Lab 3 – Service Discovery and Vulnerability Assessment

1. Service Discovery

Tools:

Nmap: A powerful network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Masscan: Like Nmap but designed for speed and can scan the entire Internet in under 6 minutes.

2. OS and Application Fingerprinting

Tools:

Nmap: Beyond port scanning, Nmap can be used for OS detection.

3. Vulnerability Scanning

Tools:

Nikto: A web server scanner which performs comprehensive tests against web servers for multiple items, including potentially dangerous files and programs.

Nmap: Nmap has a set of scripts categorized under vuln, which can be used to detect common vulnerabilities.

OpenVAS: A full-featured vulnerability scanner.

Metasploit Framework: Useful for validating identified vulnerabilities through exploitation attempts.

4. Documentation

Creating a table summarizing findings.

IP Address: List the IP addresses of the discovered hosts.

Open Services/Applications: List of the services/applications found on each host.

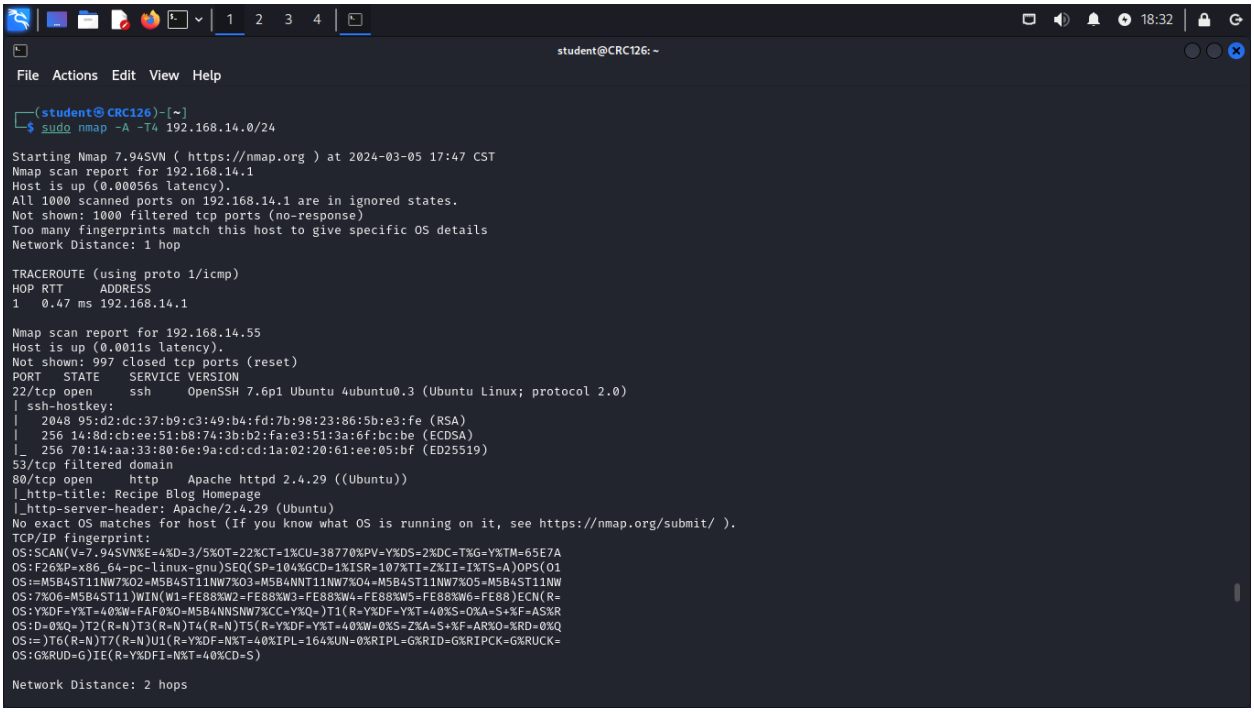
Vulnerability: Vulnerabilities detected.

Detection Method: Tools and methods used for detection (like, Nmap, Nikto, OpenVAS).

Nmap performs a SYN scan over all 65535 ports across all the hosts in the network. The -T4 option speeds up the scanning process.

```
student@CRC126: ~
File  Actions  Edit  View  Help
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

┌──(student㉿CRC126)-[~]
└─$ sudo nmap -sS -T4 192.168.14.0/24

[sudo] password for student:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 21:34 CST
Nmap scan report for 192.168.14.1
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.14.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.14.55
Host is up (0.00085s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE    SERVICE
22/tcp open     ssh
53/tcp filtered domain
80/tcp open     http

Nmap scan report for 192.168.14.102
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   filtered domain
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
```

Nmap Aggressive scan that includes service detection, OS detection, traceroute, and common scripts:



```
student@CRC126: ~
File  Actions  Edit  View  Help

┌──(student㉿CRC126)-[~]
└─$ sudo nmap -A -T4 192.168.14.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 17:47 CST
Nmap scan report for 192.168.14.1
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.14.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.47 ms 192.168.14.1

Nmap scan report for 192.168.14.55
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:d2:dc:37:b9:c3:49:b4:fd:7b:98:23:86:5b:e3:fe (RSA)
|   256 14:8d:cb:ee:51:b8:74:3b:b2:fa:e3:51:3a:6f:bc:be (ECDSA)
|_  256 70:14:aa:33:80:6e:9a:cd:cd:1a:02:20:61:ee:05:bf (ED25519)
53/tcp filtered domain
80/tcp open     http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Recipe Blog Homepage
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/5%OT=22%CT=1%CU=38770%PV=Y%DS=2%DC=T%G=Y%TM=65E7A
OS:F26%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=Z%II=I%TS=A)OPS(O1
OS:=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW
OS:7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=
OS:Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
```

Nmap Scan results: -

IP Address	Identified Services	Vulnerable Services
192.168.14.1	All 1000 scanned ports are in ignored states.	N/A
192.168.14.55	- SSH (22/tcp): OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 HTTP (80/tcp): Apache httpd 2.4.29 (Ubuntu)	**SSH (OpenSSH 7.6p1** **HTTP (Apache 2.4.29)**
192.168.14.102	FTP (21/tcp): vsftpd 2.3.4 SSH (22/tcp): OpenSSH 4.7p1 Debian 8ubuntu1 Telnet (23/tcp): Linux telnetd SMTP (25/tcp): Postfix smtpd HTTP (80/tcp): Apache httpd 2.2.8 (Ubuntu) DAV/2 Samba (139/tcp, 445/tcp) MySQL (3306/tcp): MySQL 5.0.51a-3ubuntu5 PostgreSQL (5432/tcp): PostgreSQL DB 8.3.0 - 8.3.7 Others (rpcbind, nfs, vnc, etc.)	**FTP (vsftpd 2.3.4)**: Vulnerable to backdoor entry, CVE-2011-2523. **SSH (OpenSSH 4.7p1)**: Older version, potential vulnerabilities including username enumeration (CVE-2018-15473) and others. **Telnet**: Insecure protocol, susceptible to interception and unauthorized access. **SMTP (Postfix)**: Older versions may be vulnerable to various attacks. **HTTP (Apache 2.2.8)**: Multiple vulnerabilities including CVE-2008-2364 (cross-site scripting), CVE-2009-1890 (mod_proxy reverse proxy bypass), etc. **Samba, MySQL, PostgreSQL.**

IP Address	Identified Services	Vulnerable Services
192.168.14.104	FTP (21/tcp): vsftpd 3.0.2 SSH (22/tcp): OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 SMTP (25/tcp): Postfix smtpd HTTP (80/tcp): Apache httpd 2.4.7 (Ubuntu) POP3, IMAP (110/tcp, 143/tcp): Dovecot pop3d, Dovecot imapd RPC, NFS (111/tcp, 2049/tcp) NetBIOS, SMB (139/tcp, 445/tcp): Samba smbd MySQL (3306/tcp): Unauthorized access PostgreSQL (5432/tcp): PostgreSQL DB 9.3.3 - 9.3.5 Others (CUPS, SSL/POP3, etc.)	**FTP (vsftpd 3.0.2)**: Anonymous FTP login allowed, which poses a security risk. **SSH (OpenSSH 6.6.1)**: Possible vulnerabilities include CVE-2016-0777 and CVE-2016-0778 (roaming feature vulnerabilities). **SMTP (Postfix)**: Some older versions may be vulnerable to various attacks. **HTTP (Apache 2.4.7)**: Known vulnerabilities such as CVE-2014-0226 (mod_status memory access), CVE-2014-0118 (mod_deflate denial of service), and others. **Dovecot (POP3, IMAP)**: Ensure secure configurations and check for updates. **MySQL, PostgreSQL**: Unauthorized access indicates misconfigurations or vulnerabilities; ensure strong authentication and update to the latest versions. **Samba.**

Summary of some vulnerabilities: -

192.168.14.1

No specific vulnerabilities were reported in the scan results for this IP.

192.168.14.55

No specific vulnerabilities were identified for this host. It mainly revealed open ports and services but didn't detail exploitable vulnerabilities directly.

192.168.14.102

1. FTP (vsftpd 2.3.4): Known for a backdoor vulnerability (CVE-2011-2523).
2. SSH (OpenSSH 4.7p1 Debian 8ubuntu1): May have vulnerabilities specific to its version; newer versions have fixed several issues.
3. Telnet (Linux telnetd): Telnet is inherently insecure as it transmits data in plaintext, making it susceptible to eavesdropping.

4. HTTP (Apache httpd 2.2.8): Older versions of Apache have multiple vulnerabilities. For instance, CVE-2007-6750 is a Slowloris DOS attack vulnerability.
5. Samba (smbd 3.X - 4.X): Certain versions of Samba are vulnerable to various exploits, including remote code execution vulnerabilities.
6. Bindshell (Metasploitable root shell on 1524/tcp): Indicates a backdoor access vulnerability.
7. IRC (UnrealIRCd): Known vulnerabilities include backdoors and remote execution flaws, especially in older versions.

192.168.14.104

1. FTP (vsftpd 3.0.2): Generally considered stable, but configuration and anonymous access should be reviewed for potential security issues.
2. SSH (OpenSSH 6.6.1p1): Vulnerabilities like CVE-2016-0777 and CVE-2016-0778 (roaming feature vulnerabilities) could affect this version.
3. SMTP (Postfix smtpd): While generally secure, configuration and known vulnerabilities for the specific version should be checked.
4. HTTP (Apache httpd 2.4.7): Known for vulnerabilities like CVE-2014-0226 (mod_status memory access issue) and CVE-2014-0118 (mod_deflate module DOS).
5. Samba (smbd 3.X - 4.X): Vulnerable to various exploits depending on the version, including potential for remote code execution.
6. PostgreSQL (9.3.3 - 9.3.5): Specific vulnerabilities should be checked, as database versions often have targeted exploits.
7. Apache Tomcat/Coyote JSP engine 1.1 on port 8080: Known for various vulnerabilities depending on configuration and version.

Software used to detect vulnerable services: -

Nmap

For Nmap: - Basic Vulnerability Scan I used command: --script=vuln 192.168.14.0/24

```
┌──(student㉿CRC126)-[~]
└─$ nmap --script=vuln 192.168.14.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 22:11 CST
Stats: 0:05:46 elapsed; 252 hosts completed (4 up), 4 undergoing Script Scan
NSE Timing: About 99.91% done; ETC: 22:17 (0:00:00 remaining)
Stats: 0:05:46 elapsed; 252 hosts completed (4 up), 4 undergoing Script Scan
NSE Timing: About 99.91% done; ETC: 22:17 (0:00:00 remaining)
Stats: 0:06:02 elapsed; 252 hosts completed (4 up), 4 undergoing Script Scan
NSE Timing: About 97.83% done; ETC: 22:17 (0:00:00 remaining)
Stats: 0:06:06 elapsed; 252 hosts completed (4 up), 4 undergoing Script Scan
NSE Timing: About 97.83% done; ETC: 22:17 (0:00:00 remaining)
Nmap scan report for 192.168.14.55
Host is up (0.00058s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
22/tcp open     ssh
53/tcp filtered domain
80/tcp open     http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap scan report for 192.168.14.102
Host is up (0.015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
```

I also used Metasploit Framework to search for vulnerable services: -

```
student@CRC126: ~
File  Actions  Edit  View  Help

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
         '    dB'                    BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                 dBBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                 dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP     dBP
                           --o--     dBP    dBP    dBP    dB'.BP dBP    dBP
                             |      dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                   .
              .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.3.54-dev                          ]
+ -- --=[ 2394 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsFTPd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
msf6 >
```

```
student@CRC126: ~
File  Actions  Edit  View  Help

                                                                   .
              .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.3.54-dev                          ]
+ -- --=[ 2394 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsFTPd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
msf6 > search SSL POODLE

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssl/ssl_version   2014-10-14       normal  No     SSL/TLS Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssl/ssl_version

msf6 >
```

```
student@CRC126: ~
File  Actions  Edit  View  Help
msf6 > search SSH

Matching Modules
================

   #   Name                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                      ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                        2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution      2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                          normal     No     Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh                   2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                     2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc          2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalat
ion Code Execution
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey           2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   7   auxiliary/scanner/ssh/cerberus_sftp_enumusers             2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   8   auxiliary/dos/cisco/cisco_7937g_dos                       2020-06-02       normal     No     Cisco 7937G Denial-of-Service Attack
   9   auxiliary/admin/http/cisco_7937g_ssh_privesc              2020-06-02       normal     No     Cisco 7937G SSH Privilege Escalation
   10  exploit/linux/http/cisco_asax_sfr_rce                     2022-06-22       excellent  Yes    Cisco ASA-X with FirePOWER Services Authenticated Command
Injection
   11  auxiliary/scanner/http/cisco_firepower_login                               normal     No     Cisco Firepower Management Console 6.0 Login
   12  exploit/linux/ssh/cisco_ucs_scpuser                       2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   13  auxiliary/scanner/ssh/eaton_xpert_backdoor                2018-07-18       normal     No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   14  exploit/linux/ssh/exagrid_known_privkey                   2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   15  exploit/linux/ssh/f5_bigip_known_privkey                  2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   16  exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684  2022-10-10  excellent  Yes    Fortinet FortiOS, FortiProxy, and FortiSwitchManager authe
ntication bypass.
   17  auxiliary/scanner/ssh/fortinet_backdoor                   2016-01-09       normal     No     Fortinet SSH Backdoor Scanner
   18  post/windows/manage/forward_pageant                                        normal     No     Forward SSH Agent Requests To Remote Pageant
   19  exploit/windows/ssh/freeftpd_key_exchange                 2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overf
low
   20  exploit/windows/ssh/freesshd_key_exchange                 2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overfl
ow
   21  exploit/windows/ssh/freesshd_authbypass                   2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   22  auxiliary/scanner/http/gitlab_user_enum                   2014-11-21       normal     No     GitLab User Enumeration
   23  exploit/multi/http/gitlab_shell_exec                      2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   24  exploit/linux/ssh/ibm_drm_a3user                          2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   25  post/windows/manage/install_ssh                                            normal     No     Install OpenSSH for Windows
   26  payload/generic/ssh/interact                                               normal     No     Interact with Established SSH Connection
   27  post/multi/gather/jenkins_gather                                           normal     No     Jenkins Credential Collector
   28  auxiliary/scanner/ssh/juniper_backdoor                    2015-12-20       normal     No     Juniper SSH Backdoor Scanner
```

I checked the online database with CVE.org also: -

CVE-2015-4000 PUBLISHED

View JSON

Important CVE JSON 5 Information +

Assigner: MITRE Corporation
Published: 2015-05-21 **Updated:** 2022-12-13

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

Product Status

Learn About the Versions Section +

Information not provided

CVE-2014-3566 PUBLISHED

View JSON

Important CVE JSON 5 Information +

Assigner: Red Hat, Inc.
Published: 2014-10-15 **Updated:** 2021-11-05

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Product Status

Learn About the Versions Section +

Information not provided

CVE-2015-4000 PUBLISHED

View JSON

Important CVE JSON 5 Information +

Assigner: MITRE Corporation
Published: 2015-05-21 **Updated:** 2022-12-13

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

Product Status

Learn About the Versions Section +

Information not provided

Below is an explanation of each vulnerability, providing insights into why these services may be considered vulnerable and potentially exploitable:

1. FTP (vsftpd 2.3.4)

Vulnerability: Backdoor vulnerability (CVE-2011-2523)

Details: This specific version of vsftpd was compromised, and a backdoor was introduced in the software. When triggered, this backdoor allows an attacker to gain remote command execution on the affected server. The vulnerability is activated by attempting to log in with a username containing a smiley face :). Once the backdoor is opened, it listens on TCP port 6200 for incoming connections, providing shell access to the attacker.

Mitigation: Upgrade to a version of vsftpd that does not contain this backdoor.

2. **SSH (OpenSSH 4.7p1 Debian 8ubuntu1)**

Vulnerability: Multiple vulnerabilities due to version

Details: This version of OpenSSH is outdated and may contain several vulnerabilities that have been fixed in later releases. These vulnerabilities range from information disclosure to authentication bypasses and code execution. The specific vulnerabilities would depend on the exact version and compilation options.

Mitigation: Upgrade to the latest version of OpenSSH and ensure that all patches have been applied.

3. Telnet (Linux telnetd)

Vulnerability: Inherent protocol weakness

Details: Telnet transmits all data, including passwords, in plaintext. This makes it susceptible to interception and eavesdropping, especially if the communication is not encrypted with a secondary protocol. The use of Telnet over an unsecured network exposes sensitive information to anyone capable of packet sniffing.

Mitigation: Replace Telnet with SSH or another secure protocol that encrypts the communication, preventing eavesdropping and ensuring data confidentiality and integrity.

4. HTTP (Apache httpd 2.2.8)

Vulnerability: Slowloris DOS attack vulnerability (CVE-2007-6750)

Details: The Slowloris attack allows a single machine to take down another machine's web server with minimal bandwidth by opening multiple connections to the web server and keeping them open as long as possible. Apache httpd 2.2.8 is vulnerable to such attacks, which can lead to a denial of service.

Mitigation: Upgrade to a newer version of Apache that includes fixes for Slowloris and other DOS vulnerabilities. Consider implementing rate limiting and connection timeouts.

5. Samba (smbd 3.X - 4.X)

Vulnerability: Remote code execution vulnerabilities

Details: Certain versions of Samba are vulnerable to remote code execution, allowing an attacker to execute arbitrary code on the affected system. Examples include CVE-2017-7494, where a malicious client can upload a shared library to a writable share, and then cause the server to load and execute it.

Mitigation: Upgrade to a version of Samba that has been patched against known vulnerabilities.

6. Bindshell (Metasploitable root shell on 1524/tcp)

Vulnerability: Backdoor access vulnerability

Details: The presence of a bind shell listening on a port like 1524/tcp is indicative of a backdoor, potentially installed by an attacker for easy access. This allows anyone who knows about it to connect and gain shell access, typically with root privileges.

Mitigation: Identify and remove any unauthorized services or applications. Conduct a thorough investigation to understand how the backdoor was installed and address any security breaches.

7. IRC (UnrealIRCd)

Vulnerability: Backdoors and remote execution flaws

Details: Older versions of UnrealIRCd have been found to contain backdoors and vulnerabilities that allow remote code execution. For example, a known issue allowed attackers to execute arbitrary commands due to improperly sanitized input.

Mitigation: Upgrade to a secure and updated version of UnrealIRCd. Regularly monitor and apply security patches. Ensure that IRC services, if necessary, are run with the least privileges to limit the impact of a compromise.