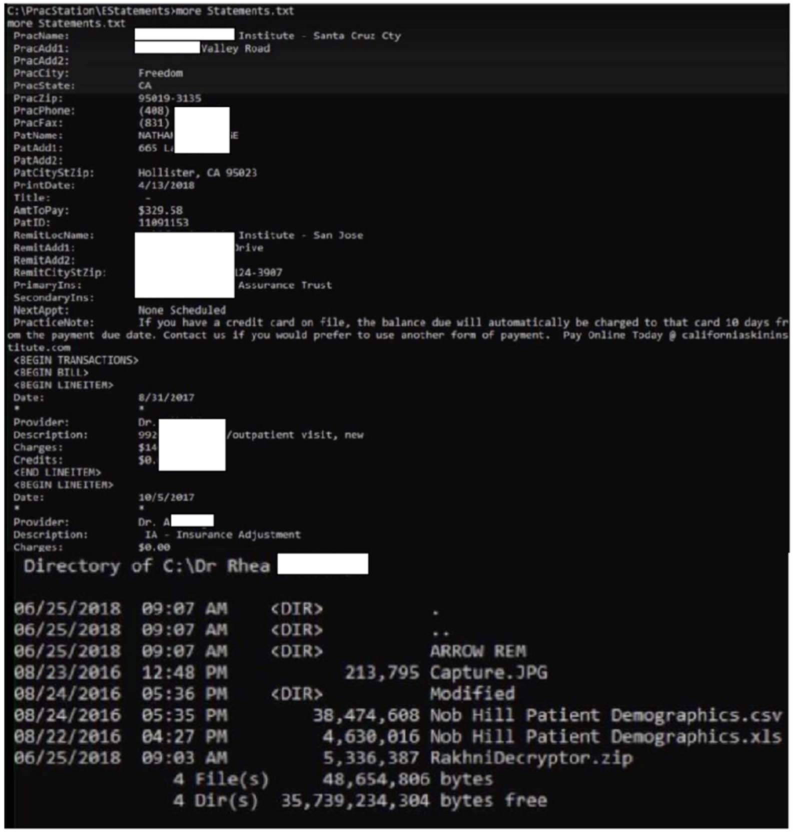
The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the SecureChannel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

EXPLOIT:
The exploit for this vulnerability is a remote code execution that typically results in a

---

From here the analyst performs several directory traversals to move to the root drive and begin reconnaissance for critical files such as patient information, ePHI, PII, and payment information. Traversing user profile document folders revealed several folders with sensitive, confidential patient and hospital information. Due to attaining access as the NT Authority user, no permissions settings or passwords prevent access to any of the files on the system.



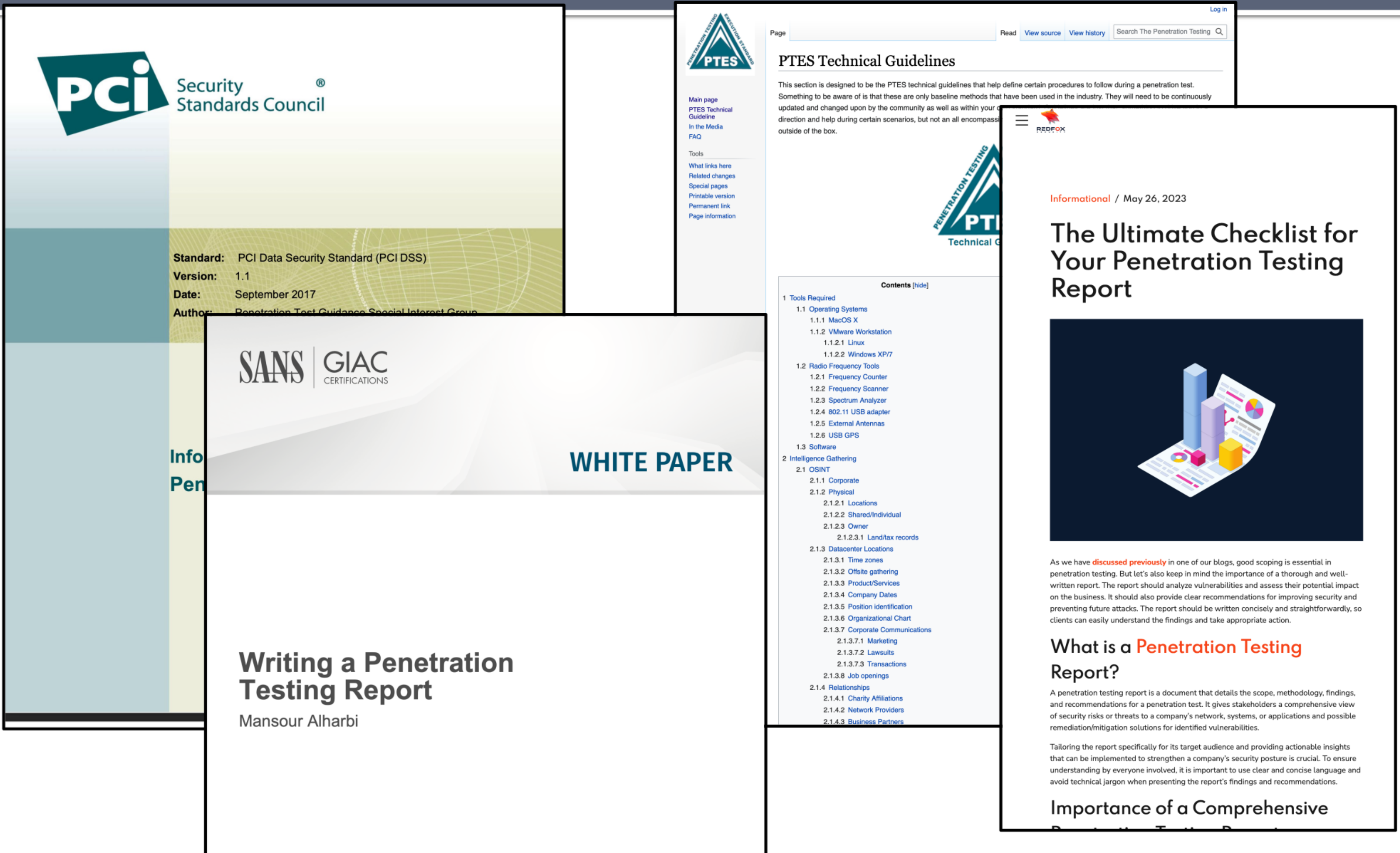
```
C:\PracStation\EStatements>more Statements.txt
more Statements.txt
 PracName:          [redacted] Institute - Santa Cruz Cty
 PracAdd1:          [redacted]Valley Road
 PracAdd2:
 PracCity:           Freedom
 PracState:          CA
 PracZip:            95019-3135
 PracPhone:          (408) [redacted]
 PracFax:            (831)
 PatName:            NATHA         E
 PatAdd1:            665 L
 PatAdd2:
 PatCityStZip:       Hollister, CA 95023
 PrintDate:          4/13/2018
 Title:               -
 AmtToPay:           $329.58
 PatID:              11091153
 RemitLocName:      [redacted] Institute - San Jose
 RemitAdd1:                    rive
 RemitAdd2:
 RemitCityStZip:               24-3907
 PrimaryIns:                   Assurance Trust
 SecondaryIns:
 NextAppt:           None Scheduled
 PracticeNote:       If you have a credit card on file, the balance due will automatically be charged to that card 10 days fr
om the payment due date. Contact us if you would prefer to use another form of payment.  Pay Online Today @ californiaskinins
titute.com
 <BEGIN TRANSACTIONS>
 <BEGIN BILL>
 <BEGIN LINEITEM>
 Date:               8/31/2017
 *                   *
 Provider:           Dr. [redacted]
 Description:        992          /outpatient visit, new
 Charges:            $14
 Credits:            $0.
 <END LINEITEM>
 <BEGIN LINEITEM>
 Date:               10/5/2017
 *                   *
 Provider:           Dr. A[redacted]
 Description:         IA - Insurance Adjustment
 Charges:            $0.00
 Directory of C:\Dr Rhea [redacted]

06/25/2018  09:07 AM    <DIR>          .
06/25/2018  09:07 AM    <DIR>          ..
06/25/2018  09:07 AM    <DIR>          ARROW REM
08/23/2016  12:48 PM           213,795 Capture.JPG
08/24/2016  05:36 PM    <DIR>          Modified
08/24/2016  05:35 PM        38,474,608 Nob Hill Patient Demographics.csv
08/22/2016  04:27 PM         4,630,016 Nob Hill Patient Demographics.xls
06/25/2018  09:03 AM         5,336,387 RakhniDecryptor.zip
               4 File(s)     48,654,806 bytes
               4 Dir(s)  35,739,234,304 bytes free
```

User profiles contain various files that, if breached, could make Example Institute liable for fines.

In addition to the noted HIPAA and ePHI files, a PFX certificate file was also located on the server.

There are Lots of Opinions



Security Standards Council ®

Standard: PCI Data Security Standard (PCI DSS)
Version: 1.1
Date: September 2017
Author: Penetration Test Guidance Special Interest Group

Info
Pen

SANS | GIAC CERTIFICATIONS

WHITE PAPER

Writing a Penetration Testing Report

Mansour Alharbi

PTES Technical Guidelines

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your
direction and help during certain scenarios, but not an all encompassi
outside of the box.

Technical G

Contents [hide]

1 Tools Required
  1.1 Operating Systems
    1.1.1 MacOS X
    1.1.2 VMware Workstation
      1.1.2.1 Linux
      1.1.2.2 Windows XP/7
  1.2 Radio Frequency Tools
    1.2.1 Frequency Counter
    1.2.2 Frequency Scanner
    1.2.3 Spectrum Analyzer
    1.2.4 802.11 USB adapter
    1.2.5 External Antennas
    1.2.6 USB GPS
  1.3 Software
2 Intelligence Gathering
  2.1 OSINT
    2.1.1 Corporate
    2.1.2 Physical
      2.1.2.1 Locations
      2.1.2.2 Shared/Individual
      2.1.2.3 Owner
        2.1.2.3.1 Land/tax records
    2.1.3 Datacenter Locations
      2.1.3.1 Time zones
      2.1.3.2 Offsite gathering
      2.1.3.3 Product/Services
      2.1.3.4 Company Dates
      2.1.3.5 Position identification
      2.1.3.6 Organizational Chart
      2.1.3.7 Corporate Communications
        2.1.3.7.1 Marketing
        2.1.3.7.2 Lawsuits
        2.1.3.7.3 Transactions
      2.1.3.8 Job openings
    2.1.4 Relationships
      2.1.4.1 Charity Affiliations
      2.1.4.2 Network Providers
      2.1.4.3 Business Partners

Informational / May 26, 2023

The Ultimate Checklist for Your Penetration Testing Report

As we have discussed previously in one of our blogs, good scoping is essential in penetration testing. But let's also keep in mind the importance of a thorough and well-written report. The report should analyze vulnerabilities and assess their potential impact on the business. It should also provide clear recommendations for improving security and preventing future attacks. The report should be written concisely and straightforwardly, so clients can easily understand the findings and take appropriate action.

What is a Penetration Testing Report?

A penetration testing report is a document that details the scope, methodology, findings, and recommendations for a penetration test. It gives stakeholders a comprehensive view of security risks or threats to a company's network, systems, or applications and possible remediation/mitigation solutions for identified vulnerabilities.

Tailoring the report specifically for its target audience and providing actionable insights that can be implemented to strengthen a company's security posture is crucial. To ensure understanding by everyone involved, it is important to use clear and concise language and avoid technical jargon when presenting the report's findings and recommendations.

Importance of a Comprehensive

Major Parts of Pen-Test Report

- Executive Summary
- Findings
- Recommendations
- Appendices

Major Parts of Pen-Test Report

- Executive Summary
  - The ***shortest possible*** version of what you found/did (~1 page max)

Major Parts of Pen-Test Report

- Executive Summary
  - The ***shortest possible*** version of what you found/did (~1 page max)
- Findings
  - Discussion of what you found, how you found it, and what it means

Major Parts of Pen-Test Report

- Executive Summary
  - The ***shortest possible*** version of what you found/did (~1 page max)
- Findings
  - Discussion of what you found, how you found it, and what it means
- Recommendations
  - How the customer can fix the things you found

Major Parts of Pen-Test Report

- Executive Summary
  - The ***shortest possible*** version of what you found/did (~1 page max)
- Findings
  - Discussion of what you found, how you found it, and what it means
- Recommendations
  - How the customer can fix the things you found
- Appendices
  - The gritty details that might not be obvious

Technical Writing Audience

Who are you communicating with?

Technical Writing Audience

Who are you communicating with?

Technical Writing Audience

Who are you communicating with?

Technical Writing Audience

Who are you communicating with?

Technical Writing Audience

Who are you communicating with?

Audience of Pen-Test Report

- Executive Summary
  - Non-technical people (C-Suite, management, …)

Audience of Pen-Test Report

- Executive Summary
  - Non-technical people (C-Suite, management, …)
- Findings
  - Technical/Semi-Technical people (IT, security, consultants, etc)

Audience of Pen-Test Report

- Executive Summary
  - Non-technical people (C-Suite, management, …)
- Findings
  - Technical/Semi-Technical people (IT, security, consultants, etc)
- Recommendations
  - Technical/Semi-Technical people (IT, security, consultants, etc)

Audience of Pen-Test Report

- Executive Summary
  - Non-technical people (C-Suite, management, …)
- Findings
  - Technical/Semi-Technical people (IT, security, consultants, etc)
- Recommendations
  - Technical/Semi-Technical people (IT, security, consultants, etc)
- Appendices
  - The really, really technical people

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
  - Yes --- **MAKE SURE THEY REALIZE THAT**

Focus on Important/Useful Details

Focus on Important/Useful Details

Bad Version

I found that your systems are vulnerable to CVE-2024-1234, CVE-2009-456, CVE-2014-789,CVE-2022-583, CVE-2025-001, CVE-2023-658, and CVE-2023-611. Please ensure they are promptly patched.

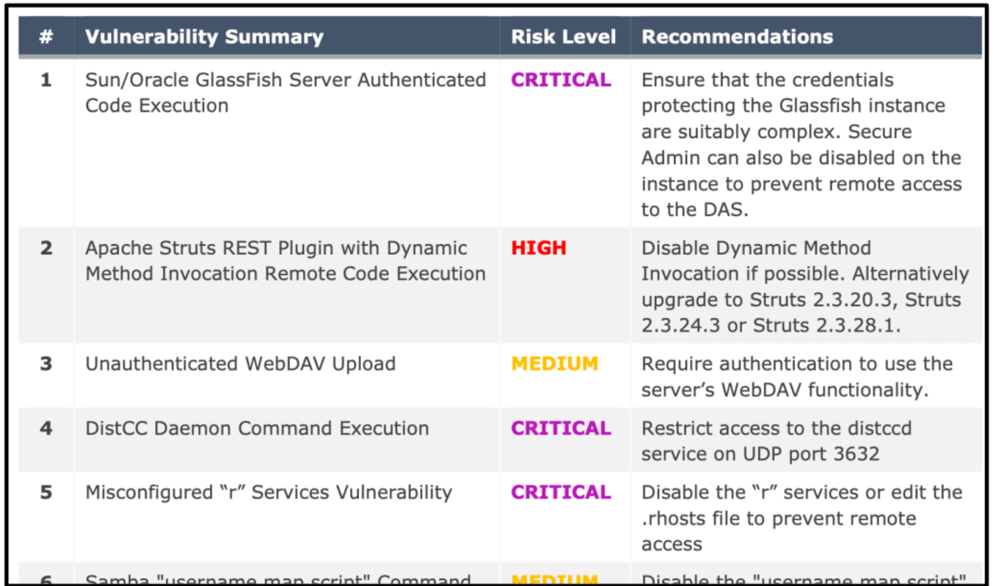
Focus on Important/Useful Details

Bad Version

I found that your systems are vulnerable to CVE-2024-1234, CVE-2009-456, CVE-2014-789,CVE-2022-583, CVE-2025-001, CVE-2023-658, and CVE-2023-611. Please ensure they are promptly patched.

Better Version

There are multiple **CRITICAL** and HIGH severity CVEs on your network:



#	Vulnerability Summary	Risk Level	Recommendations
1	Sun/Oracle GlassFish Server Authenticated Code Execution	**CRITICAL**	Ensure that the credentials protecting the Glassfish instance are suitably complex. Secure Admin can also be disabled on the instance to prevent remote access to the DAS.
2	Apache Struts REST Plugin with Dynamic Method Invocation Remote Code Execution	**HIGH**	Disable Dynamic Method Invocation if possible. Alternatively upgrade to Struts 2.3.20.3, Struts 2.3.24.3 or Struts 2.3.28.1.
3	Unauthenticated WebDAV Upload	**MEDIUM**	Require authentication to use the server's WebDAV functionality.
4	DistCC Daemon Command Execution	**CRITICAL**	Restrict access to the distccd service on UDP port 3632
5	Misconfigured "r" Services Vulnerability	**CRITICAL**	Disable the "r" services or edit the .rhosts file to prevent remote access
6	Samba "username map script" Command	**MEDIUM**	Disable the "username map script"

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
    - Yes --- **MAKE SURE THEY REALIZE THAT**

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
  - Yes --- **MAKE SURE THEY REALIZE THAT**
  - No --- …

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
  - Yes --- **MAKE SURE THEY REALIZE THAT**
  - No --- …
- Is this piece of information useful to the audience in a way that’s non-trivial?

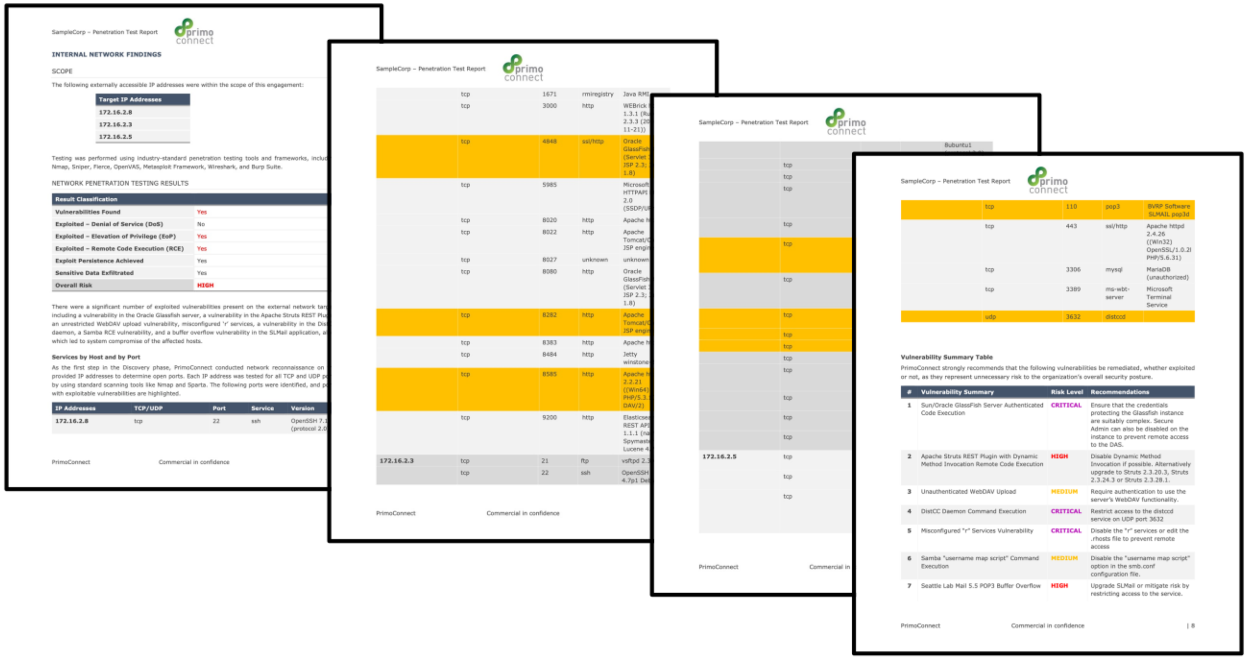
Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
  - Yes --- **MAKE SURE THEY REALIZE THAT**
  - No --- …
- Is this piece of information useful to the audience in a way that's non-trivial?
  - Yes --- If can work into writing, great. Otherwise, put in appendix.

Focus on Important/Useful Details

Bad Version

Below is network scan findings:



SampleCorp – Penetration Test Report

INTERNAL NETWORK FINDINGS

SCOPE

The following externally accessible IP addresses were within the scope of this engagement:

Target IP Addresses
172.16.2.8
172.16.2.3
172.16.2.5

Testing was performed using industry-standard penetration testing tools and frameworks, includ
Nmap, Sniper, Fierce, OpenVAS, Metasploit Framework, Wireshark, and Burp Suite.

NETWORK PENETRATION TESTING RESULTS

Result Classification	
Vulnerabilities Found	Yes
Exploited – Denial of Service (DoS)	No
Exploited – Elevation of Privilege (EoP)	Yes
Exploited – Remote Code Execution (RCE)	Yes
Exploit Persistence Achieved	Yes
Sensitive Data Exfiltrated	Yes
Overall Risk	HIGH

There were a significant number of exploited vulnerabilities present on the external network tar
including a vulnerability in the Oracle Glassfish server, a vulnerability in the Apache Struts REST Plu
an unrestricted WebDAV upload vulnerability, misconfigured 'r' services, a vulnerability in the Dis
daemon, a Samba RCE vulnerability, and a buffer overflow vulnerability in the SLMail application, a
which led to system compromise of the affected hosts.

Services by Host and by Port

As the first step in the Discovery phase, PrimoConnect conducted network reconnaissance on
provided IP addresses to determine open ports. Each IP address was tested for all TCP and UDP p
by using standard scanning tools like Nmap and Sparta. The following ports were identified, and p
with exploitable vulnerabilities are highlighted.

IP Addresses	TCP/UDP	Port	Service	Version
172.16.2.8	tcp	22	ssh	OpenSSH 7.1 (protocol 2.0

PrimoConnect Commercial in confidence

SampleCorp – Penetration Test Report

	tcp	1671	rmiregistry	Java RMI
	tcp	3000	http	WEBrick 1.3.1 (Ru 2.3.3 (20 11-21))
	tcp	4848	ssl/http	Oracle GlassFish (Servlet JSP 2.3; 1.8)
	tcp	5985		Microsoft HTTPAPI 2.0 (SSDP/U
	tcp	8020	http	Apache h
	tcp	8022	http	Apache Tomcat/ JSP engi
	tcp	8027	unknown	unknown
	tcp	8080	http	Oracle GlassFish (Servlet JSP 2.3; 1.8)
	tcp	8282	http	Apache Tomcat/ JSP engi
	tcp	8383	http	Apache h
	tcp	8484	http	Jetty winstone
	tcp	8585	http	Apache h 2.2.21 ((Win64) PHP/5.3. DAV/2)
	tcp	9200	http	Elasticse REST API 1.1.1 (na Spymast Lucene 4
172.16.2.3	tcp	21	ftp	vsftpd 2.3
	tcp	22	ssh	OpenSSH 4.7p1 Deb

PrimoConnect Commercial in confidence

SampleCorp – Penetration Test Report

				Bubuntu1
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
	tcp			
172.16.2.5	tcp			
	tcp			
	tcp			

PrimoConnect Commercial in

SampleCorp – Penetration Test Report

	tcp	110	pop3	BVRP Software SLMAIL pop3d
	tcp	443	ssl/http	Apache httpd 2.4.26 ((Win32) OpenSSL/1.0.2l PHP/5.6.31)
	tcp	3306	mysql	MariaDB (unauthorized)
	tcp	3389	ms-wbt-server	Microsoft Terminal Service
	udp	3632	distccd	

Vulnerability Summary Table

PrimoConnect strongly recommends that the following vulnerabilities be remediated, whether exploited or not, as they represent unnecessary risk to the organization's overall security posture.

#	Vulnerability Summary	Risk Level	Recommendations
1	Sun/Oracle GlassFish Server Authenticated Code Execution	CRITICAL	Ensure that the credentials protecting the Glassfish instance are suitably complex. Secure Admin can also be disabled on the instance to prevent remote access to the DAS.
2	Apache Struts REST Plugin with Dynamic Method Invocation Remote Code Execution	HIGH	Disable Dynamic Method Invocation if possible. Alternatively upgrade to Struts 2.3.20.3, Struts 2.3.24.3 or Struts 2.3.28.1.
3	Unauthenticated WebDAV Upload	MEDIUM	Require authentication to use the server's WebDAV functionality.
4	DistCC Daemon Command Execution	CRITICAL	Restrict access to the distccd service on UDP port 3632
5	Misconfigured "r" Services Vulnerability	CRITICAL	Disable the "r" services or edit the .rhosts file to prevent remote access
6	Samba "username map script" Command Execution	MEDIUM	Disable the "username map script" option in the smb.conf configuration file.
7	Seattle Lab Mail 5.5 POP3 Buffer Overflow	HIGH	Upgrade SLMail or mitigate risk by restricting access to the service.

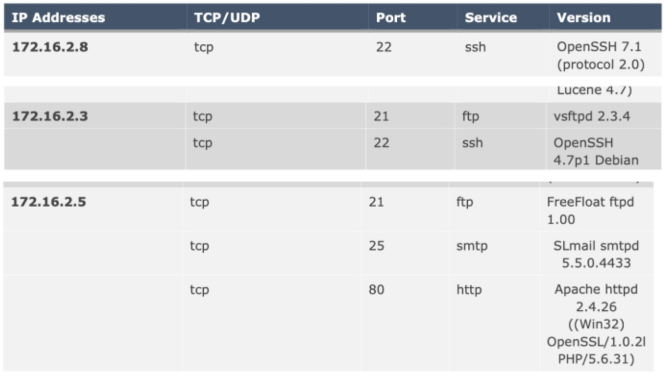
PrimoConnect Commercial in confidence | 8

Focus on Important/Useful Details

Bad Version

Better Version

Complete network scan results are in Appendix XXXX, but the material elements are:



IP Addresses	TCP/UDP	Port	Service	Version
172.16.2.8	tcp	22	ssh	OpenSSH 7.1 (protocol 2.0)
				Lucene 4.7)
172.16.2.3	tcp	21	ftp	vsftpd 2.3.4
	tcp	22	ssh	OpenSSH 4.7p1 Debian
172.16.2.5	tcp	21	ftp	FreeFloat ftpd 1.00
	tcp	25	smtp	SLmail smtpd 5.5.0.4433
	tcp	80	http	Apache httpd 2.4.26 ((Win32) OpenSSL/1.0.2l PHP/5.6.31)

Focus on Important/Useful Details

- Does the audience need to know this specific piece of information at this exact moment?
  - Yes --- **MAKE SURE THEY REALIZE THAT**
  - No --- …
- Is this piece of information useful to the audience in a way that's non-trivial?
  - Yes --- If can work into writing, great. Otherwise, put in appendix.
  - No --- Then archive it (logs, notes, etc.)

Omit Unnecessary Details

Omit Unnecessary Details

Bad Version

I was able to access the formula for Coke by first scanning your network for in-use IP addresses via nmap [https://nmap.org/]. Then for each in-use IP address, scanning for commonly used ports then all TCP ports. I first used the -sn flags followed by the –sT flags. I then created a local reproductions using PHP 8.1 installed in an Ubuntu VM via the command sudo apt install php. Upon completion of installation, I manually executing 739 different tests consisting of the following case:

- HTML
- HTML+CSS
- HTML+JavaScript
- HTML+PHP
- HTML+CSS+JavaScript
- HTML+CSS+PHP
- ….

Omit Unnecessary Details

Bad Version

I was able to access the formula for Coke by first scanning your network for in-use IP addresses via nmap [https://nmap.org/]. Then for each in-use IP address, scanning for commonly used ports then all TCP ports. I first used the -sn flags followed by the –sT flags. I then created a local reproductions using PHP 8.1 installed in an Ubuntu VM via the command sudo apt install php. Upon completion of installation, I manually executing 739 different tests consisting of the following case:

- HTML
- HTML+CSS
- HTML+JavaScript
- HTML+PHP
- HTML+CSS+JavaScript
- HTML+CSS+PHP
- ….

Better Version

Using standard network enumeration tools, we identified a weakness in the PHP's server's handling of image uploads allowing us to upload/execute arbitrary PHP code.

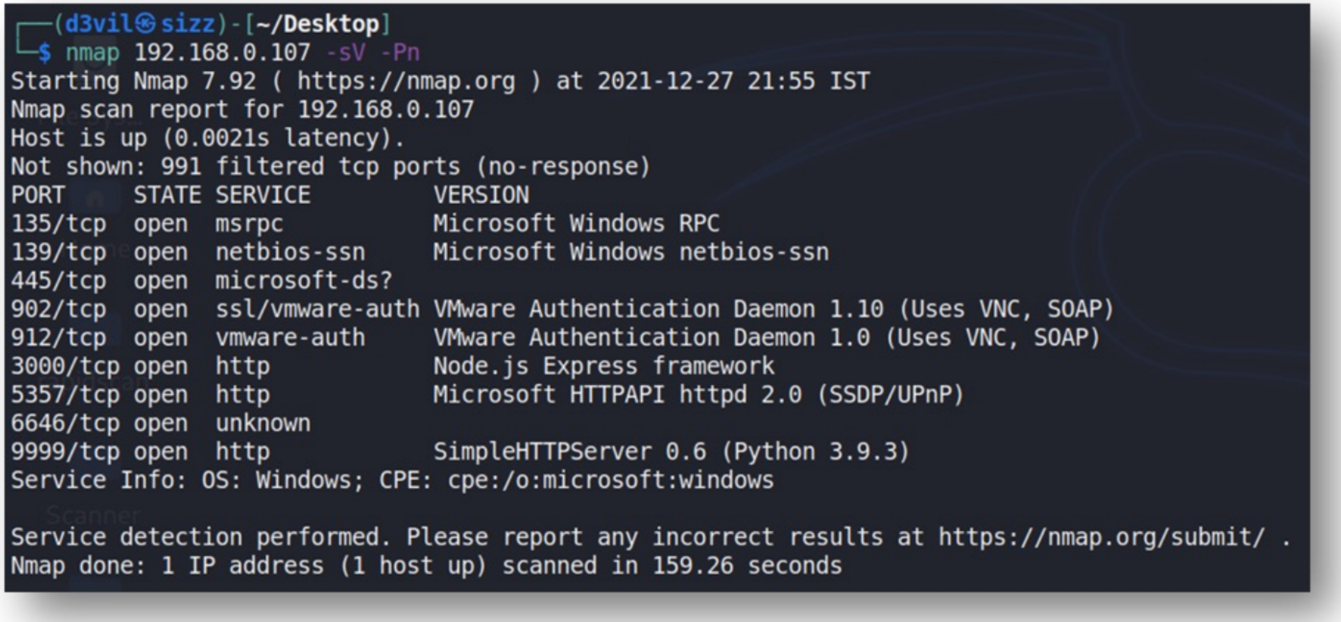
Interpret for your Audience

Interpret for your Audience

- Your audience chose **you** for a reason
    - May not have the technical skills, time, etc.

Interpret for your Audience

- Your audience chose **you** for a reason
  - May not have the technical skills, time, etc.

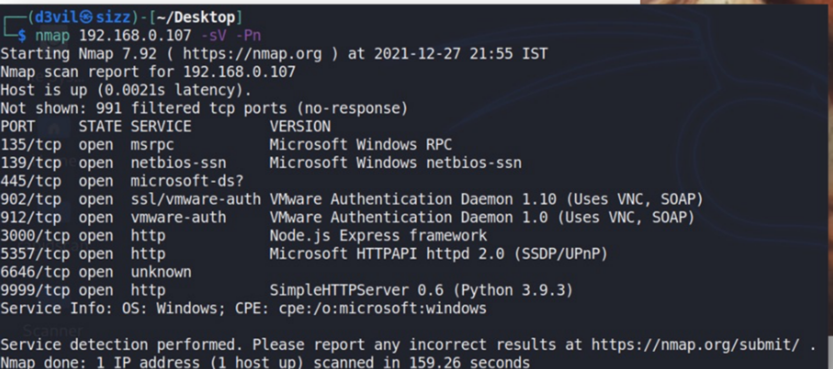


```
┌──(d3vil㉿sizz)-[~/Desktop]
└─$ nmap 192.168.0.107 -sV -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-27 21:55 IST
Nmap scan report for 192.168.0.107
Host is up (0.0021s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
135/tcp  open  msrpc          Microsoft Windows RPC
139/tcp  open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3000/tcp open  http           Node.js Express framework
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp open  unknown
9999/tcp open  http           SimpleHTTPServer 0.6 (Python 3.9.3)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.26 seconds
```

Interpret for your Audience

- Your audience chose **you** for a reason
  - May not have the technical skills, time, etc.



```
┌──(d3vil㉿sizz)-[~/Desktop]
└─$ nmap 192.168.0.107 -sV -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-27 21:55 IST
Nmap scan report for 192.168.0.107
Host is up (0.0021s latency).
Not shown: 991 filtered tcp ports (no-response)
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?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3000/tcp open  http            Node.js Express framework
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp open  unknown
9999/tcp open  http            SimpleHTTPServer 0.6 (Python 3.9.3)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.26 seconds
```

Interpret for your Audience

- Your audience chose **you** for a reason
  - May not have the technical skills, time, etc.

- **You** are the most knowledgeable person

Interpret for your Audience

- Your audience chose **you** for a reason
    - May not have the technical skills, time, etc.

- **You** are the most knowledgeable person

- Your audience wants **you** to provide:
    - The thing they asked for
    - Confidence that it's what they wanted
    - Ability to use it for their purpose

Interpret for your Audience

- Your audience chose **you** for a reason
  - May not have the technical skills, time, etc.

- **You** are the most knowledgeable person

- Your audience wants **you** to provide:
  - The thing they asked for
  - Confidence that it's what they wanted
  - Ability to use it for *<u>their purpose</u>*

PenTest Reports are NOT…

- Experience reports
- Mechanical, fill-in-the-blank documents
- English prose
- Word-smithed legalese discussions
- “Guesstimations”

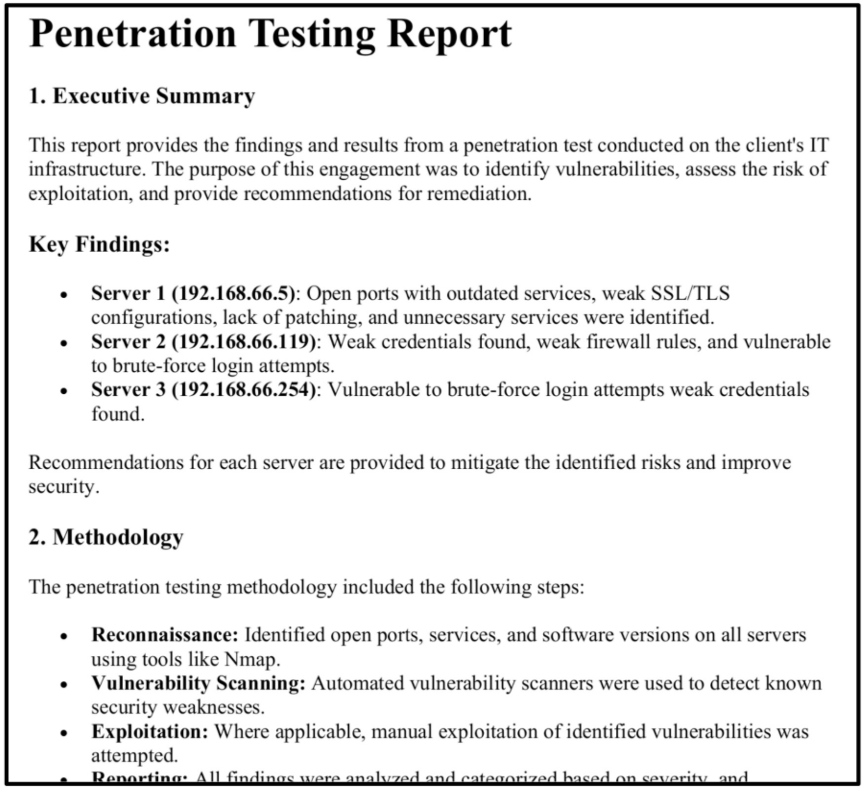
Threats and Countermeasures

Lecture 08:
PenTest Report Review

COMP-5830/-6830
Spring 2025

BAD REPORT EXAMPLE---DO NOT REPLICATE

BAD REPORT EXAMPLE---DO NOT REPLICATE



Penetration Testing Report

1. Executive Summary

This report provides the findings and results from a penetration test conducted on the client's IT infrastructure. The purpose of this engagement was to identify vulnerabilities, assess the risk of exploitation, and provide recommendations for remediation.

Key Findings:

- **Server 1 (192.168.66.5)**: Open ports with outdated services, weak SSL/TLS configurations, lack of patching, and unnecessary services were identified.
- **Server 2 (192.168.66.119)**: Weak credentials found, weak firewall rules, and vulnerable to brute-force login attempts.
- **Server 3 (192.168.66.254)**: Vulnerable to brute-force login attempts weak credentials found.

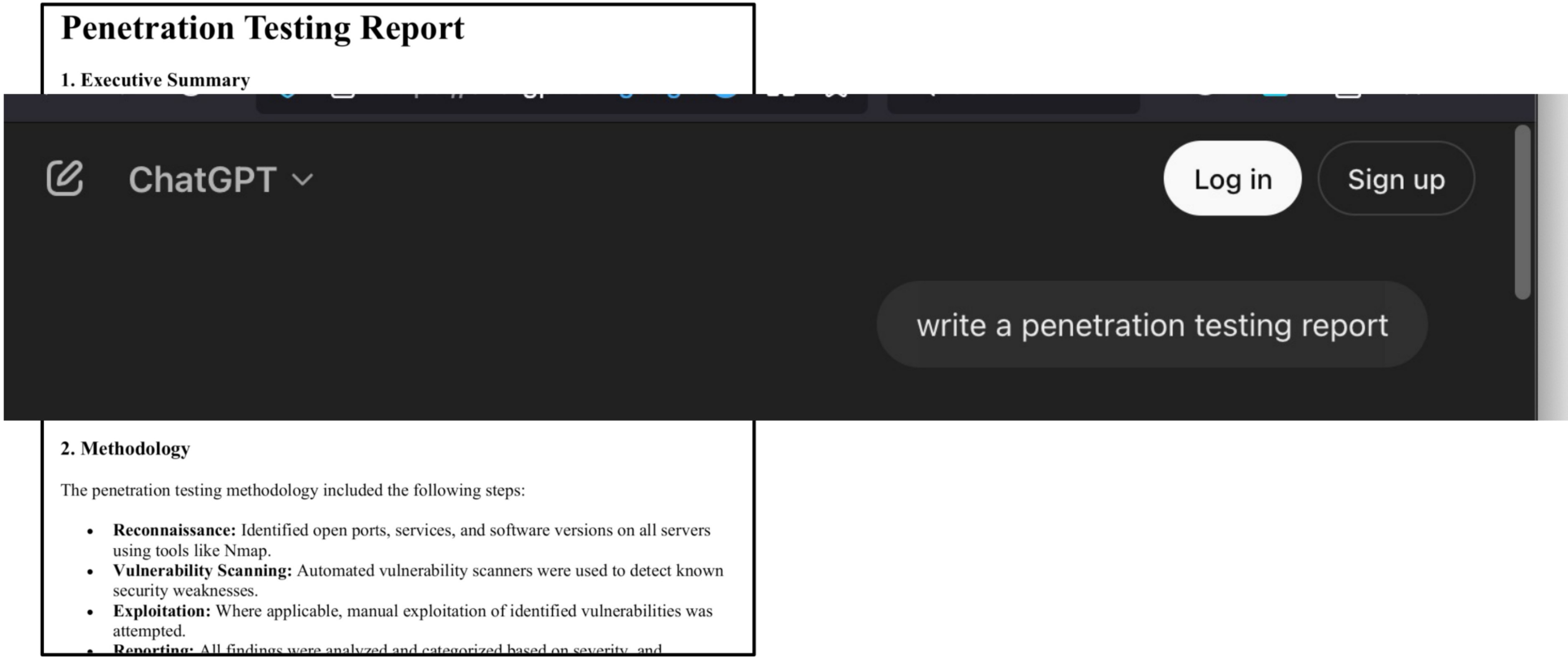
Recommendations for each server are provided to mitigate the identified risks and improve security.

2. Methodology

The penetration testing methodology included the following steps:

- **Reconnaissance:** Identified open ports, services, and software versions on all servers using tools like Nmap.
- **Vulnerability Scanning:** Automated vulnerability scanners were used to detect known security weaknesses.
- **Exploitation:** Where applicable, manual exploitation of identified vulnerabilities was attempted.
- **Reporting:** All findings were analyzed and categorized based on severity, and

BAD REPORT EXAMPLE---DO NOT REPLICATE



write a penetration testing report

Penetration Testing Report

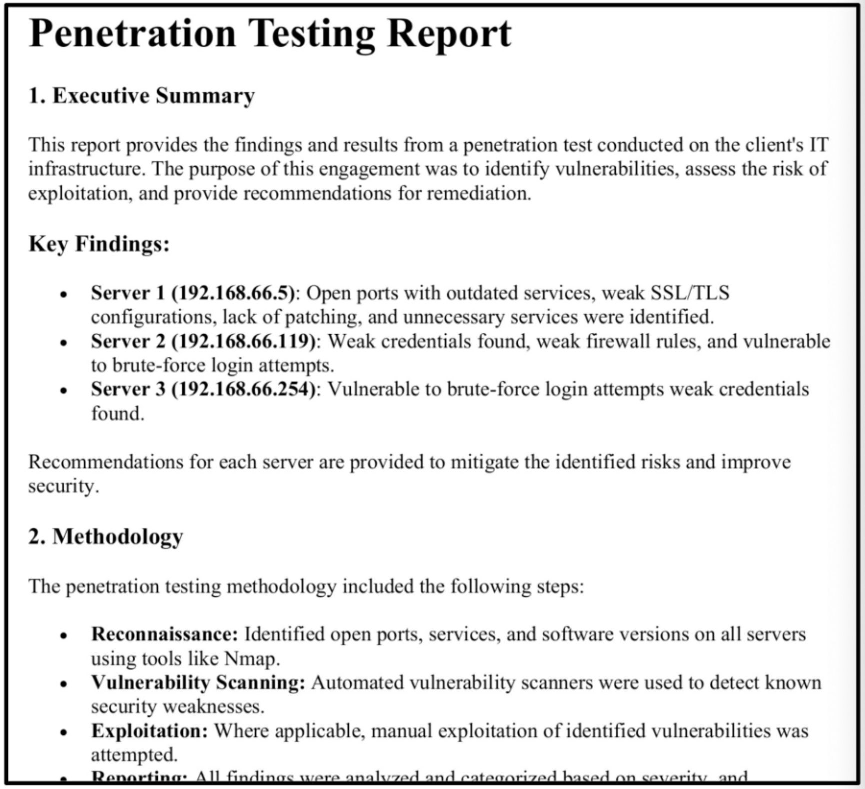
1. Executive Summary

2. Methodology

The penetration testing methodology included the following steps:

- **Reconnaissance:** Identified open ports, services, and software versions on all servers using tools like Nmap.
- **Vulnerability Scanning:** Automated vulnerability scanners were used to detect known security weaknesses.
- **Exploitation:** Where applicable, manual exploitation of identified vulnerabilities was attempted.
- **Reporting:** All findings were analyzed and categorized based on severity, and

BAD REPORT EXAMPLE---DO NOT REPLICATE



Penetration Testing Report

1. Executive Summary

This report provides the findings and results from a penetration test conducted on the client's IT infrastructure. The purpose of this engagement was to identify vulnerabilities, assess the risk of exploitation, and provide recommendations for remediation.

Key Findings:

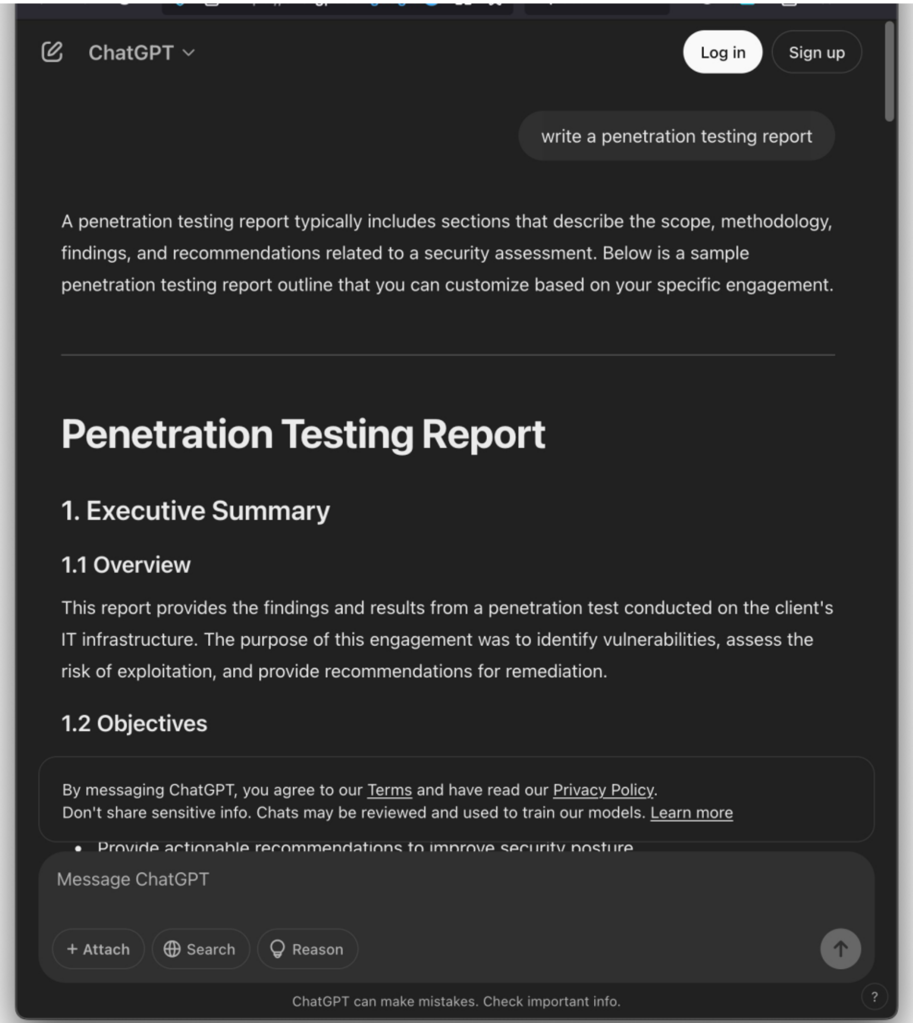
- **Server 1 (192.168.66.5)**: Open ports with outdated services, weak SSL/TLS configurations, lack of patching, and unnecessary services were identified.
- **Server 2 (192.168.66.119)**: Weak credentials found, weak firewall rules, and vulnerable to brute-force login attempts.
- **Server 3 (192.168.66.254)**: Vulnerable to brute-force login attempts weak credentials found.

Recommendations for each server are provided to mitigate the identified risks and improve security.

2. Methodology

The penetration testing methodology included the following steps:

- **Reconnaissance:** Identified open ports, services, and software versions on all servers using tools like Nmap.
- **Vulnerability Scanning:** Automated vulnerability scanners were used to detect known security weaknesses.
- **Exploitation:** Where applicable, manual exploitation of identified vulnerabilities was attempted.
- **Reporting:** All findings were analyzed and categorized based on severity, and



write a penetration testing report

A penetration testing report typically includes sections that describe the scope, methodology, findings, and recommendations related to a security assessment. Below is a sample penetration testing report outline that you can customize based on your specific engagement.

Penetration Testing Report

1. Executive Summary

1.1 Overview

This report provides the findings and results from a penetration test conducted on the client's IT infrastructure. The purpose of this engagement was to identify vulnerabilities, assess the risk of exploitation, and provide recommendations for remediation.

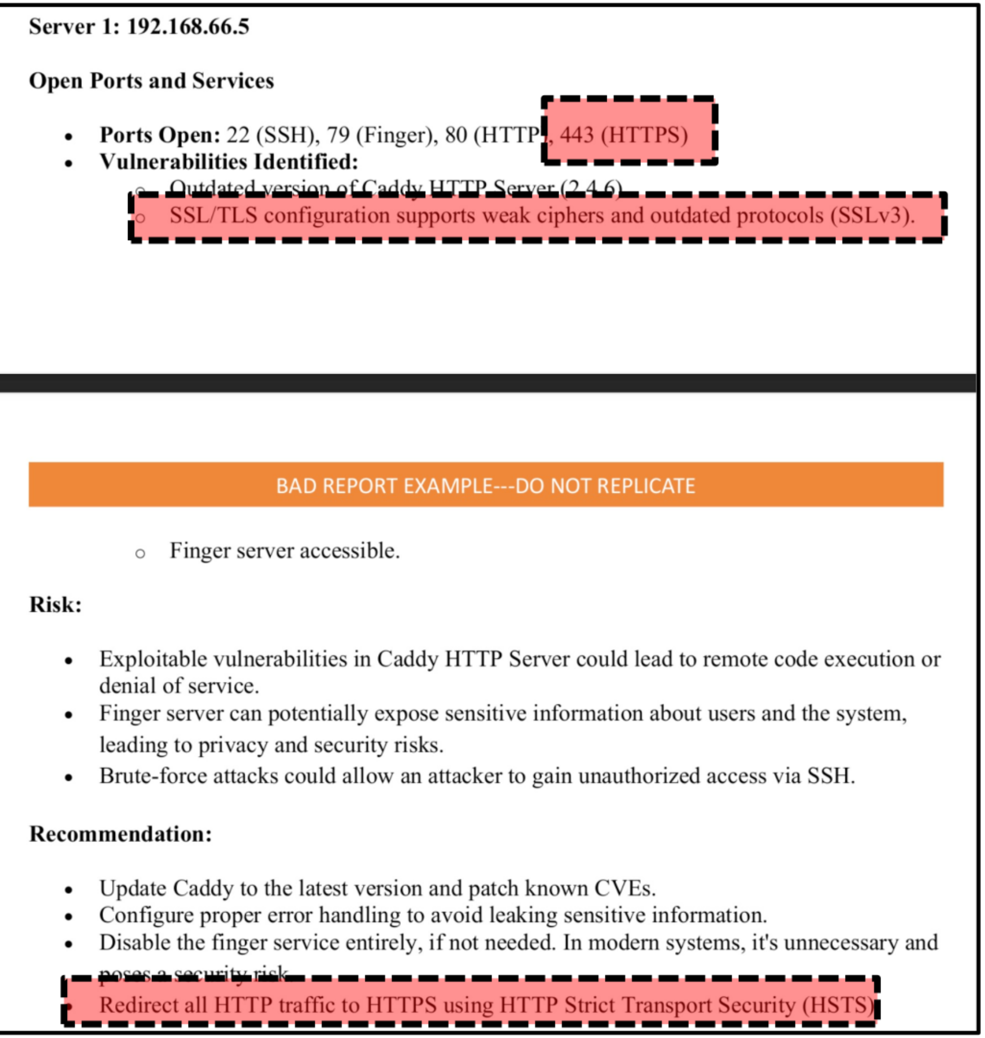
1.2 Objectives

By messaging ChatGPT, you agree to our Terms and have read our Privacy Policy. Don't share sensitive info. Chats may be reviewed and used to train our models. Learn more

- Provide actionable recommendations to improve security posture

ChatGPT can make mistakes. Check important info.

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP, 443 (HTTPS)
- **Vulnerabilities Identified:**
  - Outdated version of Caddy HTTP Server (2.4.6)
  - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

  - Finger server accessible.

Risk:

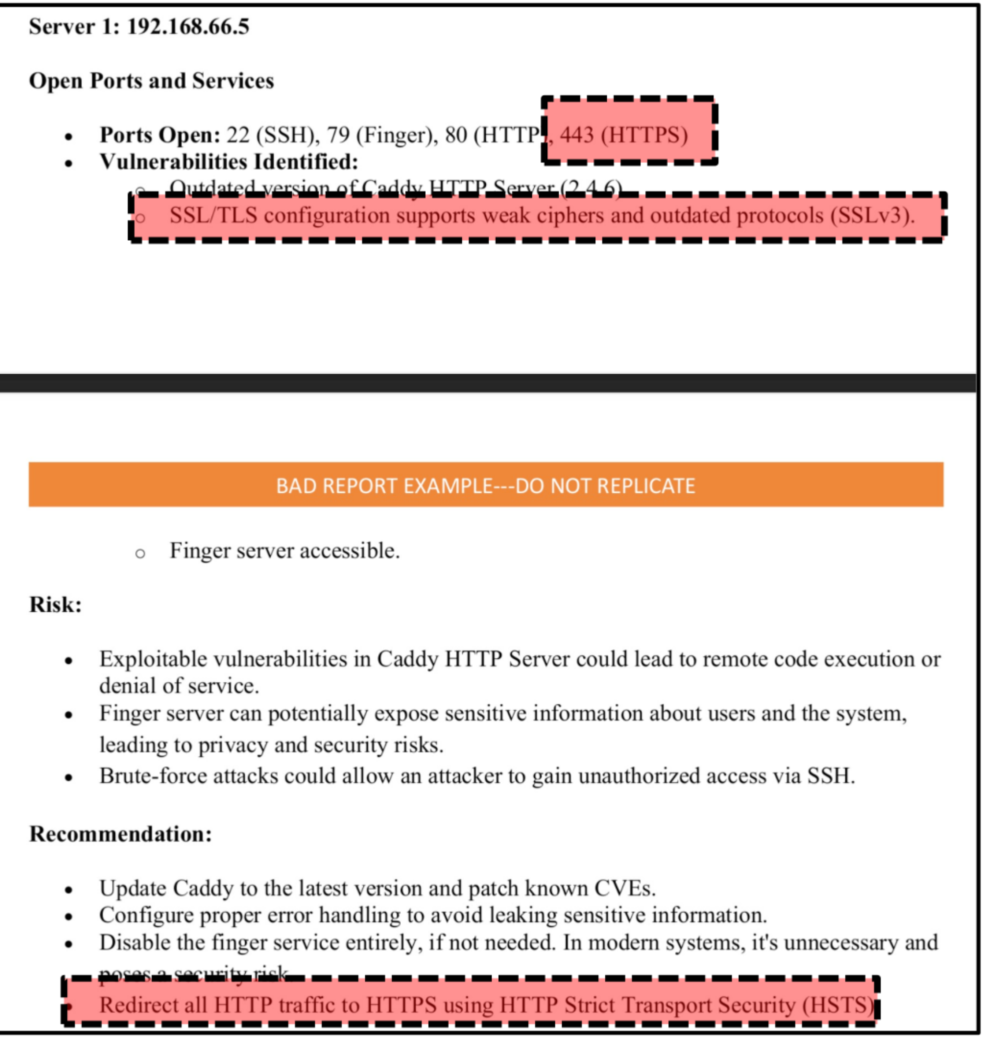
- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS)

- CLAIM: HTTPS is misconfigured

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
  - Outdated version of Caddy HTTP Server (2.4.6)
  - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

  - Finger server accessible.

Risk:

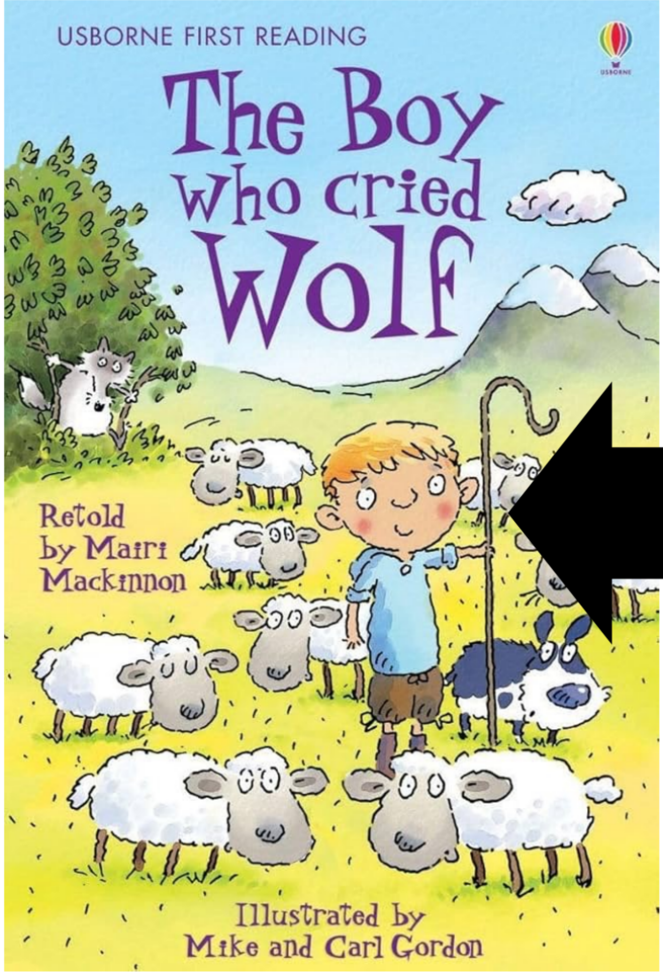
- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS)

- CLAIM: HTTPS is misconfigured

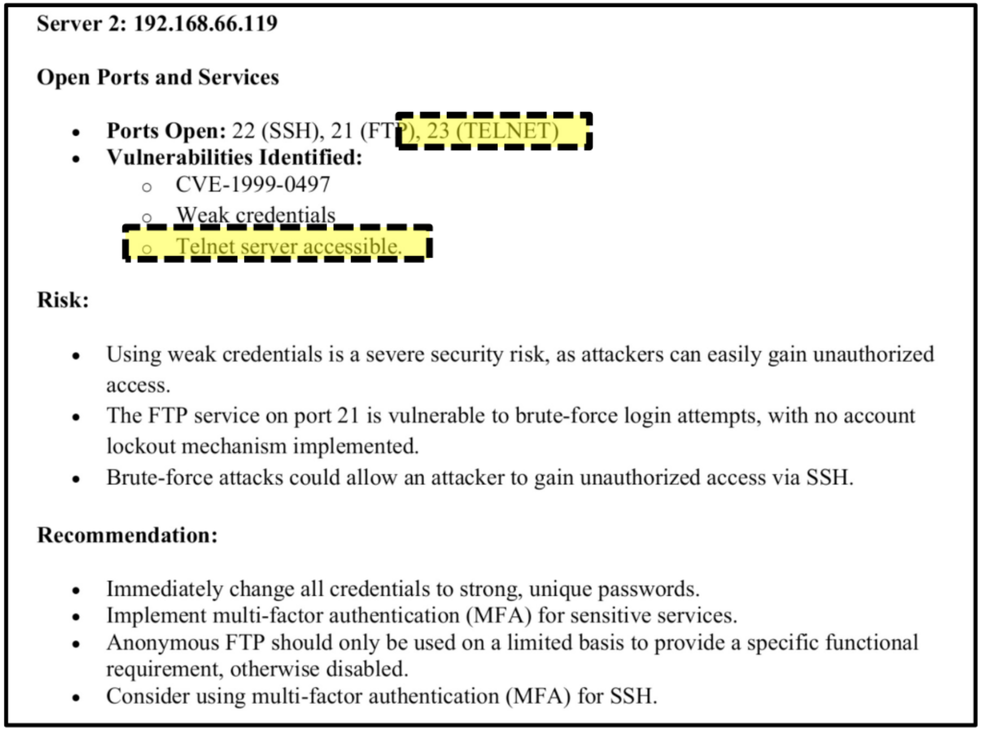
THERE IS NO HTTPS CONFIGURED


USBORNE FIRST READING
USBORNE
The Boy who cried Wolf
Retold by Mairi Mackinnon
Illustrated by Mike and Carl Gordon

Don’t be this guy

BAD REPORT EXAMPLE---DO NOT REPLICATE

- CLAIM: TELNET bad



Server 2: 192.168.66.119

Open Ports and Services

- **Ports Open:** 22 (SSH), 21 (FTP), 23 (TELNET)
- **Vulnerabilities Identified:**
  - CVE-1999-0497
  - Weak credentials
  - Telnet server accessible.

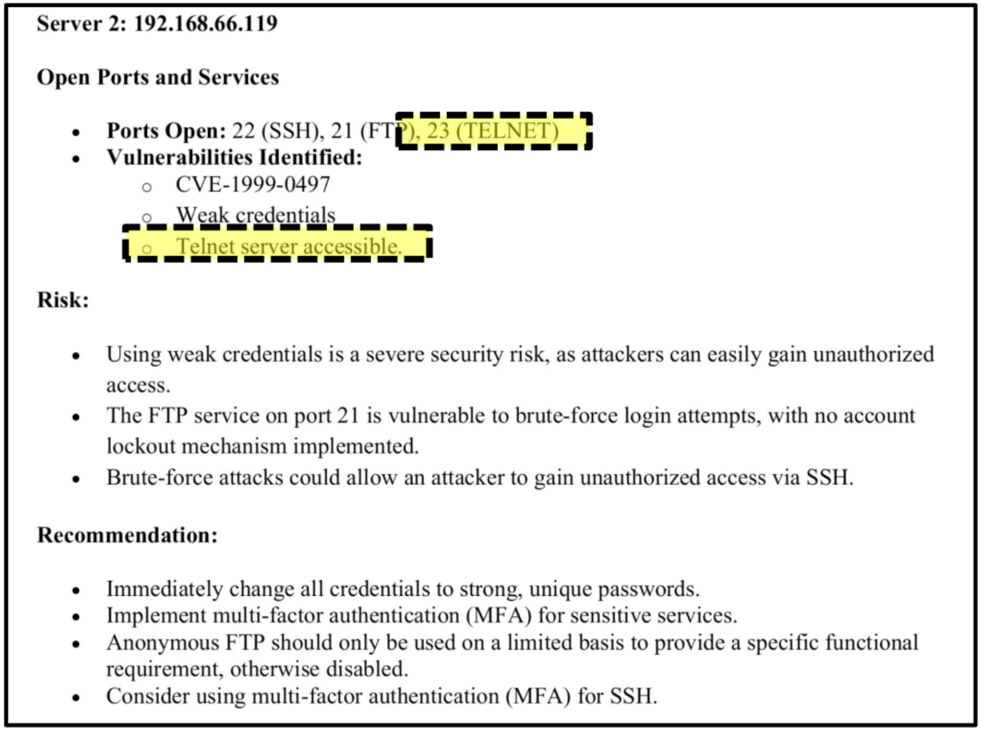
Risk:

- Using weak credentials is a severe security risk, as attackers can easily gain unauthorized access.
- The FTP service on port 21 is vulnerable to brute-force login attempts, with no account lockout mechanism implemented.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Immediately change all credentials to strong, unique passwords.
- Implement multi-factor authentication (MFA) for sensitive services.
- Anonymous FTP should only be used on a limited basis to provide a specific functional requirement, otherwise disabled.
- Consider using multi-factor authentication (MFA) for SSH.

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 2: 192.168.66.119

Open Ports and Services

- **Ports Open:** 22 (SSH), 21 (FTP), 23 (TELNET)
- **Vulnerabilities Identified:**
  - CVE-1999-0497
  - Weak credentials
  - Telnet server accessible.

Risk:

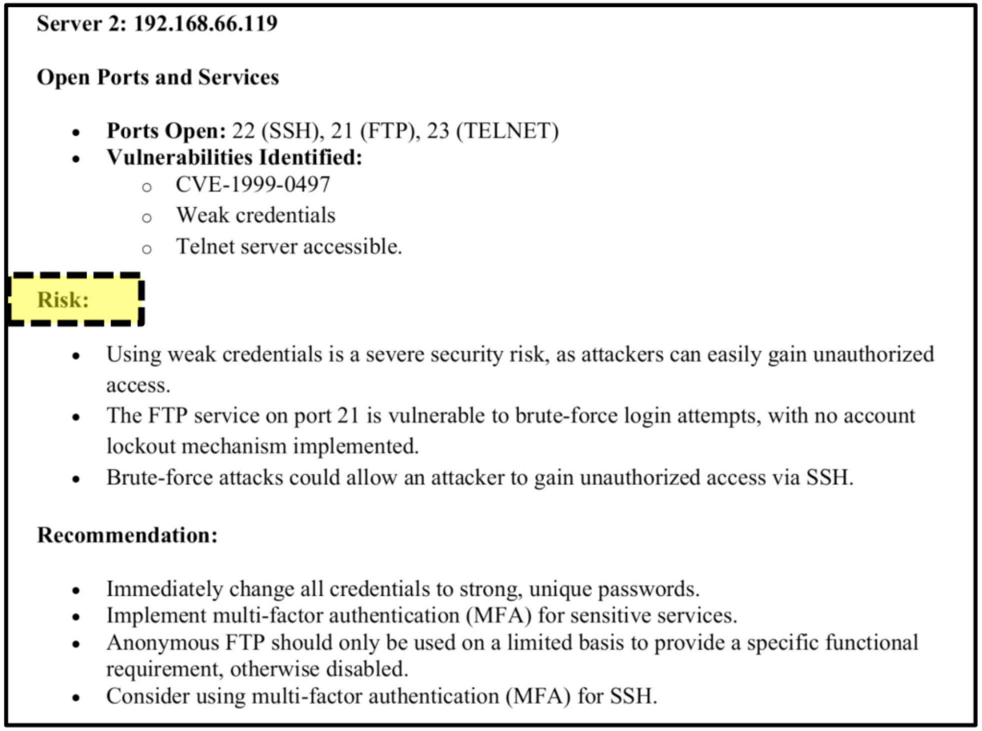
- Using weak credentials is a severe security risk, as attackers can easily gain unauthorized access.
- The FTP service on port 21 is vulnerable to brute-force login attempts, with no account lockout mechanism implemented.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Immediately change all credentials to strong, unique passwords.
- Implement multi-factor authentication (MFA) for sensitive services.
- Anonymous FTP should only be used on a limited basis to provide a specific functional requirement, otherwise disabled.
- Consider using multi-factor authentication (MFA) for SSH.

- CLAIM: TELNET bad
  - … that's it …

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 2: 192.168.66.119

Open Ports and Services

- **Ports Open:** 22 (SSH), 21 (FTP), 23 (TELNET)
- **Vulnerabilities Identified:**
    - CVE-1999-0497
    - Weak credentials
    - Telnet server accessible.

Risk:

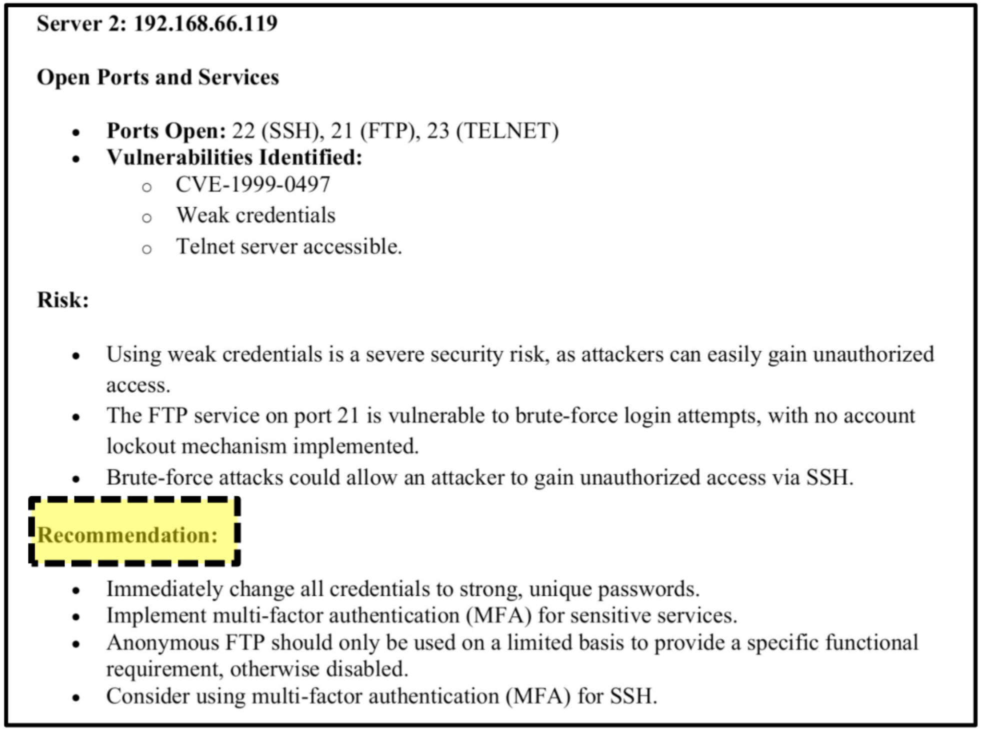
- Using weak credentials is a severe security risk, as attackers can easily gain unauthorized access.
- The FTP service on port 21 is vulnerable to brute-force login attempts, with no account lockout mechanism implemented.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Immediately change all credentials to strong, unique passwords.
- Implement multi-factor authentication (MFA) for sensitive services.
- Anonymous FTP should only be used on a limited basis to provide a specific functional requirement, otherwise disabled.
- Consider using multi-factor authentication (MFA) for SSH.

- CLAIM: TELNET bad
    - … that’s it …
    - No explanation

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 2: 192.168.66.119

Open Ports and Services

- **Ports Open:** 22 (SSH), 21 (FTP), 23 (TELNET)
- **Vulnerabilities Identified:**
  - CVE-1999-0497
  - Weak credentials
  - Telnet server accessible.

Risk:

- Using weak credentials is a severe security risk, as attackers can easily gain unauthorized access.
- The FTP service on port 21 is vulnerable to brute-force login attempts, with no account lockout mechanism implemented.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

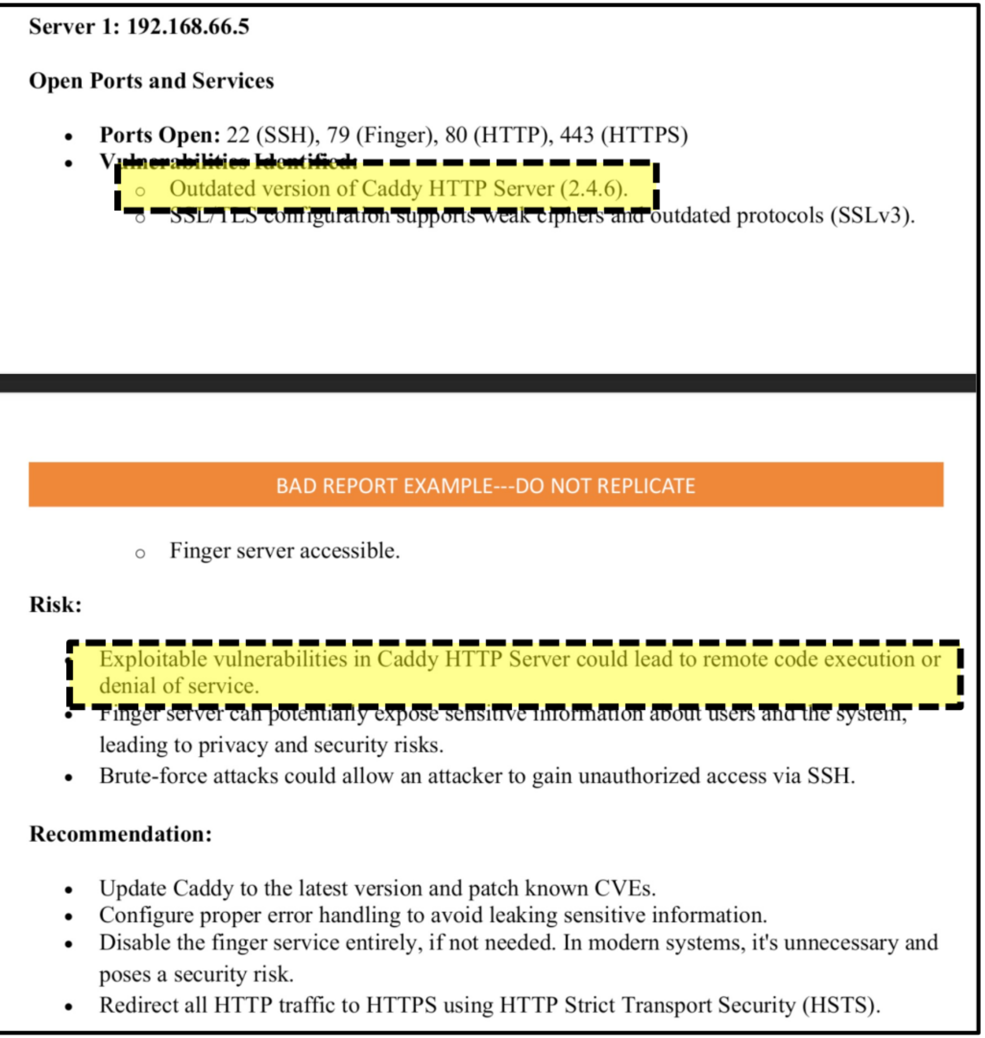
Recommendation:

- Immediately change all credentials to strong, unique passwords.
- Implement multi-factor authentication (MFA) for sensitive services.
- Anonymous FTP should only be used on a limited basis to provide a specific functional requirement, otherwise disabled.
- Consider using multi-factor authentication (MFA) for SSH.

- CLAIM: TELNET bad
  - … that’s it …
  - No explanation
  - No mitigations

I don't want to play with you anymore

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

    - Finger server accessible.

Risk:

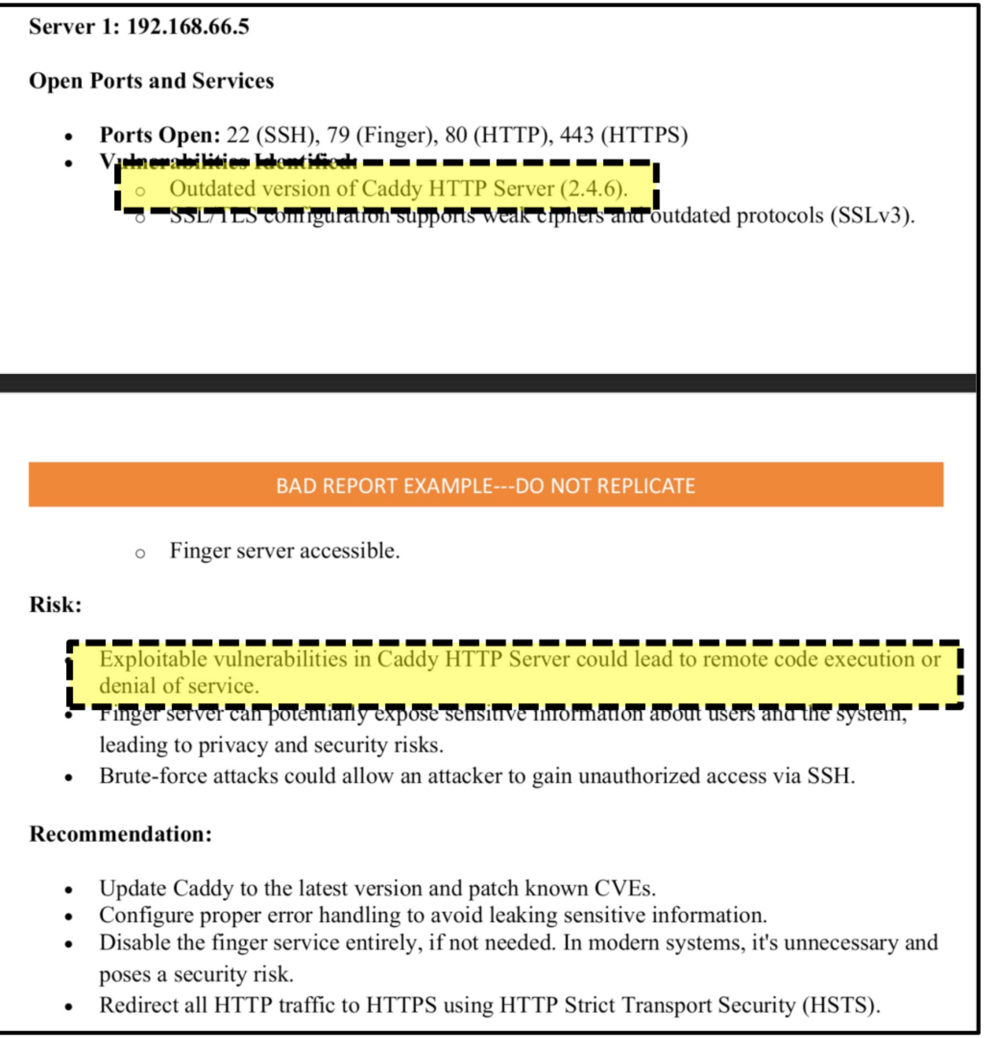
- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

- CLAIM: Vulns in Caddy web server

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

- Finger server accessible.

Risk:

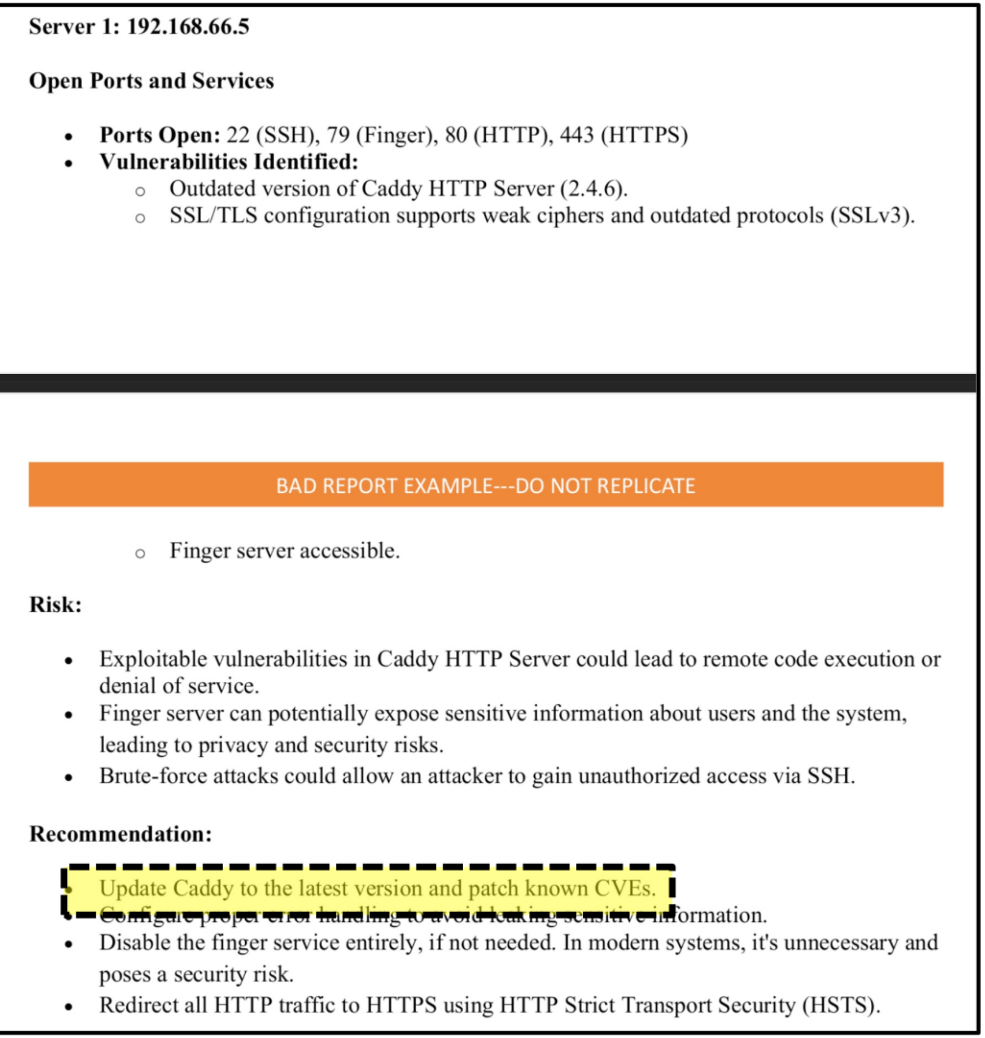
- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

- CLAIM: Vulns in Caddy web server
    - What vulns? What's wrong? How hard to exploit? How easy to patch?

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

-
    - Finger server accessible.

Risk:

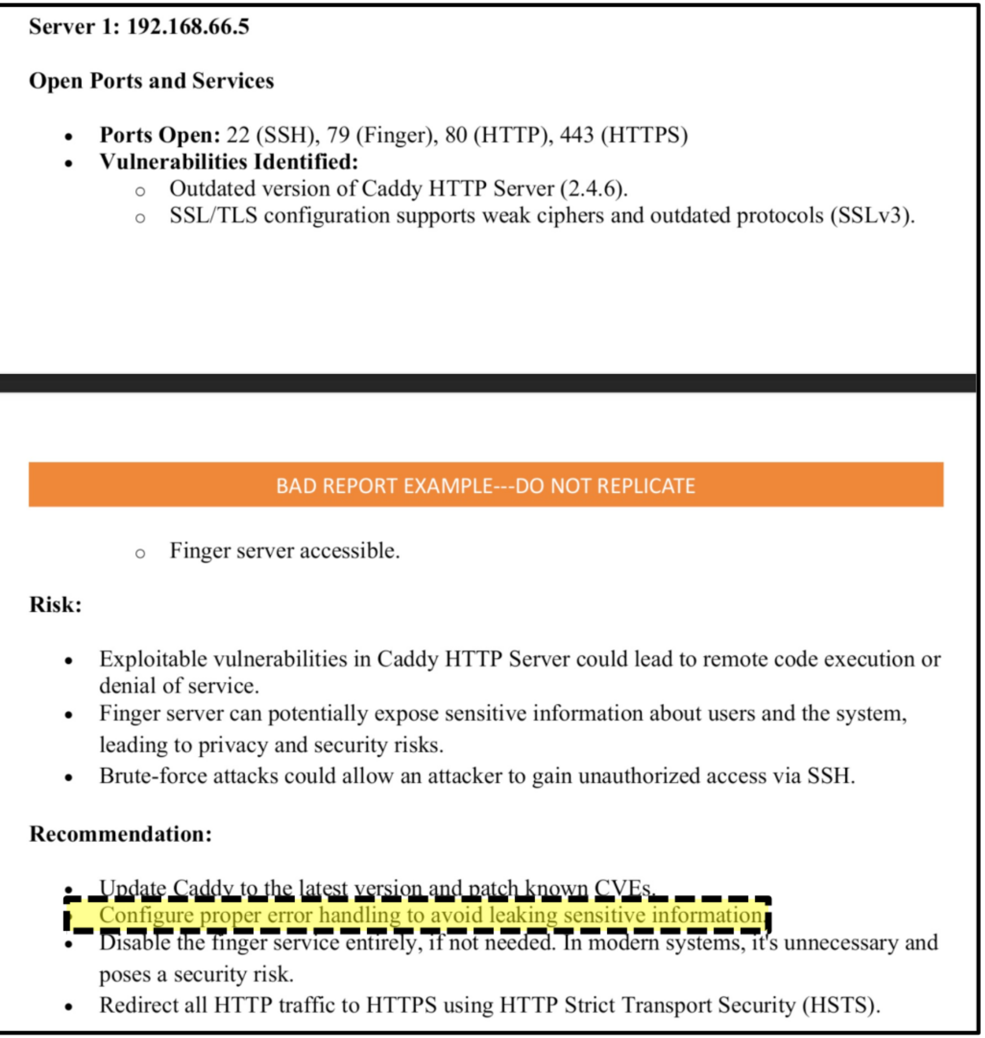
- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

- CLAIM: Vulns in Caddy web server
    - What vulns? What's wrong? How hard to exploit? How easy to patch?
    - What CVEs?

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

- Finger server accessible.

Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

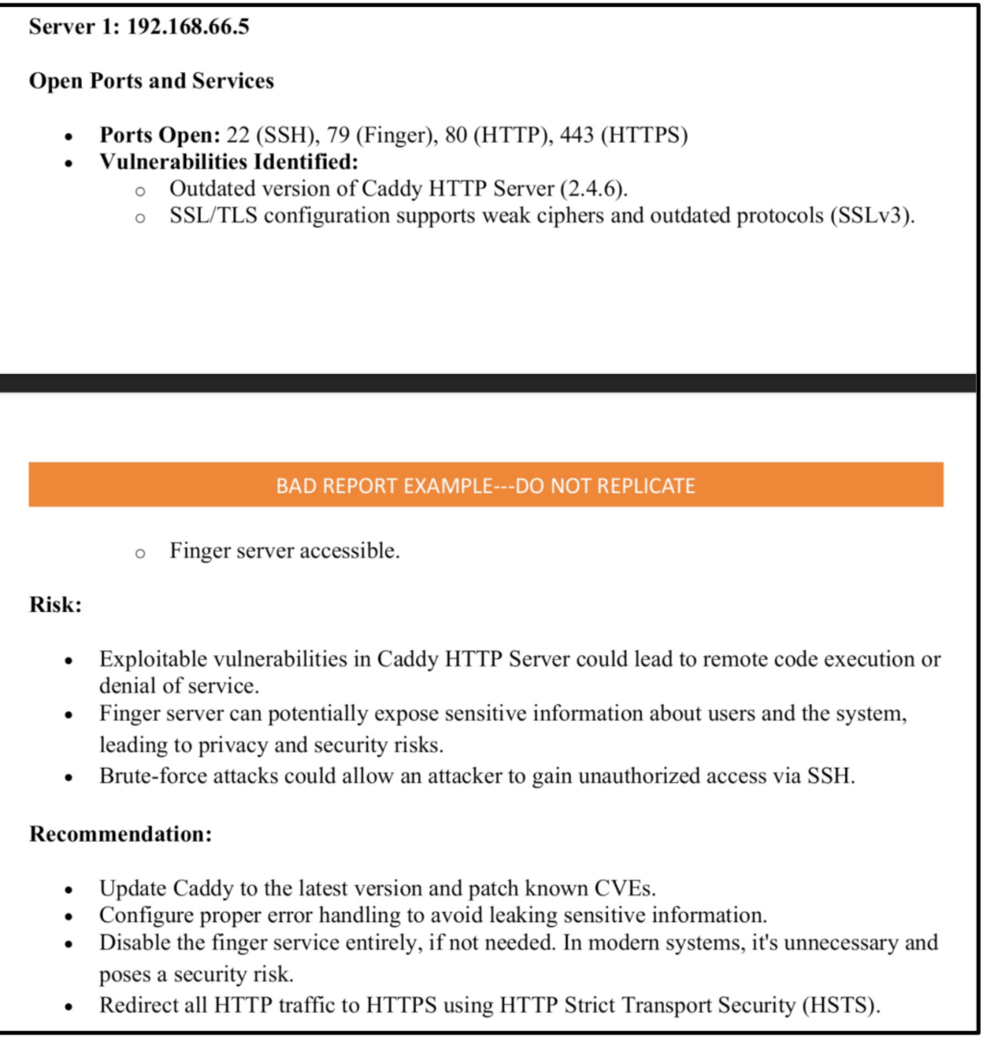
- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

- CLAIM: Vulns in Caddy web server
    - What vulns? What’s wrong? How hard to exploit? How easy to patch?
    - What CVEs?
    - What error handling?

HAVE YOU SEEN ME?
LAST SEEN WITH:

HAVE YOU SEEN ME?
LAST SEEN WITH:
CAR GONE! CAR GONE!

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
  - Outdated version of Caddy HTTP Server (2.4.6).
  - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

  - Finger server accessible.

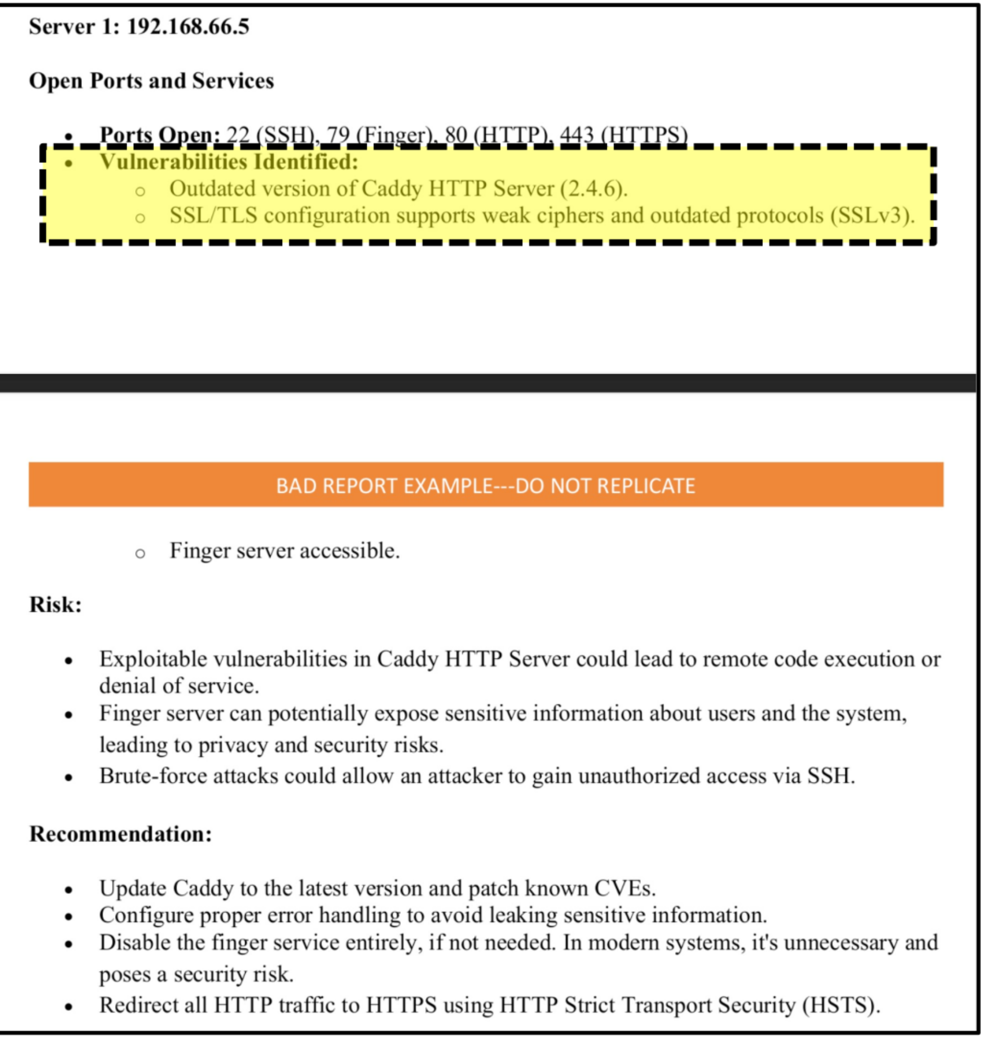
Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
  - Outdated version of Caddy HTTP Server (2.4.6).
  - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

  - Finger server accessible.

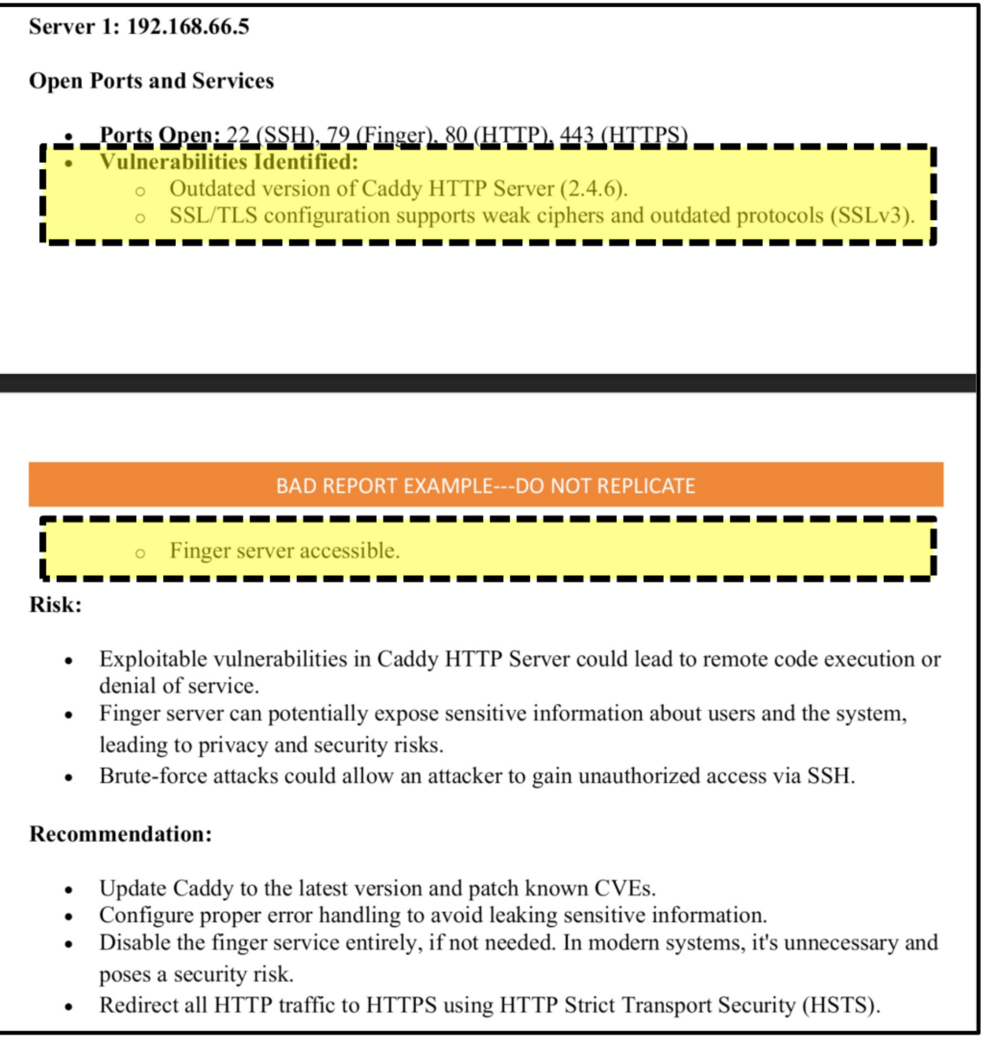
Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
  - Outdated version of Caddy HTTP Server (2.4.6).
  - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

  - Finger server accessible.

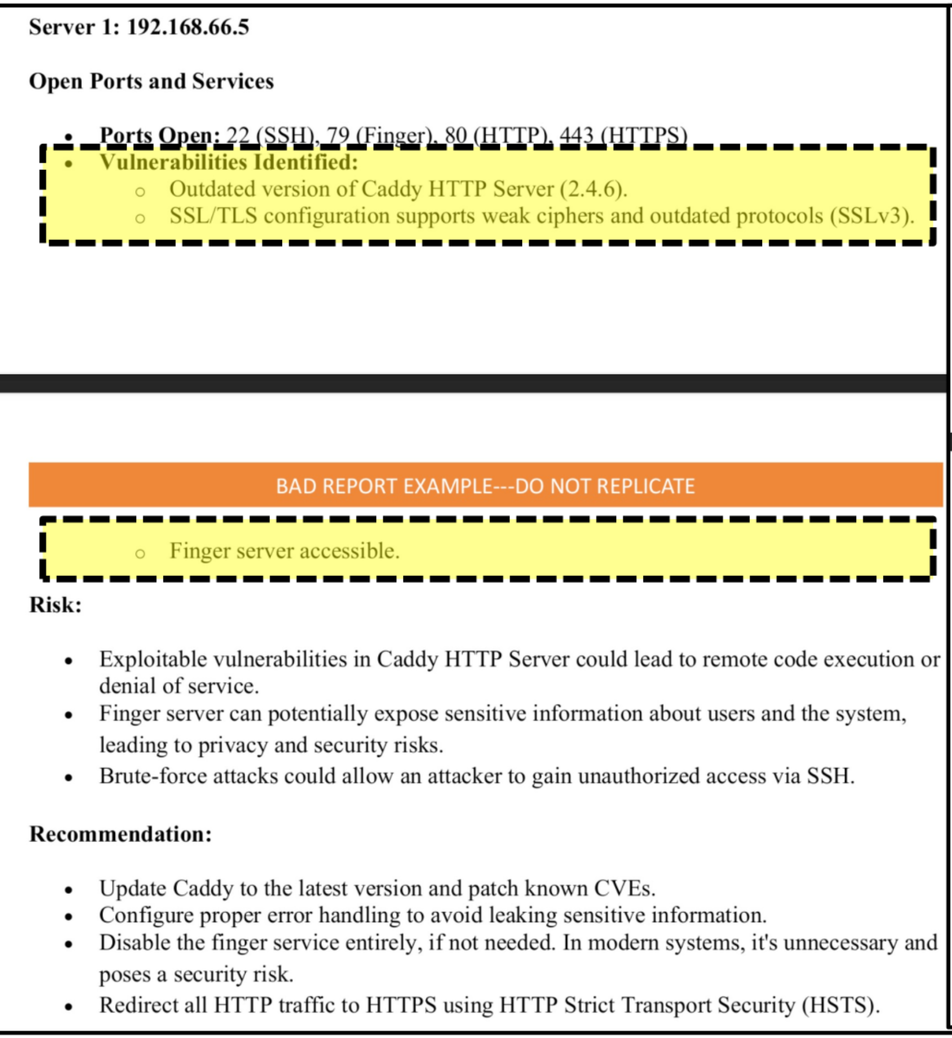
Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

BAD REPORT EXAMPLE---DO NOT REPLICATE



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).

BAD REPORT EXAMPLE---DO NOT REPLICATE

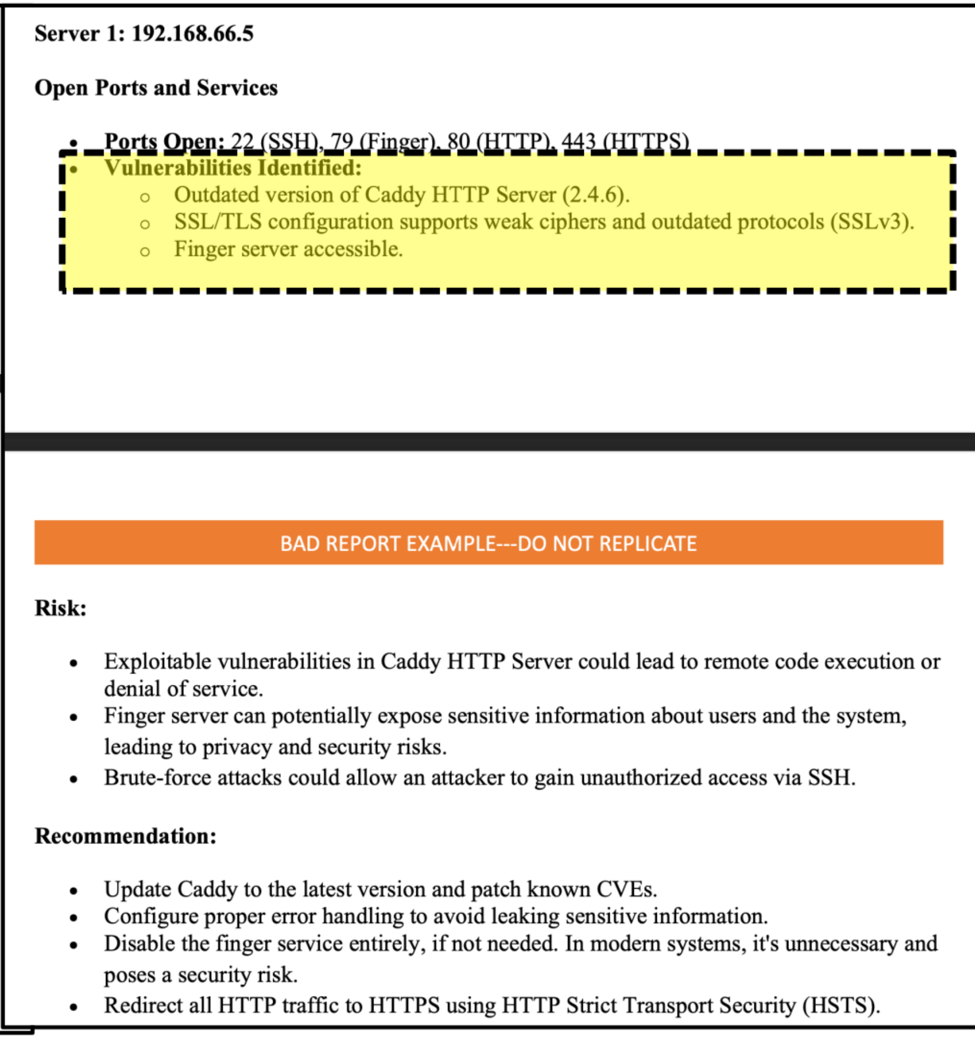
- Finger server accessible.

Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).



Server 1: 192.168.66.5

Open Ports and Services

- **Ports Open:** 22 (SSH), 79 (Finger), 80 (HTTP), 443 (HTTPS)
- **Vulnerabilities Identified:**
    - Outdated version of Caddy HTTP Server (2.4.6).
    - SSL/TLS configuration supports weak ciphers and outdated protocols (SSLv3).
    - Finger server accessible.

BAD REPORT EXAMPLE---DO NOT REPLICATE

Risk:

- Exploitable vulnerabilities in Caddy HTTP Server could lead to remote code execution or denial of service.
- Finger server can potentially expose sensitive information about users and the system, leading to privacy and security risks.
- Brute-force attacks could allow an attacker to gain unauthorized access via SSH.

Recommendation:

- Update Caddy to the latest version and patch known CVEs.
- Configure proper error handling to avoid leaking sensitive information.
- Disable the finger service entirely, if not needed. In modern systems, it's unnecessary and poses a security risk.
- Redirect all HTTP traffic to HTTPS using HTTP Strict Transport Security (HSTS).

Threats and Countermeasures

Lecture 08:
Privilege Escalation

COMP-5830/-6830
Spring 2025