

NETWORK VULNERABILITY ASSESSMENT

EXTION INFOTECH PROJECT - 1

Lokeshwaran R

—

Cybersecurity Intern

—

August 5,2024

Table of Contents

INTRODUCTION TO PROJECT:	2
NETWORK VULNERABILITY TESTING:.....	3
ASSESSMENT METHODOLOGY	4
TOOLS:	4
VULNERABILITY CLASSIFICATIONS	5
ASSESSMENT FINDINGS	8
MITIGATION STRATEGIES	11
CONCLUSION	13
SUMMARY OF FINDINGS:	13
KEY RECOMMENDATIONS:	13
REFERENCES	16
REFERENCE 1: Overall Scan Result	16
REFERENCE 2: Apache Tomcat AJP connector Request Injection.....	17
REFERENCE 3: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness..	17
REFERENCE 4: UnrealIRCd Backdoor Detection.....	18
REFERENCE 5: Samba Badlock Vulnerability	18
REFERENCE 6: rsh Service Detection	19
REFERENCE 7: Bind Shell Backdoor Detection	19

INTRODUCTION TO PROJECT:

The project titled “Network Vulnerability Assessment” was created by the security team working at ABC Corp (imaginary company) with the aim of finding out what kind of vulnerabilities the company faces, as a way to not only resolve them but act as a proactive means towards avoiding future recurrences of vulnerabilities.

At ABC Corp, securing our digital infrastructure is a top priority, and we are committed to implementing advanced measures to protect our systems and data. As part of our ongoing efforts to fortify our cybersecurity defenses, we are launching a comprehensive Vulnerability Scanning Project. This initiative aims to systematically identify and address potential security weaknesses within our network and applications.

To achieve this, we will be employing two highly effective tools: **Nmap** and **Nessus**. These tools will be crucial in conducting thorough assessments and enhancing our overall security posture.

Nmap (Network Mapper): Nmap is a widely respected open-source tool designed for network discovery and security auditing. It will be used to perform scans of our network infrastructure, identifying active devices, open ports, and the services running on them. This initial phase of our project will provide us with critical insights into our network’s structure and potential vulnerabilities that could be exploited by malicious actors.

Nessus: Complementing Nmap's capabilities, Nessus is a leading vulnerability scanner known for its in-depth analysis and comprehensive vulnerability database. Nessus will be deployed to perform detailed scans on our systems to detect known vulnerabilities, misconfigurations, and security gaps. The tool's extensive plugin library will allow us to generate actionable reports, helping us prioritize and address issues effectively.

The Vulnerability Scanning Project at ABC Corp is designed to proactively identify and mitigate risks, ensuring that our infrastructure remains resilient against potential threats. By leveraging Nmap and Nessus, we aim to enhance our security framework, protect our digital assets, and maintain the highest standards of cybersecurity.

We are committed to safeguarding our organization's resources and look forward to the valuable insights and improvements that this project will deliver.

NETWORK VULNERABILITY TESTING:

Network vulnerability testing is a crucial security process aimed at identifying and evaluating potential weaknesses within a network's infrastructure. The primary goal is to detect vulnerabilities that could be exploited by attackers to gain unauthorized access, disrupt operations, or compromise sensitive data. Vulnerability testing systematically evaluates, reviews and analyses an

organizations network infrastructure by finding vulnerabilities and loopholes that may jeopardize the company's security or be a method used for cyberattacks. The strength of a company's network security is determined by vulnerability testing and hereby will determine the ability of a company to maintain business continuity, protection of sensitive data, compliance and network privacy. Without network vulnerability testing, it is impossible for a company to manage its vulnerabilities, due to the fact that it cannot begin its management process without identifying what areas require to be managed more strategically.

ASSESSMENT METHODOLOGY

The project was conducted through the use of one Vulnerability scanner, and manually through the command Nmap on Kali Linux. The rationale behind using various sources and methods was to ensure a comprehensive and wide range of vulnerabilities to be detected. It was also to ensure a lack of overreliance on one source, but to implement various sources to increase accuracy in results and findings.

TOOLS:

The primary goal of Network Reconnaissance was performed using the following tools:

1. **Nessus:** Nessus is a vulnerability scanner powered by Tenable that seeks to help identify potential vulnerabilities within a system, out of compliance

settings and misconfigurations that may be used by exploits for malicious purposes.

2. **Nmap**: Nmap known as “Network Mapper” is a tool that can be used on Linux as an open-source tool for Network discovery, security auditing, discovering hosts and operating systems. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities

The tools were used for overall network reconnaissance and vulnerability scanning. Nmap was used to understand the network architecture of the company as well as understanding attack surfaces on the network including open ports and vulnerabilities. Nessus was used for vulnerabilities within the company network such as software’s that are not in compliance with industry standards, potential attacks ABC Corp is susceptible to and CVE vulnerabilities according to NIST.

VULNERABILITY CLASSIFICATIONS

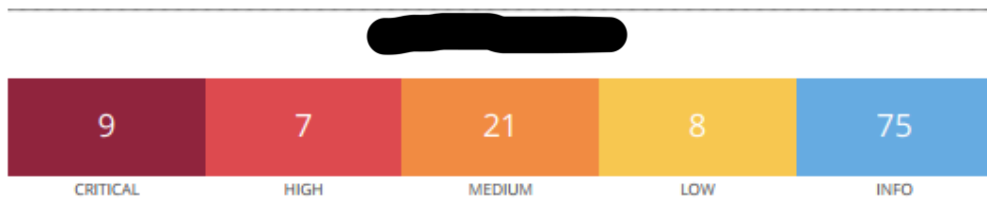
The results that were outputted by the vulnerability scanner: Nessus were categorized according to the National Vulnerability Database Common Vulnerability Scoring system (CVSS) through five score metrics: Critical, High, Medium, Low or Informational.

1. **Critical:** These are vulnerabilities with a CVSS score of 9.0 to 10.0, that indicate they can be easily exploited by an attacker and system can be compromised.
2. **High:** Vulnerabilities with a CVSS score of 7.0 to 8.9, that indicate local users can gain privileges that can allow unauthenticated remote users to view resources or cause a denial of service.
3. **Medium:** Vulnerabilities with a CVSS score of 4.0 to 6.9, that indicate flaws that may be difficult for third parties to exploit but are cause for concern as they can still lead to compromise.
4. **Low:** Vulnerabilities with CVSS score of 0.1 to 3.9, that indicate vulnerabilities that if exploited may cause either no adverse effect or minimal adverse consequences.

Basic information of our target:

Host Information

DNS Name: cpe-192-166-32-11.gpon.tczew.net.pl
Netbios Name: [REDACTED]
IP: [REDACTED]
MAC Address: [REDACTED]
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)



Vulnerabilities

Total: 120

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.0817	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0817	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	5.9	0.015	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	0.6495	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	3.6	0.0157	35450	DNS Server Spoofed Request Amplification DDoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0323	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	0.015	10205	rlogin Service Detection
HIGH	7.5*	6.7	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.1218	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonir
MEDIUM	6.5	3.6	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

192.166.32.11

4

ASSESSMENT FINDINGS

Through the use of two sources, Nessus identified a total of sixteen Vulnerabilities with one being “High” and three scored a CVSS of “Medium”.

On the other hand , vulnerability scanning on Nmap revealed two vulnerabilities that were both categorized as “Medium”.

Below are the vulnerabilities found that are non-informational and found from the various sources. Evidence of the collated vulnerabilities can be referenced to at the end of the document.

1. CVE-2020-1745

Name: Apache Tomcat AJP Connector Request Injection (Ghostcat)

Severity: High

CVSS Score: 9.8

Detail: A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

2. CWE 310

Name: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Severity: Critical

CVSS Score: 10.0

Detail: The remote SSH host keys are weak. The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

3. CVE-2010-2075

Name: UnrealIRCd Backdoor Detection

Severity: Critical

CVSS Score: 10.0

Detail: The remote IRC server contains a backdoor. The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

4. CVE-2016-2118

Name: Samba Badlock Vulnerability

Severity:Medium

CVSS Score: 6.5

Detail: The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

5. CVE-1999-0651

Name: rsh Service Detection

Severity: High

CVSS Score: 7.5

Detail: The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing

(from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

6. #plugin 51988

Name: Bind Shell Backdoor Detection

Severity: Critical

CVSS Score: 9.8

Detail: The remote host may have been compromised. A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

MITIGATION STRATEGIES

1. CVE-2020-1745

- Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

2. CWE 310

- Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

3. CVE-2010-2075

- Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

4. CVE-2016-2118

- Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later

5. CVE-1999-0651

- Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

6. #plugin 51988

- Verify if the remote host has been compromised, and reinstall the system if necessary .

By implementing these mitigation and remediation methods, it is possible to maintain security within the organizations system. Furthermore, by identifying the various risks the organization is vulnerable to, it has allowed us to stay ahead by making the necessary patches to our system and areas that need to be reconfigured entirely.

CONCLUSION

The project conducted by the security team at ABC Corp was an overall success as it allowed us to identify, evaluate and protect our systems from vulnerabilities we are susceptible to as an organization. Through the use of Nessus and Nmap, top six main vulnerabilities were found to exist with one being categorized as “High” while the rest maintained an overall scoring of “Medium”.

SUMMARY OF FINDINGS:

1. ***Vulnerabilities identified with a CVSS Critical score:*** Bind shell backdoor detected
2. ***Vulnerabilities identified with a CVSS Medium score:*** Samba Badlock Vulnerability

KEY RECOMMENDATIONS:

Based on the assessment findings from Nessus and Nmap, several critical vulnerabilities have been identified in the network infrastructure. Below are key recommendations for addressing each vulnerability to mitigate risks and enhance overall security.

1. CVE-2020-1745: Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Severity:** High
- **CVSS Score:** 9.8

Recommendation:

- **Immediate Action:** Update the AJP configuration to enforce proper authorization requirements.
- **Upgrade:** Upgrade Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31, or later to address this vulnerability.
- **Configuration Review:** Ensure that the server configuration is secured, especially for file upload functionalities.

2. CWE-310: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Severity:** Critical
- **CVSS Score:** 10.0

Recommendation:

- **Regenerate Keys:** Treat all existing cryptographic material as compromised. Re-generate all SSH, SSL, and OpenVPN keys.
- **Update System:** Ensure that the OpenSSL library is updated to a version that contains the necessary entropy sources.
- **Monitor:** Regularly review cryptographic practices and key management policies to prevent future issues.

3. CVE-2010-2075: UnrealIRCd Backdoor Detection

- **Severity:** Critical
- **CVSS Score:** 10.0

Recommendation:

- **Reinstallation:** Re-download the UnrealIRCd software from a trusted source, verify the integrity using published MD5/SHA1 checksums, and perform a clean installation.
- **Verification:** Ensure that the newly installed software is free from backdoors and vulnerabilities.

4. CVE-2016-2118: Samba Badlock Vulnerability

- **Severity:** Medium
- **CVSS Score:** 6.5

Recommendation:

- **Upgrade Samba:** Update Samba to version 4.2.11, 4.3.8, 4.4.2, or later to mitigate this vulnerability.
- **Configuration Review:** Review Samba configurations to ensure secure communication and proper authentication levels.

5. CVE-1999-0651: rsh Service Detection

- **Severity:** High
- **CVSS Score:** 7.5

Recommendation:

- **Disable rsh Service:** Comment out the 'login' line in /etc/inetd.conf and restart the inetd process, or completely disable the rsh service.
- **Switch to SSH:** Replace rsh with a more secure protocol like SSH for remote command execution.

6. #plugin 51988: Bind Shell Backdoor Detection

- **Severity:** Critical
- **CVSS Score:** 9.8

Recommendation:

- **Immediate Investigation:** Verify if the remote host has been compromised by conducting a thorough forensic investigation.
- **System Reinstallation:** If compromise is confirmed, reinstall the affected system from a clean backup to remove any backdoor access.

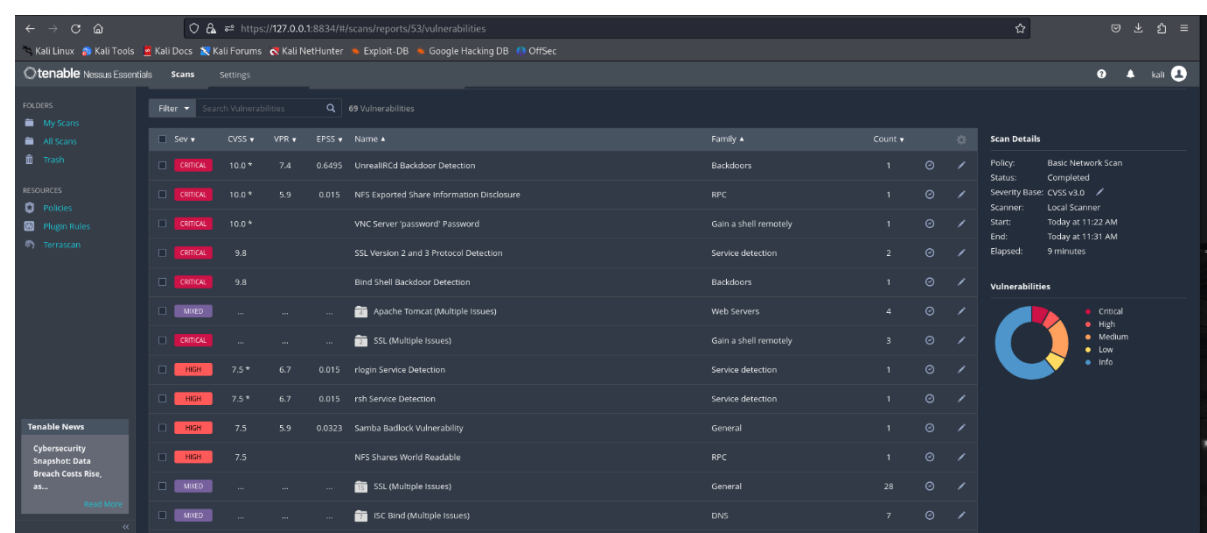
General Recommendations

- **Regular Updates:** Ensure that all software and systems are regularly updated to their latest versions to mitigate known vulnerabilities.
- **Security Best Practices:** Implement and adhere to security best practices, including regular vulnerability scanning and system reviews.
- **Incident Response:** Develop and maintain an incident response plan to quickly address and remediate security breaches.

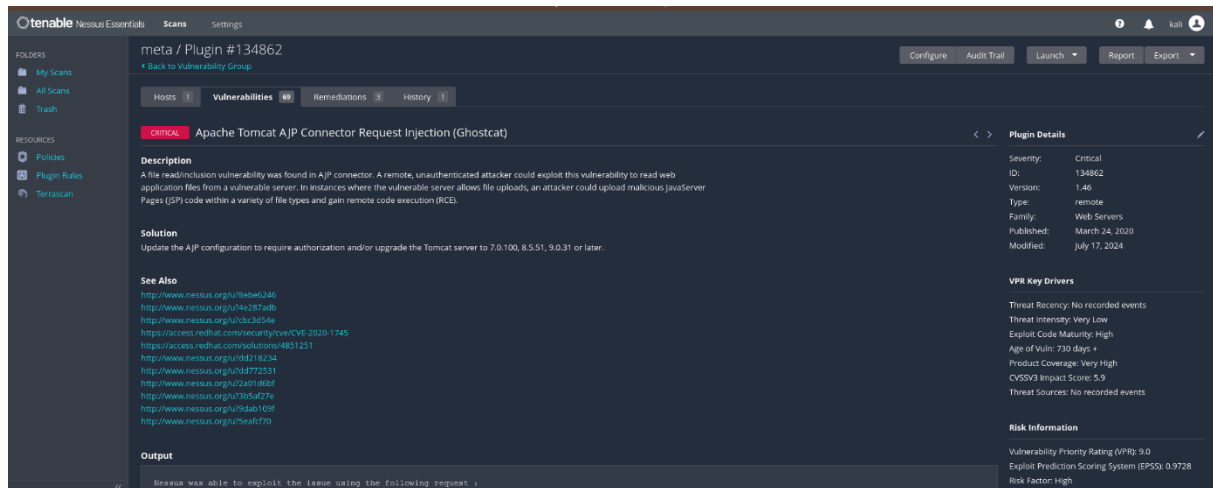
By following these recommendations, ABC Corp can effectively mitigate the identified vulnerabilities, strengthen its security posture, and reduce the risk of potential attacks. Regular assessments and updates are essential to maintaining a secure and resilient network environment.

REFERENCES

REFERENCE 1: Overall Scan Result

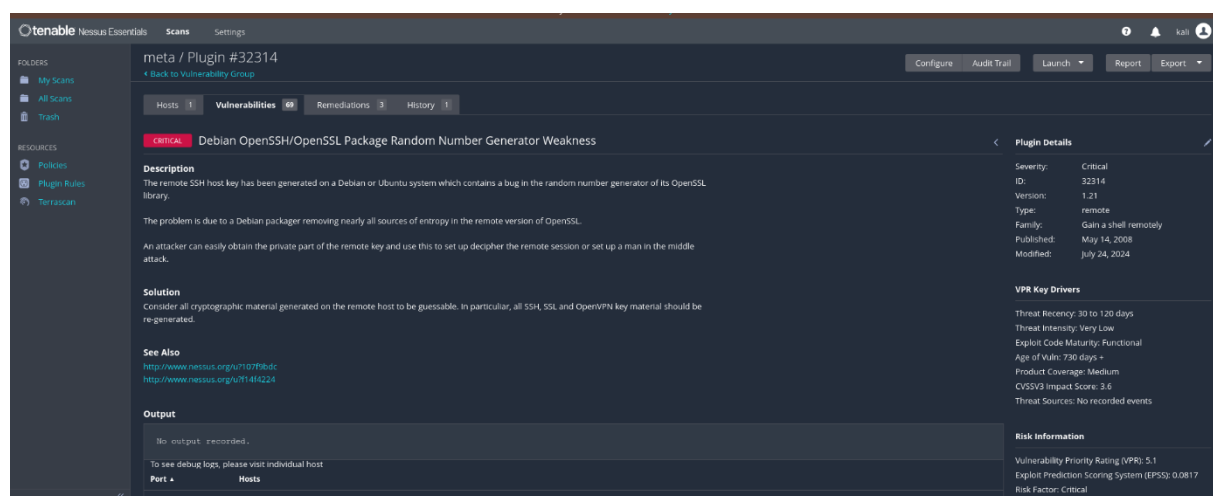


REFERENCE 2: Apache Tomcat AJP connector Request Injection



The screenshot displays the Tenable Nessus Essentials interface. The left sidebar shows the navigation menu with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'meta / Plugin #134862' and includes tabs for 'Hosts', 'Vulnerabilities', 'Remediations', and 'History'. The 'Vulnerabilities' tab is active, showing a 'CRITICAL' severity vulnerability titled 'Apache Tomcat AJP Connector Request Injection (Ghostcat)'. The description states: 'A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE)'. The solution advises updating the AJP configuration to require authorization and/or upgrading the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later. The 'See Also' section lists several CVEs and their corresponding Nessus plugin IDs. The 'Output' section shows a snippet of an exploit request. On the right, the 'Plugin Details' panel provides metadata: Severity: Critical, ID: 134862, Version: 1.40, Type: remote, Family: Web Servers, Published: March 24, 2020, Modified: July 17, 2024. Below this, the 'VPR Key Drivers' section lists factors like Threat Recency, Threat Intensity, and Exploit Code Maturity. The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 9.0, an Exploit Prediction Scoring System (EPSS) of 0.9728, and a Risk Factor of High.

REFERENCE 3 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness



The screenshot displays the Tenable Nessus Essentials interface for Plugin #32314: 'Debian OpenSSH/OpenSSL Package Random Number Generator Weakness'. The left sidebar is identical to the previous screenshot. The main content area shows the 'Vulnerabilities' tab with a 'CRITICAL' severity vulnerability. The description explains that the remote SSH host key was generated on a Debian or Ubuntu system with a bug in the OpenSSL random number generator, and that the problem is due to a Debian packager removing entropy sources. It notes that an attacker can obtain the private part of the remote key to decipher sessions or perform a man-in-the-middle attack. The solution suggests regenerating cryptographic material on the remote host. The 'See Also' section lists CVEs and Nessus plugin IDs. The 'Output' section indicates 'No output recorded'. The 'Plugin Details' panel on the right shows: Severity: Critical, ID: 32314, Version: 1.21, Type: remote, Family: Gnu's shell remotely, Published: May 14, 2008, Modified: July 24, 2024. The 'VPR Key Drivers' section lists Threat Recency (30 to 120 days), Threat Intensity (Very Low), Exploit Code Maturity (Functional), Age of Vuln (730 days), Product Coverage (Medium), and CVSSv3 Impact Score (3.6). The 'Risk Information' section shows a Vulnerability Priority Rating (VPR) of 5.1, an EPSS of 0.0817, and a Risk Factor of Critical.

REFERENCE 4 UnrealIRCd Backdoor Detection

meta / Plugin #46882

[Back to Vulnerabilities](#)

Hosts 1 | **Vulnerabilities 69** | Remediations 3 | History 1

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://redlists.org/fulldisclosure/2010jun277>
<https://redlists.org/fulldisclosure/2010jun284>
<http://www.unrealircd.com/xt/unrealircdadvocary.20100612.txt>

Output
The remote IRC server is running as :
uid=0 (root) gid=0 (root)

To see debug logs, please visit individual host

Port **Hosts**
6667 / tcp / irc

Plugin Details

Severity: Critical
ID: 46882
Version: 1.16
Type: remote
Family: Backdoors
Published: June 14, 2010
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuhn: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4
Exploit Prediction Scoring System (EPSS): 0.6495
Risk Factor: Critical

REFERENCE 5 Samba Badlock Vulnerability

meta / Plugin #90509

[Back to Vulnerabilities](#)

Hosts 1 | **Vulnerabilities 69** | Remediations 3 | History 1

HIGH Samba Badlock Vulnerability

Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also
<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output
Nessus detected that the Samba Badlock patch has not been applied.

To see debug logs, please visit individual host

Port **Hosts**
445 / tcp / cifs

Plugin Details

Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuhn: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.0323
Risk Factor: Medium

REFERENCE 6: rsh Service Detection

meta / Plugin #10245

[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 6 Remediations 3 History 1

HIGH rsh Service Detection

Description
The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in plaintext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution
Comment out the rsh line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Output
No output recorded.
To see debug logs, please visit individual host

Port	Hosts
514/tcp/rsh	[REDACTED]

Plugin Details

Severity: High
ID: 10245
Version: 1.38
Type: remote
Family: Service detection
Published: August 22, 1999
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.7
Exploit Prediction Scoring System (EPSS): 0.015
Risk Factor: High

REFERENCE 7: Bind Shell Backdoor Detection

meta / Plugin #46882

[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 6 Remediations 3 History 1

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://redlists.org/fulldisclosure/2010/jun/277>
<https://redlists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/text/unrealsecadvicory/20100612.txt>

Output
The remote IRC server is running as :
uid=0 (root) gid=0 (root)

To see debug logs, please visit individual host

Port	Hosts
6667/tcp/irc	[REDACTED]

Plugin Details

Severity: Critical
ID: 46882
Version: 1.16
Type: backdoors
Family: Backdoors
Published: June 14, 2010
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Functional
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4
Exploit Prediction Scoring System (EPSS): 0.6495
Risk Factor: Critical