Cyber Risk Assessment Project

For University of Iceland

Version 1.0

December 9, 2019

Major: Cybersecurity

By: Markail Bruner

**Table of Contents**

CONTENTS………………………………………………………………………………………………………………………………… 2

1 EXECUTIVE SUMMARY……………………….……………..…………………………………………………………………… 4

1.1 SCOPE OF WORK…….……………………………………..…………………………………………………………………… 4

1.2 POTENTIAL SOLUTIONS……………………………………………………………….……………………………………… 4

1.3 SYSTEMS AND SECURITY…………………………………………………………………………………………………….. 4

1.4 SUMMARY OF FINDINGS………………………………………………………………………………………..…………… 5

1.5 SUMMARY OF RECOMMENDATION.…………………………………………..………………………….…………… 5

2 METHODOLOGY …………………………………………………………………………………………………………….……… 6

2.1 SEVERITY LIST OF TARGETS ………………………………………………………………………………………………… 6

2.2 METASPLOITABLE 2 ………………..……………………………………………………………………….………………… 6

2.3 WINDOWS 7 …………………………………………………………………………………………………………………….. 12

2.4 SEEDUbuntu …………………………………………………………………………………………………………………….. 13

2.5 WINDOWS XP………………………………………………………………………………………………………….……….. 13

3.0 DETAILED FINDINGS………………………………………………………………………………………………………….. 14

3.1 CONSEQUENCES……………………………………………………………………………………………………………….. 15

3.2 RECOMMENDATIONS……………………………………………………………………………………………………….. 15

**List of Tables / Graphs**

**Tables**

Table 1 Risk Levels and Count

Table 2 Detailed Port, Protocol, and Service

Table 3 Detailed Port, Protocol, and Service

Table 4 Detailed Port, Protocol, and Service

**Graphs**

Graph 1 Percentage of Severity Levels and Count

**1. Executive Summary**

**1.1 Scope of work**

For the vulnerability assessment I began with the four target VMs and went into discovering that there are common problems across most of the VMs that were a common occurrence. Whether it was shell remote, web servers, or general problems they seemed to contain problems regarding the insecure nature.

**1.2 Potential Solutions**

According to NIST NVD a lot of the solutions require security patches for most of the findings because there was a lot of outdated or unsupported versions. They also recommended vendor advisory’s which were concluded to be weak in nature or not recommended due to flaws. NIST NVD mentions to take certain actions to fix exploits which they recommend by redirecting to a third-party solution.

**1.3 Systems and Security**

There were three different targets that had vulnerabilities which included Metasploit 2 the one in which had the most risk, windows 7, and SEEDUbuntu. Metasploit 2 was very insecure containing a laundry list of either exploitable flaws, outdated, or unsupported versions. The other two had medium level risk but still had their problems that could have severe consequences if nothing is done. Windows Xp was the only target that was secure with information being the only result.

**1.4 Summary of Findings**

**Table 1**

|  |  |
| --- | --- |
| Level of Risk | Number of Risks |
| Information | 210 |
| Low | 4 |
| Medium | 16 |
| High | 2 |
| Critical | 7 |

**Graph 1**

**1.5 Summary of Recommendation**

There are a lot of problems mentioned here and as seen above largely around the medium level of risk but still containing some critical risks that need immediate attention. The medium levels are mainly around outdated or unsupported certificates that need to be purchased or versions that need security patches. Going through each of the vulnerabilities making sure versions are up to date, updating passwords, and thorough evaluation of each target in order to make sure the system is secure.

**2 Methodology**

**2.1 Severity List of Targets at Risk from High to Low –**

**2.2 Metasploitable 2** -192.168.217.134 (6 Critical, 2 High, 12 Medium, 4 Low)

CRITICAL RISK:

**Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | CVSS Score: 10.0**

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 remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random generator of its OpenSSL library.

The Debian packager removes almost all sources of entropy in the remote version of OpenSSL.

**SCENARIO**: An attacker can easily get the private part of a remote key and use the setup to decipher the remote session or set up a man in the middle attack.

**Bind Shell Backdoor Detection | CVSS Score: 9.8**

A shell is listening on the remote port without any authentication being required.

**SCENARIO**: The attacker could connect to the remote port and send the commands directly.

**NFS Exported Share Information Disclosure**

At least one of the NSF Shares exported by the remote server could be mounted by the scanning host.

**SCENARIO**: An attacker could leverage this to read and potentially write files on the remote host.

**Unix Operating System Unsupported Version Detection | CVSS Score: 10.0**

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**SCENARIO**: The potential vulnerabilities can be exploiting depending on the kind of vulnerability it is which could lead to fatal consequences for the system.

**VNC Server ‘password’ Password | CVSS Score: 10.0**

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of ‘password’.

**SCENARIO**: Due to the fact of such a simple, unsecure password an attacker could use exploit this and take control of the system.

HIGH RISK:

**Unsupported Web Server Detection | CVSS Score: 10.0**

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Scenario: An attacker can exploit the server by using methods that were patched in newer versions on this server allowing them unauthorized access.

**SSL Version 2 and 3 Protocol Detection | CVSS Score: 7.5**

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, these versions of SSL are affected by several cryptographic flaws which include, insecure padding scheme with CBC ciphers and insecure session renegotiation and resumption schemes.

**SCENARIO**: An attacker can exploit these flaws by conducting a man-in-the-middle attack to decrypt communications between the affected service and clients.

MEDIUM RISK:

**SSL Certificate Cannot Be Trusted | CVSS Score: 6.5**

The certificate chain sent by the server might not be descended from a known public certificate authority, it may contain a certificate that is not valid at the time of the scan, or the certificate chain may contain a signature that either did not match the certificate’s information or could not be verified.

**SCENARIO**: The attacker could have an easier time conduction a man-in-the-middle attack against the remote host because of the public host which makes it more difficult to verify authenticity and identity of web server.

**SSL Certificate Expiry | CVSS Score: 5.3**

This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

**SSL Certificate with Wrong Hostname | CVSS Score: 5.3**

The ‘commonName’ (CN) attribute of the SSL certificate presented for this service is for a different machine.

**SSL Medium Strength Cipher Suites Supported (SWEET32) | CVSS Score: 7.5**

The remote host supports the use of SSL ciphers that offer medium strength encryption.

**SSL Self-Signed Certificate | CVSS Score: 6.4**

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.

**SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability | CVSS Score: 6.8**

The remote host is affected by a man-in-the-middle information disclosure vulnerability known as POODLE. The vulnerablitiy is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

**SCENARIO**: The man-in-the-middle attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

**HTTP TRACE / TRACK Methods Allowed | CVSS Score: 5.3**

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

**SSH Weak Algorithms Supported | CVSS Score 4.3**

The remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4523 advises against use Arcfour due to an issue with weak keys.

**Apache Tomcat Default Files | CVSS Score 5.3**

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server.

**SCENARIO**: The attacker could uncover information about the remote Tomcat install or host itself.

**SMB Signing not required | CVSS Score 5.3**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**NFS Share World Readable | CVSS Score 7.5**

The remote NFS server is exporting or more shares without restricting access (based on hostname, IP, or IP range).

Samba Badlock Vulnerability

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 Security Account Manager (SAM) and Local Security Authority protocols due to improper authentication level negotiation over Remote Procedure Call channels.

**SCENARIO**: If an attacker conducts a man-in-the-middle attack intercepting the traffic between client and server this flaw can be exploited which will downgrade the authentication level allowing arbitrary calls leading to modification of Active Directory.

LOW RISK:

**SSL RC4 Cipher Suites Supported (Bar Mitzvah) | CVSS Score: 5.9**

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

**SCENARIO**: If the plaintext is repeatedly encrypted and the attacker is able to obtain many ciphertexts then they may be able to derive the plaintext.

**SSH Server CBC Mode Ciphers Enabled | CVSS Score: 2.6**

The SSH server is configured to support Cipher Block Chaining encryption.

**SCENARIO**: The attacker could recover the plaintext message from the cipher text.

**SSH Weak MAC Algorithms Enabled | CVSS Score: 2.6**

The remote SSH server is configured to allow wither MD5 or 96-bit MAC algorithms, both are considered weak.

**X Server Detection | CVSS Score: 2.6**

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Scenario: An attacker could eavesdrop on the connection due to the insecure traffic that is passed on the X11.

**2.3 Windows 7** – 192.168.217.135 (1 Critical, 2 Medium)

CRITICAL RISK:

**MS17-010: Security Update for Microsoft Windows SMB Server (4013389) | CVSS Score: 8.1**

Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 due to improper handling of certain requests.

**SCENARIO**: A remote attacker will exploit the vulnerabilities by creating a specific packet to execute arbitrary code.

MEDIUM RISK:

**MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) | CVSS Score: 6.8**

The remote Windows host is affected by an elevation of privilege vulnerability 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.

**SCENARIO**: The attacker can use man-in-the-middle exploitation to intercept communications between a client and a server hosting a SAM database which will allow the attacker to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

**SMB Signing not required | CVSS Score 5.3**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**2.4 SeedUbuntu** – 192.168.234.139 (2, Medium)

MEDIUM RISK:

**HTTP Reverse Proxy Detection | CVSS Score: 5.4**

This web server is reachable through a reverse HTTP proxy.

**Unencrypted Telnet Server | CVSS Score: 6.5**

The remote host is running a Telnet server over an unencrypted channel.

**SCENARIO**: Once the attacker conducts a MITM attack to eavesdrop on a Telnet session they will obtain the information needed and modify traffic that is exchanged between client and server.

**2.5 Windows Xp** -192.168.217.136 (None, just information given)

**3.0 Detailed Findings** –

Detailed Systems Information

Ip Address: 192.168.217.134 IP Address: 192.168.217.135

OS Information: Metasploit OS Information: Windows 7

Table 2 Table 3

|  |  |  |
| --- | --- | --- |
| Port# | Protocol | Service Name |
| 22 | tcp | ssh |
| 5432 | tcp | postrgesql |
| 1524 | Tcp | wild\_shell |
| 2049 | tcp | rpc-nfs |
| 5900 | tcp | vnc |
| 8180 | tcp | www |
| 5432 | tcp | postgresql |
| 80 | tcp | www |
| 6000 | tcp | x11 |

|  |  |  |
| --- | --- | --- |
| Port# | Protocol | Service Name |
| 445 | tcp | Cifs |
| 49156 | tcp | dce-rpc |

IP Address: 192.168.234.139

|  |  |  |
| --- | --- | --- |
| Port# | Protocol | Service Name |
| 3128 | tcp | http\_proxy |
| 23 | tcp | telnet |

OS Information: SEEDUbuntu

Table 4

**3.1 Consequences:**

Potential exploitation of these various issues can lead to confidential information being leaked such as company inside secrets that contain pertinent details to a project. Servers being targeted for DoS attacks and other hosts that are easily eavesdropped on may lead to more time to be secure leading to more downtime.

**3.2 Recommendations**:

A lot of issues that are targeted by attackers using the man-in-the-middle attack method and to prevent that regenerate any SSH, SSL, and OpenVPN keys. As well as updating any out of date, unsupported or old versions that require a security patch. Purchasing any outdated or insecure certificates per services. Make sure all passwords are changed to more complex and less weak passwords, and restrict accesses to unsecure ports or disable the ports in general.