Eli -

- **Metasploitable - ISC BIND Service Downgrade / Reflected DoS - CVE-2020-8616**
  - Service:
    - BIND (Berkeley Internet Name Domain) is one of the most popular domain name services (DNS) in use
    - It was created in the 1980's
    - BIND can be used to run a caching DNS server or an authoritative name server, and provides features like load balancing, notify, dynamic update, split DNS, DNSSEC, IPv6, and more
  - Vulnerability:
    - In older versions of BIND, the service does not limit the number of fetches that can be performed while processing a referral response
    - A malicious actor can exploit this lack of limitation by sending many referrals to the server that causes it to attempt to issue a significant amount of fetches that leads to degradation of the server and slowing down fetching times
    - Additionally, this exploit of the referral issuing server can be used as a reflector in a DoS reflection amplification attack
  - Patch / Solutions:
    - Update BIND to the patch release most closely related to your version of BIND: Our version is 9.4.2 - We would want to upgrade to 9.11.19
    - Create a firewall rule that blocks an ip that sends more than a hundred packets to the server in a short amount of time

  Sources: https://kb.isc.org/docs/cve-2020-8616 – https://ns1.com/resources/bind-dns-pros-cons-and-alternatives

- **OWASPBWA - SSL Certificate Signed Using Weak Hashing Algorithm - CVE-2004-2761**
  - Service:
    - SSL, or Secure Sockets Layer, is a protocol used to create authenticated and encrypted links between networked devices.
    - SSL uses Asymmetric cryptography to secure its traffic using public and private keys
  - Vulnerability:
    - SSL previously used SHA-1 as its cryptographic hash algorithm, but this method has been declared as vulnerable after Jan 1, 2017
    - Currently, attackers can utilize a collision attack against the outdated hashes to exploit the service and generate a certificate with the same signature as an authentic connection and perform Man in The Middle attacks with the copied signature.
  - Patch / Solutions:
    - Issue a new SSL certificate for the web server with an updated hash
    - Disable SSL completely from the web server

  Sources: https://www.ssl.com/faqs/faq-what-is-ssl/ – https://nvd.nist.gov/vuln/detail/CVE-2004-2761

- **Metasploitable - Apache Tomcat AJP Connector Request Injection (a.k.a Ghostcat) - CVE-2020-1745**
    - Service:
        - Apache Tomcat is a web server for implementing Java EE specifications like, Java Servlet, JavaServer Pages, Java Expression Language, and Java WebSockets.
        - Apache JServ Protocol (AJP) is used for communicating between Tomcat and Apache web servers
    - Vulnerability:
        - The AJP connector on Tomcat, by default, listens on all addresses on port 8009. The connection is treated with more trust than a normal http connection
        - This allows attackers to exploit it and perform file uploads that are not intended. Attackers can upload Javascript files through the open port to the Tomcat server to execute code remotely
    - Patch / Solutions:
        - Comment out or delete the AJP protocol in the server.xml file for Tomcat:
            - <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

Sources: https://www.chaitin.cn/en/ghostcat – https://blog.qualys.com/product-tech/2020/03/10/detect-apache-tomcat-ajp-file-inclusion-vulnerability-cve-2020-1938-using-qualys-was – https://www.jrebel.com/blog/what-is-apache-tomcat

Tanner -

Metasploitable: rexecd Service Detection

- Description
    - Service designed to allow users of a network to execute commands remotely.
- Vulnerability
    - rexecd does not provide any proper means of authentication, so it may be abused by an attacker to scan a third-party host.
- Solution
    - Comment out the ‘exec’ line in the inetd configuration file and restart process

Metasploitable: rsh Service Detection

- Description
    -
- Vulnerability
    - Data is passed between the rsh client and server in cleartext
    - May allow poorly authenticated logins without passwords
    -
- Solution
    - Comment out the ‘rsh’ line in the inetd configuration file
    - Disable service and implement ssh

OWASPBWA: Samba Badlock, Unix OS Unsupported Version

- Samba Description
  - CIFS/SMB server for Linux and Unix
  - Provides users with secure, stable and fast file and print services since 1992
  - Can function as a domain controller or as a regular domain member
  - Free software
- Samba Vulnerability
  - PiTM can intercept any DCERPC traffic between a client and a server
  - Privilege escalation through intercepted traffic
- Solution
  - Update software
  -

The Unix operating system currently installed is now an EOL product and needs to be replaced

Luc - OWASP:

SSL Version 2 and 3 Protocol Detection:

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'.

Jon -
Metasploitable - rlogin Service Detection
Service Description

- Remote login is a tool for remotely using a computer over a network. It has been replaced by the more secure SSH.

Vulnerability Description

- 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 or remove the service and replace it with SSH.

Metasploitable - SMTP Service STARTTLS Plaintext Command Injection
Service Description

- STARTTLS is an email protocol command
- SMTP (Simple mail transfer protocol)

Vulnerability Description

- The remote SMTP 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

Metasploitable - UnrealIRCd Backdoor Detection

Service Description

- An open source IRC server

Vulnerability 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.
-

Patch / Solution

- Update to latest version