Project Patch and Protect

Eli Burton, Jon Bellovin,Tanner Valencia, Luc Selman

Project Patch and Protect

Research and Patching of Vulnerabilities contained in Virtual Machines

- We have made a selection of two Operating Systems or Virtual Machines (referred to as “VM”’s) and subsequently analyzed their commonly known vulnerabilities in an effort to provide a framework to rectify and resolve them to a minimum operable standard that will provide the best possible configuration to protect against exploitation and provide the strongest “security stance”
    - The VM’s chosen for analysis are:
        - “Metasploitable,” a Linux-based security project designed by Rapid7, LLC that provides information about security vulnerabilities and aids developers in the creation and testing of tools designed to prevent intrusion into a computer network
        - “Broken Web Applications,” an infrastructure designed by OWASP (Open Web Application Security Project) which aggregates a number of vulnerable Web Applications into a serviceable Linux-based VM as a tool for education on the nature and structure of common services used in server-client interaction

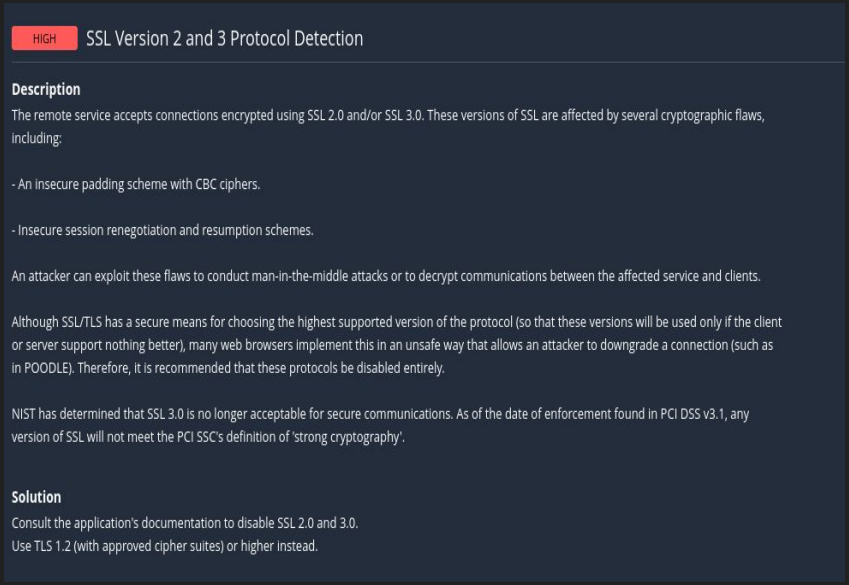
Project Patch and Protect

Research and Patching of Vulnerabilities contained in Virtual Machines

- Analysis of each VM begins by using a Vulnerability Scanner- a tool designed to test designated targets for a myriad of known vulnerabilities and exploits and catalog and organize them into a navigable and interpretable format. Our chosen Vulnerability Scanner is a service called “Nessus”
  - Nessus scans provide a picture of a given target’s vulnerabilities and assigns them a Common Vulnerability Score against the Common Vulnerability Score System. This system assigns a score from 0.1 to 10.0 with 0.1 being the lowest vulnerable score, and 10.0 being the highest or most “Critical” score
  - This CVSS classification provides an accurate picture to analysts about the greatest threats to a given target and allows for the proper prioritization with which to address a given vulnerability, along with providing a set of approaches to potential resolution. These resolutions are not an exclusive means to addressing the vulnerabilities, but simply provide a starting to point with which to address and resolve a given exploit
  - The vulnerabilities our group has chosen to address along with their viable resolutions are detailed as follows:

SSL Version 2.0, 3.0 (OWASP BWA, CVS Score 7.5)

The Nessus scan for the BWA VM details this exploit having cryptographic flaws that could allow for de-crypted communications or man-in-the-middle attacks.



HIGH SSL Version 2 and 3 Protocol Detection

Description

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, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

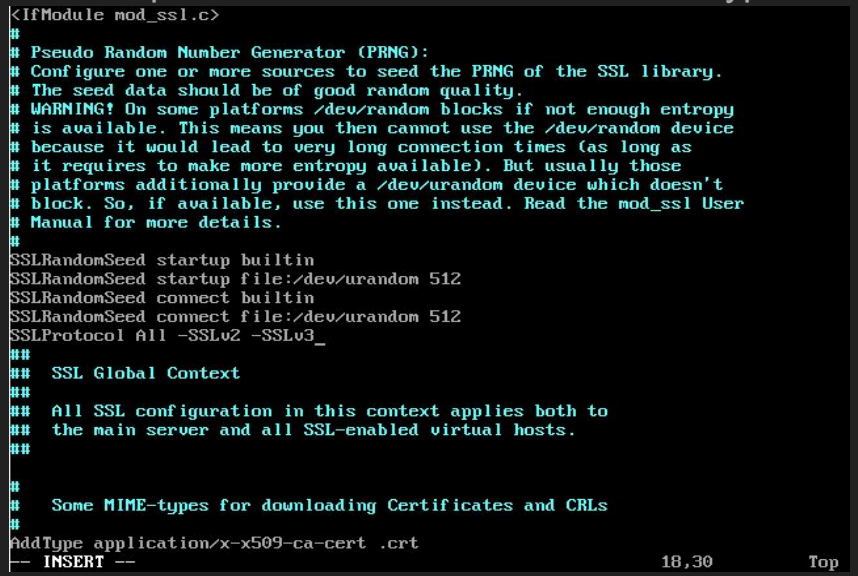
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

By accessing the OpenSSL ".conf" file, SSL versions 2.0 and 3.0 can be disabled. Instead, TLS 1.2 is enabled to prevent the transfer of data in plain-text format and maintain encryption

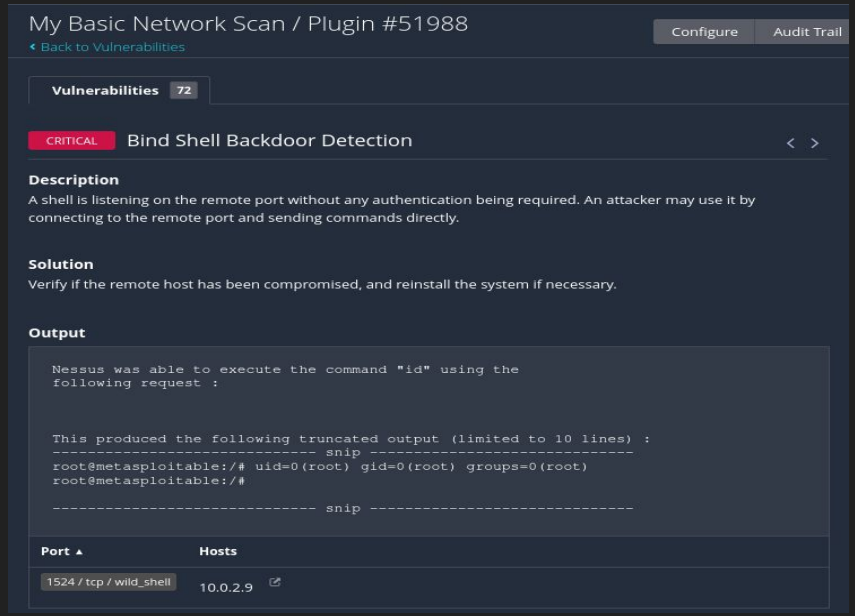


```
<IfModule mod_ssl.c>
#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough entropy
# is available. This means you then cannot use the /dev/random device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device which doesn't
# block. So, if available, use this one instead. Read the mod_ssl User
# Manual for more details.
#
SSLRandomSeed startup builtin
SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect builtin
SSLRandomSeed connect file:/dev/urandom 512
SSLProtocol All -SSLv2 -SSLv3_
##
##  SSL Global Context
##
##  All SSL configuration in this context applies both to
##  the main server and all SSL-enabled virtual hosts.
##


#
#   Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
-- INSERT --                                          18,30         Top
```

Bindshell Backdoor (Metasploitable, CVS Score 9.8)

The Nessus scan for Metasploitable details this vulnerability as a remote shell connected over an unassigned TCP port, port 1524



Nessus further details this vulnerability as allowing a remote connection direct access to the VM's command line interface without any required authentication, potentially allowing an attacker to access any and all information contained on the device. The command line tool "iptables" will allow for the native firewall to block all communication over port 1524, effectively deterring an attacker by using the following syntax:

"/sbin/iptables -A INPUT -p tcp --destination-port 1524 -j DROP"

Metasploitable - Apache Tomcat AJP Connector Request Injection (a.k.a Ghostcat) - CVE-2020-1745 - CVSS Score: 9.8

Service:

- Apache Tomcat is a web server for implementing Javascript files to an Apache web server
- Apache JServ Protocol (AJP) is used for communicating between the Tomcat and Apache web servers

Vulnerability:

- The AJP connector on Tomcat, by default, listens for all ip addresses on port 8009, allowing anybody to connect through the port to the service.
- This allows attackers to exploit it and perform file uploads of Javascript files through the open port to the Tomcat server to execute code remotely

Tomcat AJP Patch / Solution

1 - If an AJP connection is not required, comment out or delete the AJP protocol enabler code in the server.xml file for Tomcat

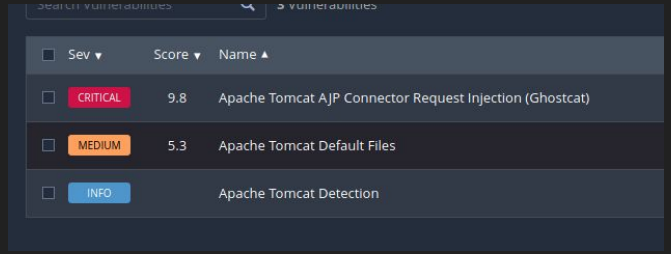
Code:

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

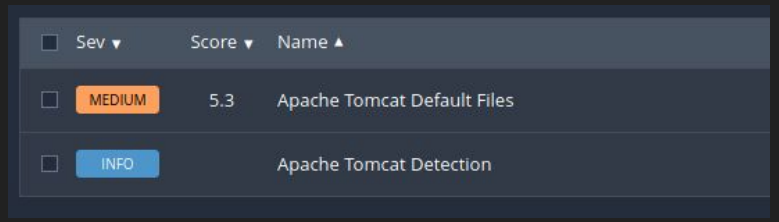
2 - If AJP is needed for functionality of the server, add a password to the AJP protocol code in the server.xml file for Tomcat to restrict direct access to the service:

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" address="YOUR_TOMCAT_IP_ADDRESS" requiredSecret="YOUR_AJP_SECRET" />

Before Fixes:



After Fixes:



Metasploitable - ISC BIND Service Downgrade / Reflected Denial of Service CVE-2020-8616 - CVSS Score: 8.6

Service

- BIND is a Domain Name Service (DNS) used to run a caching DNS server or an authoritative name server

Vulnerability

- In older versions of BIND, the service does not limit the number of requests that can be given to the server in a short amount of time by one client
- A malicious actor can exploit this lack of limitation by sending many requests to the server which causes it to attempt to issue a significant amount of fetches leading to degradation of the server and slowing down fetching times for all other clients

ISC BIND Denial of Service Patch / Solution

1. **Update BIND to the most recent patch release to enable the fix for limiting packet traffic**

2. **Create a firewall rule that blocks an ip that sends more than a hundred packets to the server in a short amount of time**

```
msfadmin@metasploitable:~$ sudo /sbin/iptables -A INPUT -p tcp --dport 53 -i eth
0 -m state --state NEW -m recent --update --seconds 10 --hitcount 100 -j DROP
msfadmin@metasploitable:~$
```

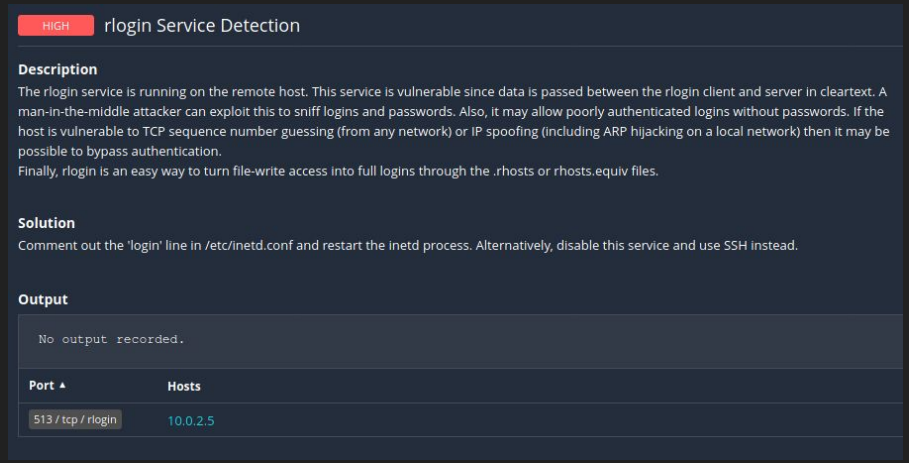
rlogin Service Detection Vulnerability - Metasploitable

- Vulnerability: The rlogin service is running on the remote host, allowing a man-in-the-middle attack to sniff logins and passwords, IP spoofing such as ARP hijacking on a local network, and poorly authenticated logins without passwords.
- Patch/Solution: Comment out the 'login' line in /etc/inetd.conf to disable the service.

```
msfadmin@metasploitable:/etc$ vim inetd.conf
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlo
```

- In a case where the rlogin service exemplifies a necessary legacy system, disabling the service may not be possible.
- An approach to mitigate the risk, while keeping the rlogin service active, could be to create rules through SNORT or ICTABLES to limit connections to the port and IP address of the personnel needing to use this service.

CVSSv3 Impact Score: 5.9



SMTP Service StartTLS Plaintext Command Injection - Metasploitable

- Vulnerability:
  - The remote SMTP (Simple Mail Transfer Protocol) service contains a software flaw in its StartTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.
  - Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer)
- Patch/Solution:
  - STRIPTLS attacks can be blocked by configuring SMTP clients to require TLS for outgoing connections
  - Update SMTP version or Windows Server version

CVSSv3 Impact Score: 5.5

RSH Service Detection Metasploitable CVSSv2: 10.0

RSH Service

- Stands for ‘Remote Shell’
- Tool for executing remote commands on a machine.
- Recommended to be disabled immediately, superseded by SSH

Vulnerability

- Passes data between rsh client and server in cleartext or non-securely
- May allow poorly authenticated logins without passwords

Solution

- Comment out the line for RSH in the inetd.conf file
- Disable the service and implement SSH

Samba Badlock OWASPBWA CVSSv3: 7.5

Samba Service

- CIFS/SMB server for Linux and Unix operating systems
- Designed to provide users with secure,stable and fast file and print services in 1992
- Free software that can function as a domain controller or as a regular domain member

Vulnerability

- Susceptible to PiTM(Person in the middle) style attacks
- PiTM can intercept any dcerpc traffic between a client and server
- Can be a gateway for privilege escalation through intercepted traffic

Solution

- Update to the latest Samba software
- As a workaround privileged account login attempts should not be authenticated over unprotected or unknown networks and only accessed on the physical console so that authentication does not involve any network communication