EXTERNAL NETWORK VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

Prepared for: XYZ
v1.0
September | 30 | 2022

CONTENTS

DOCUMENT DETAILS

DOCUMENT CONTROL	
Document Title	External Network Penetration Testing Report
Document Classification	Final Report
Last Edit Date	30-Sept-202X

DOCUMENT HISTORY			
DATE	VERSION	PREPARED BY	STATUS
30/09/2022	1.0		Final Report

CUSTOMER INFORMATION			
Company Name			
Address			
Website			
Contact Name			
Title			
Telephone			
Email			

CONSULTANT INFORMATION		
Name	Role	Responsibility
	Sr. Security Consultant	Document Preparation
	Sr. Security Consultant	Document Preparation
	Lead Consultant	Document Review
	Technical Manager	Document Approval
	CTO	Document Final Approval

INTRODUCTION

CyberPWN Technologies conducted **external network penetration test** for [CLIENT] which was initiated on [DATE] and concluded on [Date], based upon the Authorization to Test document provided by the Company. Cyberpwn followed a testing methodology that sought to identify vulnerabilities and, through manual pentesting determine the impact to the Company's assets. Cyberpwn assigned a risk level based on goals achieved during testing.

SCOPE & DURATION

The scope includes network vulnerability assessment and penetration testing for below mentioned targets.

IP ADDRESSES	Priority	Notes
Blank	P1	Blank
Blank	P2	Blank
Blank	P3	Blank

The test was performed from [] to [] including reporting.

LIMITATIONS & CONSTRAINTS

Testing occurred under the following constraints:

- Intentional attacks that could cause outages, such as denial of service attacks, were not performed.
- The Company should investigate any downtime experienced during testing as it may indicate a lack of service or organizational resiliency.
- Hosts that are not defined within the scope of the engagement were excluded from testing.

EXECUTIVE SUMMARY

CyberPWN was engaged by Client to conduct external penetration testing of client's external interface facing system. The security assessment covered 1xx external IP address that was conducted during the period [] to [] from the CyberPWN offshore promise at

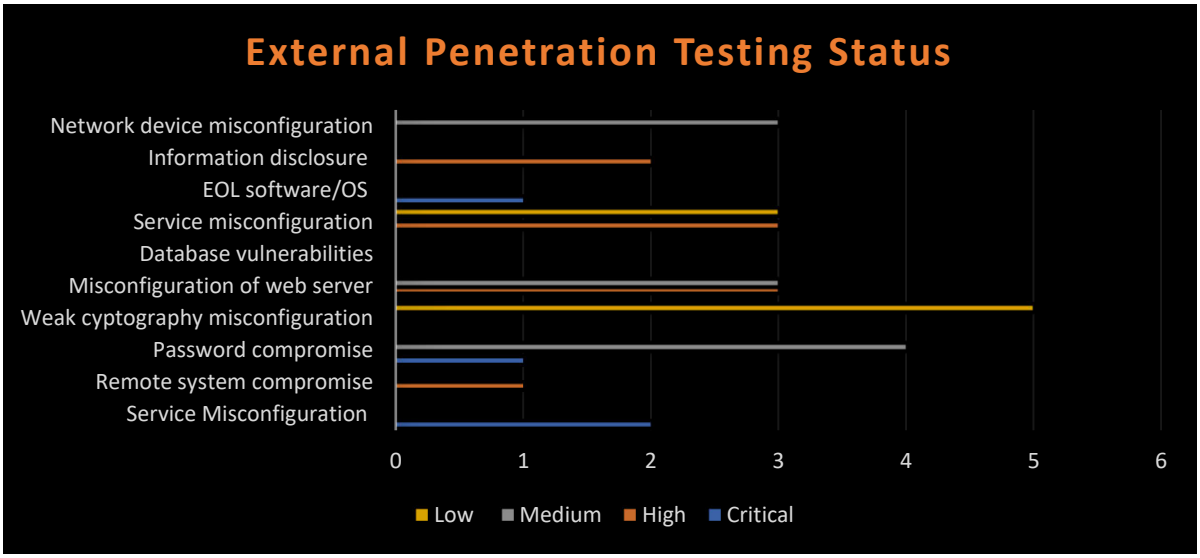
However, the assessment identified 05 critical, 03 high, 07 Medium and 10 Low risks finding as an outcome of external penetration testing was performed internet facing system which were selected based on the operational criticality and the type of active network service.

- The 05 critical rated risk is pertaining to exploitation vulnerabilities name here.
- The 03 High rated risk is pertaining to exploitation vulnerabilities name here.
- The 07 Medium rated risk is pertaining to exploitation vulnerabilities name here.
- The 10 Low rated risk is pertaining to exploitation vulnerabilities name here.

Summary of Finding

Total Vulnerabilities					
Critical	High	Medium	Low	Info	Total
5	3	7	10	0	25

Finding Categorization



Introduction to Network Penetration Testing

Network vulnerability assessment and penetration testing is a comprehensive cybersecurity process that aims to identify, assess, and address vulnerabilities within the infrastructure to identify potential vulnerabilities and weaknesses that could be exploited by malicious attackers.

Vulnerability Scoring

A scoring system is used to grade all of the vulnerabilities listed in this report. Cyberpwn employs the industry-standard CVSSv4. It provides a system for determining the severity of vulnerabilities, regardless of the software/hardware platform or service function.

Every vulnerability is assigned a score between 0 and 10, giving each discovered vulnerability a score that aids in identifying the most vulnerable systems and prioritizing responses to each problem. The National Vulnerabilities Database (NVD) uses the CVSS system to calculate scores for almost all known vulnerabilities, and these are the scores referred to in this report.

Further information can be found at https://www.first.org/cvss/calculator/4.0.

https://nvd.nist.gov/

Severity Rating

Based on the severity of the vulnerability, they are assigned below ratings:

CVSS Severity Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
Informational	0.0

Risk Rating Definitions

Severity Rating	Definitions
Critical	Critical severity vulnerabilities usually have most of the following traits: • A successful attack may lead to complete compromise of the system • Exploitation can be done remotely over an untrusted connection – such as the Internet • Exploiting the vulnerability is very easy or straightforward. It may not require privilege accounts or user interaction. • It has a very significant impact on confidentiality, integrity and/or availability of the targeted system
High	High severity vulnerabilities demonstrate some of the following characteristics: • It is not straight-forward to exploit and may require some user interaction and has minimum dependency. • Usually gives an attacker elevated privilege. • It has a significant impact on confidentiality, integrity and availability
Medium	• Vulnerabilities scored medium generally: • Require specific user privileges or conditions to execute the attack. • Grant attacker access to non-critical privileged functionality/data. • Moderately affects Confidentiality, Integrity or availability .
Low	Vulnerabilities scored low usually exhibit some of the following characteristics: • They have little impact on the confidentiality, integrity or availability of the organization's data or assets. • Requires a great amount of computational power to exploit the vulnerability. • Require excessive privileges or access to execute an attack • Exploits are not known publicly

APPROACH AND METHODOLOGY

Cyberpwn Technologies penetration testing methodology is based upon frameworks and standards mentioned below and it contains the following phases:

The Penetration Testing Execution Standard (pentest-standard.org)
External Network Penetration Testing Methodology – Product Docs | Cobalt
National Institute of Standards and Technology (NIST)
OSSTMM (Open Source Security Testing Methodology Manual)

PLANNING

- Cyberpwn Technologies prepares for initial planning sessions with the Company by reviewing the Company's business processes, key personnel, physical locations and Internet-accessible footprint.
- Cyberpwn Technologies and the Company collaborate to create the rules, attack scenarios, and goals for testing.
- The Company may provide additional documentation and access to applications, systems and networks to facilitate targeted testing.
- The Customer Company is responsible for ensuring that the scope contains all targets for testing and that the Company has the authority to permit Cyberpwn Technologies to perform penetration testing against the identified targets.

DISCOVERY

- The discovery phase of penetration testing includes two parts. The first part is the start of actual testing, and covers information gathering and scanning. Network port and service identification is conducted to identify potential targets. In addition to port and service identification, other techniques are used to gather information on the targeted network:
- Host name and IP address information can be gathered through many methods, including DNS interrogation, InterNIC (WHOIS) queries, and network sniffing (generally only during internal tests).
- System information, such as names and shares can be found through methods such as NetBIOS enumeration (generally only during internal tests) and Network Information System (NIS) (generally only during internal tests).
- Application and service information, such as version numbers, can be recorded through banner grabbing.

AUTOMATED SCANNING

Vulnerability scans are conducted via automated vulnerability scanning tools to identify potential risk exposures and attack vectors across an organization's networks, hardware, software, and systems.

VULNERABILITY ANALYSIS

- Provides an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to threats to its environment.
- Defining and classifying network or System resources.
- Assigning Risk priority to the resources(Ex: – High, Medium, Low)
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most prioritized problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

EXPLOITATION

After interpreting the results from the vulnerability assessment, our expert penetration testers will use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities. Automation and machine learning can't do what an expert pen tester can. An expert penetration tester is able to exploit vulnerabilities that automation could easily miss.

REPORTING

Cyberpwn Technologies regularly communicates on the progress and results of testing during the engagement. Cyberpwn Technologies immediately notifies the Company if a critical-risk finding is discovered so that the Company can quickly remediate the issue.

Cyberpwn Technologies creates a report that contains, at minimum, the following items:

- **Executive Summary** - provides a high-level overview of the testing results and is intended to be read by executives, customers, and business partners.
- **Findings** - describes each exploitable vulnerability. The findings results are intended to be distributed
- to technical teams
- **Recommendations** - recommendations on how to resolve each identified issue
- **Risk Ranking** - each issue identified is assigned a risk ranking that is derived from the Common Vulnerability Scoring System (CVSS). The rating is based on the specific instances identified in the company environment.
- **Steps to Reproduce** - additional details that provide enough information such that the issue can be replicated by technical teams
- **Rescan** - updates about the finding, such as retesting status or management responses and revalidation report.

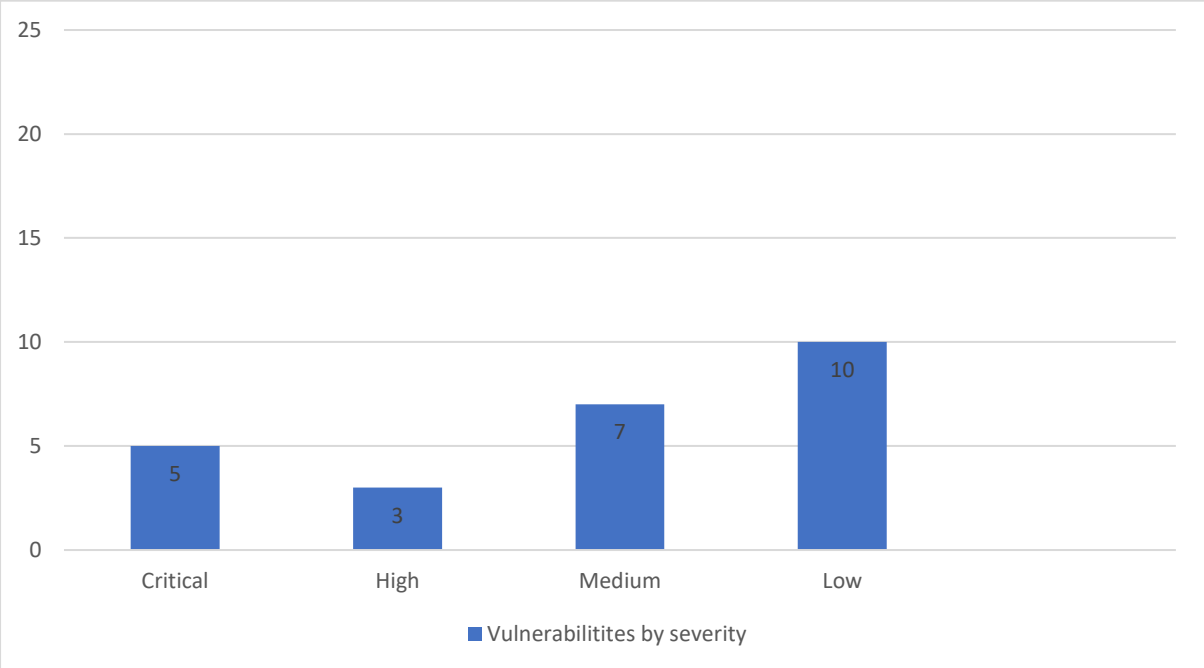
RESULT OVERVIEW

Cyberpwn Technologies Security team discovered 25 risks and potential vulnerabilities in customer's network.

The below table summarizes the list of vulnerabilities with corresponding risk ratings.

SL. No.	Vulnerability Name	Severity Rating
1.	DistCC Daemon Command Execution	Critical
2.	Misconfigured "r" Services Vulnerability	Critical
3.	Apache Struts REST Plugin with Dynamic Method Invocation Remote Code Execution	High
4.	Multiple SSL Vulnerabilities	Medium
5.	Multiple Apache Vulnerabilities	Medium
6.	Multiple OpenSSL Vulnerabilities	Medium
7.	SNMP Agent Default Community Name	Medium
8.	Server Version Disclosure	Low
9.	Default Web Server Page Disclosure	Low

GRAPHICAL PRESENTATION



HIGH LEVEL RECOMMENDATIONS

The following recommendations offer guidance on enhancing the security posture of XYZ networks and business-critical assets:

1. Conduct Windows workstation hardening to disable LLMNR and NBT-NS protocols and require SMB signing across the network.
2. Disable the SNMP service on the remote host if it is not in use.
3. Enforce message signing in the host's configuration.
4. Apply necessary Windows patches.
5. Disable unused services.

VULNERABILITIES DETAILS

1. DistCC Daemon Command Execution		
Description	distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.	
Severity	Critical	
CVSS Score	9.3	
Instances	**Host**	**Port**
	XX.XX.2.3	3632(TCP)
	XX.XX.2.25	3632(TCP)
	XX.XX.2.56	3632(TCP)
	XX.XX.2.158	3632(TCP)
Impact	There is a complete loss of system protection, resulting in the entire system being compromised. The attacker can render the resource completely unavailable.	
Remediation	Restrict access to the distccd service on TCP port 3632, or remove this service entirely from the host.	
CVSS String	Kept Blank Intentionally	
Reference	https://cvedetails.com/cve/CVE-2004-2687/ http://distcc.samba.org/security.html	
Proof of Concept		

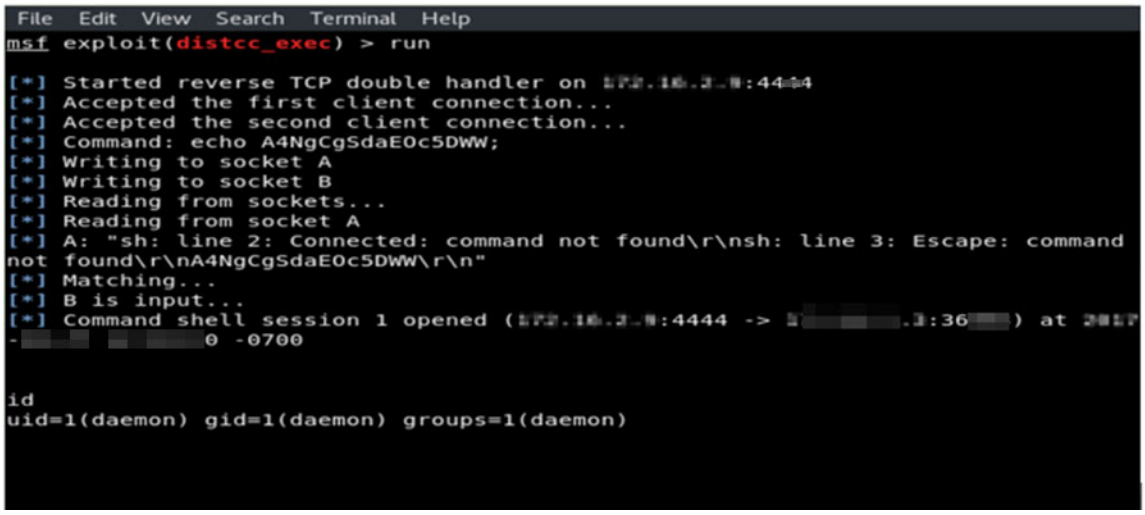


FIGURE 1: DISTCC DAEMON COMMAND EXECUTION

2.Misconfigured “r” Services Vulnerability		
Description	TCP ports 512, 513, and 514 are known as "r" services, and have been misconfigured to allow remote access from any host (a standard ".rhosts + +" situation). An attacker can easily log as root via these services, completely compromising the target host.	
Severity	Critical	
CVSS Score	9.3	
Instances	**Host**	**Port**
	XX.XX.2.3	512, 513, 514(TCP)
Impact	There is a complete loss of system protection, resulting in the entire system being compromised. The attacker can render the resource completely unavailable.	
Remediation	Consider the benefits of removing these services from the host. If they are necessary for business functions, then edit the .rhosts file to prevent remote access from any host.	
CVSS String	Kept Blank Intentionally	
Reference	https://docs.oracle.com/cd/E19455-01/805-7229/remotehowtoaccess-3/index.html	
Proof of Concept		

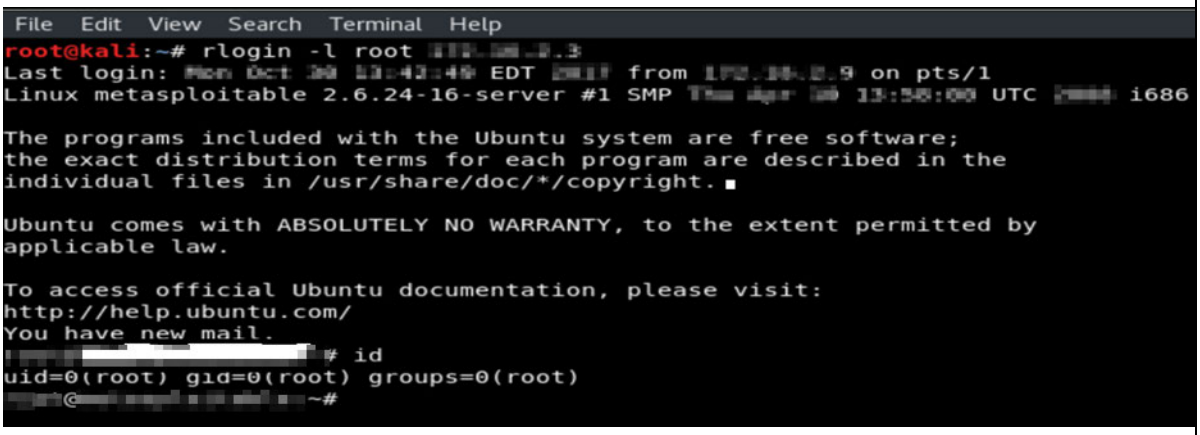


FIGURE 2: RLOGIN UTILITY TO GAIN ACCESS TO THE HOST WITH ROOT PRIVILEGES

3. Apache Struts REST Plugin with Dynamic Method Invocation Remote Code Execution		
Description	Apache Struts 2.3.20.x before 2.3.20.3, 2.3.24.x before 2.3.24.3, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via vectors related to an ! (exclamation mark) operator to the REST Plugin.	
Severity	High	
CVSS Score	7.5	
Instances	**Host**	**Port**
	XX.XX.2.8	8282(TCP)
Impact	There is a complete loss of system protection, resulting in the entire system being compromised. An unauthenticated, remote attacker can exploit this, via a crafted expression, to execute arbitrary code. (CVE-2016-3081, CVE-2016-3082 and CVE-2016-3087)	
Remediation	Upgrade to Apache Struts version 2.3.28.1 or later. Alternatively, apply the workarounds referenced in the vendor advisories.	
CVSS String	Kept Blank Intentionally	
Reference	https://www.cvedetails.com/cve/CVE-2016-3087/ https://cwiki.apache.org/confluence/display/WW/S2-033 http://www.securityfocus.com/bid/90960	

Proof of Concept

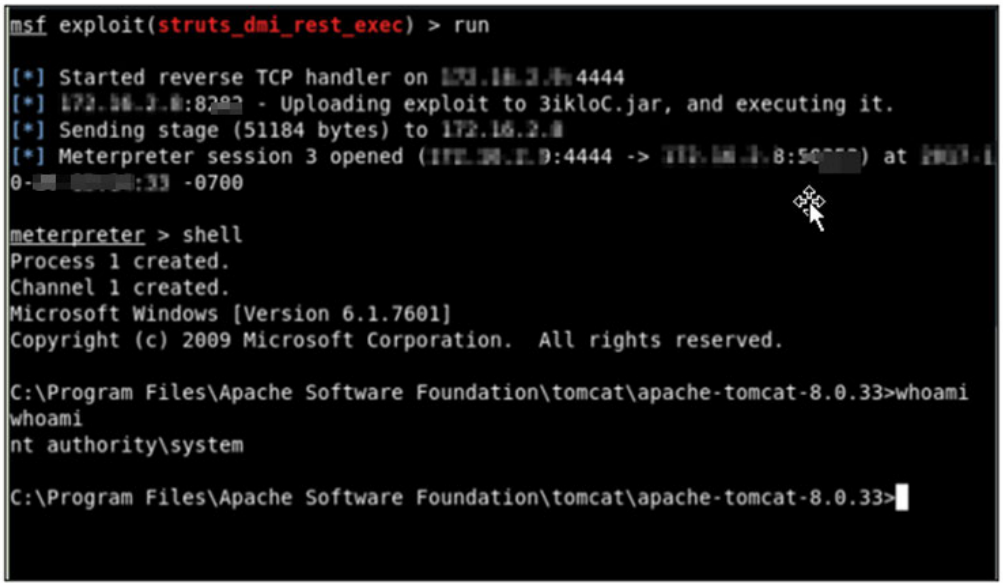


FIGURE 3: RLOGIN UTILITY TO GAIN ACCESS TO THE HOST WITH ROOT PRIVILEGES

4. Multiple SSL Vulnerabilities		
Description	During assessment it was observed that the host is vulnerable to multiple SSL attacks.	
Severity	Medium	
CVSS Score	4.9	
Instances	**Host**	**Port**
	XX.XX.12.66	8443 (TCP)
	XX.XX.12.66	10443 (TCP)
Impact	• **SSL Self-Signed Certificate / SSL Certificate Cannot Be Trusted:** The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections • **Use of Weak Hashing SHA1 Algorithm** These hashing algorithms are known to be vulnerable to collision attacks and Weaknesses in these hashing algorithms can lead to situations in which attackers can create or obtain fraudulent certificates. • **Lucky 13** LUCKY13 is a timing attack can be used against implementations of the TLS protocol using the cipher block chaining mode of operation. The vulnerability affects the TLS 1.1 and 1.2 specification as well of certain forms of earlier versions. The attack allows a full plaintext recovery for OpenSSL.	
Remediation	• **SSL Self-Signed Certificate / SSL Certificate Cannot Be Trusted:** The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections. • **Use of Weak Hashing SHA1 Algorithm** It is recommended to use strong hashing algorithm like SHA 256 and SHA 512. • **Lucky 13** Disable compression and / or the SPDY service.	

CVSS String	Kept Blank Intentionally
Reference	https://www.openssl.org/news/secadv/20210824.txt

Proof of Concept

```
Common Name (CN)            FortiGate
subjectAltName (SAN)        missing (NOT ok) -- Browsers are complaining
Trust (hostname)            certificate does not match supplied URI
Chain of trust              NOT ok (self signed)
EV cert (experimental)      no
Certificate Validity (UTC)  3310 ⩾ 60 days (2020-10-02 08:11 ⟶ 2030-10-03 08:11)
                            ⩾ 10 years is way too long
ETS/"eTLS", visibility info not present
Certificate Revocation List --
OCSP URI                    --
                            NOT ok -- neither CRL nor OCSP URI provided
OCSP stapling               not offered
```

FIGURE 5: SSL CERTIFICATE CANNOT BE TRUSTED

```
  Server Signature Algorithm(s):
TLSv1.3  rsa_pss_rsae_sha256
TLSv1.3  rsa_pss_rsae_sha384
TLSv1.3  rsa_pss_rsae_sha512
TLSv1.2  rsa_pkcs1_sha1
TLSv1.2  rsa_pkcs1_sha224
TLSv1.2  rsa_pkcs1_sha256
TLSv1.2  rsa_pkcs1_sha384
TLSv1.2  rsa_pkcs1_sha512
TLSv1.2  rsa_pss_rsae_sha256
TLSv1.2  rsa_pss_rsae_sha384
TLSv1.2  rsa_pss_rsae_sha512

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  FortiGate
Issuer:   FortiGate
```

FIGURE 6: SHA1 ALGORITHM IN USE

5. Multiple Apache Vulnerabilities

Description	During assessment it was observed that the host is using the vulnerable version of apache.	
Severity	Medium	
CVSS Score	4.5	
Instances	**Host**	**Port**
	XX.XX.12.66	8443(TCP)
Impact	The version of Apache httpd installed on the remote host is prior to 2.4.46. Therefore, it is affected by multiple vulnerabilities: **CVE-2020-11984:** Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE. **CVE-2020-11993:** Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above info will mitigate this vulnerability for unpatched servers.	
Remediation	It is recommended to upgrade to Apache version 2.4.46 or later.	
CVSS String	Kept Blank Intentionally	
Reference	CVE-2020-1927 | Apache HTTP Server mod_rewrite redirect (vuldb.com)	

Proof of Concept

```
report for [redacted]
Host is up (0.10s latency).

PORT     STATE SERVICE  VERSION
8443/tcp open  ssl/http Apache httpd 2.4.41 ((Unix)) OpenSSL/1.1.1 mod_fastcgi/mod_fastcgi-SNAP-0910052141)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
```

FIGURE 7: APACHE 2.4.41 VULNERABLE VERSION IN USE

6. Multiple OpenSSL Vulnerabilities		
Description	During assessment it was observed that the host is using the vulnerable version of OpenSSL.	
Severity	Medium	
CVSS Score	4.5	
Instances	**Host**	**Port**
	XX.XX.12.66	8443
Impact	The version of OpenSSL installed on the remote host is prior to 1.1.1l. Therefore, it is affected by multiple vulnerability: **CVE-2021-3711 :** In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically, an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1.	
Remediation	It is recommended to upgrade to OpenSSL version 1.1.1l or later.	
CVSS String	Kept Blank Intentionally	
Reference	https://www.openssl.org/news/secadv/20210824.txt	
Proof of Concept Sample report		

FIGURE 8: VULNERABLE OPENSSL VERSION IN USE

7. SNMP Agent Default Community Name		
Description	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).	
Severity	Medium	
CVSS Score	4.5	
Instances	**Host**	**Port**
	Sample Report – Intentionally blank	161/udp
Impact	This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.	
Remediation	It is recommended to Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port or change the default community string.	
CVSS String	Kept Blank Intentionally	
Reference	Sample Report	
Proof of Concept Sample Report		

8. Server Version Disclosure

Description	During assessment it was observed that the host is Disclosing server version in http response.	
Severity	Low	
CVSS Score	3.5	
Instances	**Host**	**Port**
	XX.XX.2.3	8843
Impact	This version disclosure will expose information about the technology used in the system and attacker can look for specific security vulnerabilities for the version identified through its response. This information can help an attacker to gain a greater understanding of the system in use and potentially to develop further attacks.	
Remediation	It is recommended to • Reconfigure the application to remove any details about server version in the response headers.	
CVSS String	Kept Blank Intentionally	
Reference	http://projects.webappsec.org/Information-Leakage	

Proof of Concept

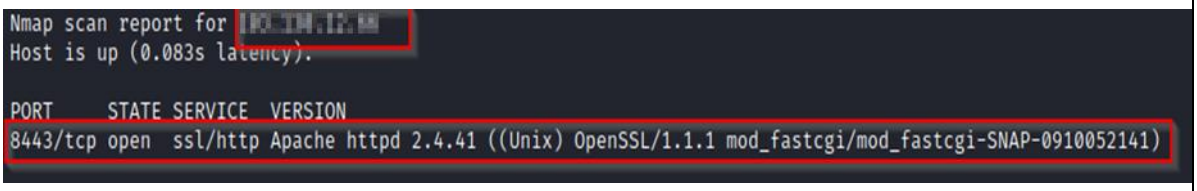


FIGURE 9: SERVER VERSION DISCLOSURE

9. Default Web Server Page Disclosure		
Description	During analysis, it was observed that the default page of the server with the version was getting disclosed in the application.	
Severity	Low	
CVSS Score	3.1	
Instances	**Host**	**Port**
	XX.XX.2.3	2001(TCP)
Impact	There is a complete loss of system protection, resulting in the entire system being compromised. The attacker can render the resource completely unavailable.	
Remediation	Restrict access to the distccd service on UDP port 3632, or remove this service entirely from the host.	
CVSS String	Kept Blank Intentionally	
Reference	https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/	

Proof of Concept

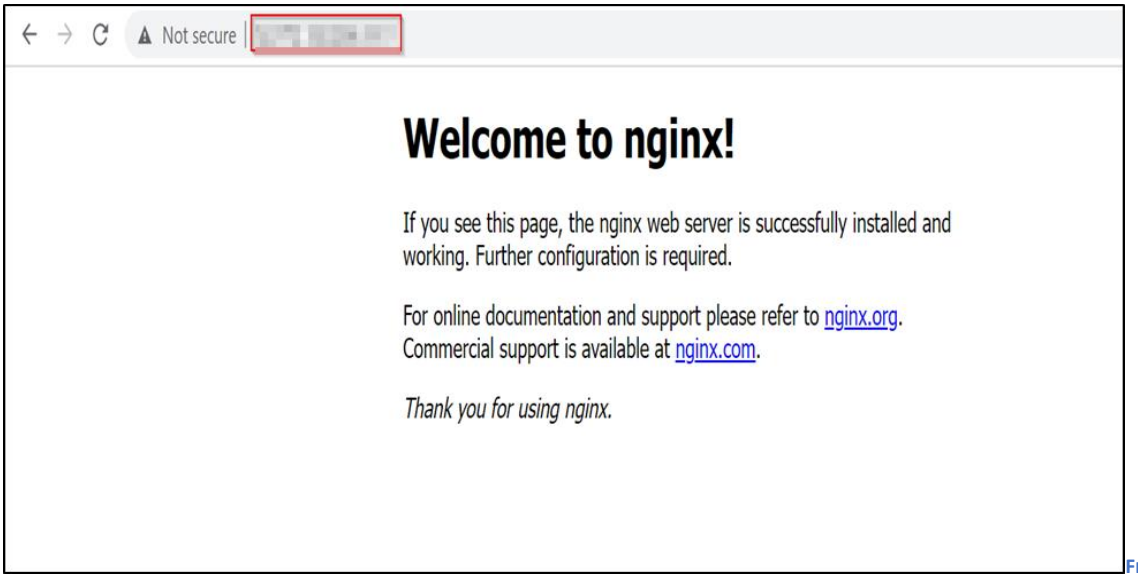


FIGURE 10: DEFAULT WEB SERVER PAG

PORT SCAN STATUS

TCP Scan

IP address: - XX.XX.XX.XX

Port	Protocol	Service Running	Service Version
512	UDP	rlogin	
3632	TCP	Dstccd	
443	TCP	Https	

UDP Scan

IP address: - XX.XX.2.8

Port	Protocol	Service Running	Service Version
161	UDP	SNMP	XX

CONCLUSION

Our security assessment revealed 25 vulnerabilities in the target network, issues are related to command execution, information disclosure, misconfiguration, etc.

Annexure A – CHANGES TO ENVIRONMENT

No changes were made to the environment in scope, such as creating new user accounts or uploading files to the target system. This is provided as the full accounting of modifications by the penetration testing team.

Annexure B – TOOLS USED

Nmap	Nmap is an open-source utility for network discovery and security auditing. Nmap is used to discover the hosts and services on a computer network by sending packets and analysing the responses.
Nessus	Nessus is vulnerability scanner useful for finding and documenting vulnerabilities mostly from the inside of a given network.
SSLSCAN	The SSL Scanner uses a scanning engine based on the *testssl.sh* tool, together with multiple tweaks, adjustments, and improvements. The scanner works by connecting to the target SSL server and trying various ciphers and SSL/TLS protocol versions to determine existing vulnerabilities.
Metasploit	Metasploit is an open-source tool is used to probe systematic vulnerabilities on networks and servers.
Netdiscover	Simple and quick network scanning tool.
The Harvester	E-mails, subdomains and names Harvester - OSINT
WireShark	Wireshark is a network traffic analyzer, or "sniffer", for Unix and Unix-like operating systems.
Netspy	A tool to quickly detect the reachable network segments of the intranet
Qualys	A unique inference-based scan engine to find vulnerabilities.
Empire	An open-source, cross-platform remote administration and post-exploitation framework.
Hashcat	To crack password hashes
Mimikatz	Extracts sensitive information, such as passwords and credentials, from a system's memory.
Kali Linux	Used to initiate advanced-level Security Auditing and Penetration Testing.
Customer Exploit Scripts	

Annexure B - LIST OF VAPT TESTS PERFORMED

Test Cases
Recon
Fingerprinting
SSH Testing
Outdated Software exploit
Unpatched Systems
Clear text protocol
Command Execution
Misconfigured Services Vulnerability Exploit
Remote Code Execution
Multiple SSL Vulnerabilities
Multiple Apache Vulnerabilities
Multiple OpenSSL Vulnerabilities
Server Version Disclosure
Default Web Server Page Disclosure
Weak and default passwords