Pen-Test Report

Targeted Network: [redacted]

May want to expand on [redacted] to get a better picture

1. Introduction

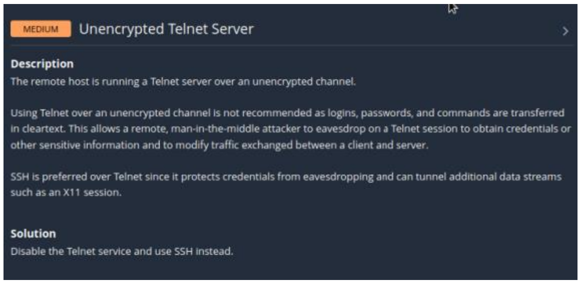
In this penetration test report, we are performing an information gathering and a reconnaissance on the network [redacted]. We want to detect the number of hosts on the network, the open ports, the services run and their versions, the operating systems, and establish a list of vulnerabilities. We also want to have a topology of the entire network.

2. Reconnaissance Results

Ip address & DNS names

Host #1: [redacted]

- Operating system: Oracle Virtual Box
  - Unix
  - Linux
- CPE:
  - Linux_kernel
- Software versions
  - Bay Networks Baystack 450 switch → version3.1.0.22
- Open ports
  - 23/TCP → telnet → version: Linux telnetd
  - 21/TCP → ftp → version: vsftpd 3.0.3
- Traceroute:
  - Hop 1:
    - RTT: 7.45 ms
    - Address: [redacted]
  - Hop 2:
    - RTT: 7.50 ms
    - Address: [redacted]
- Vulnerabilities discovered
  - Total Vulnerabilities: 17
    - 1 Medium
    - 16 Info
  - Important vulnerabilities:
    - Unencrypted Telnet Server:
      - Risk factor: Medium
      - CVSS v3.0 Base Score 6.5



MEDIUM Unencrypted Telnet Server

Description

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

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

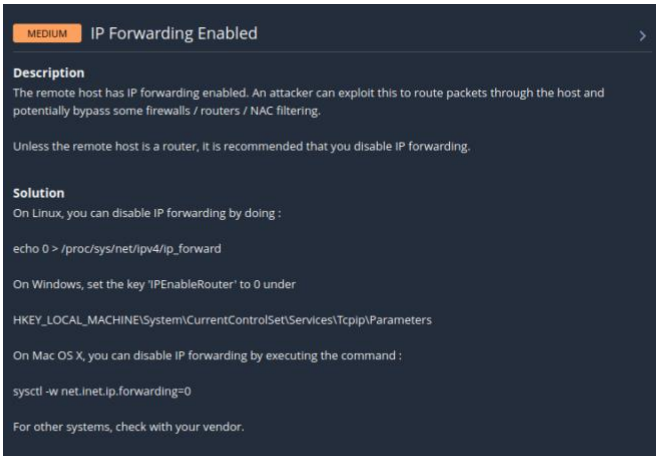
Solution

Disable the Telnet service and use SSH instead.

Fig1. Result from Nessus

Host #2: [redacted] (Web Server)

- Operating System: Oracle Virtual Box, QEMU, Bay Networks embedded
- Services running
  - Host: localhost
- Software versions
  - Bay Networks Baystack 450 switch → version3.1.0.22
- Open ports:
  - 80/TCP → http → version: Apache httpd 2.4.41 (Ubuntu)
  - 443/TCP → https → version: Apache httpd 2.4.41
- Traceroute:
  - Hop 1:
    - RTT: 4.75 ms
    - Address: [redacted]
  - Hop 2:
    - RTT: 4.83 ms
    - Address: [redacted]
- Vulnerabilities discovered
  - Total Vulnerabilities: 23
    - 1 Medium
    - 22 Info
  - Important vulnerabilities:
    - IP Forwarding Enabled:
      - Risk factor: Medium
      - CVSS v3.0 Base Score 6.5



MEDIUM IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

On Mac OS X, you can disable IP forwarding by executing the command :

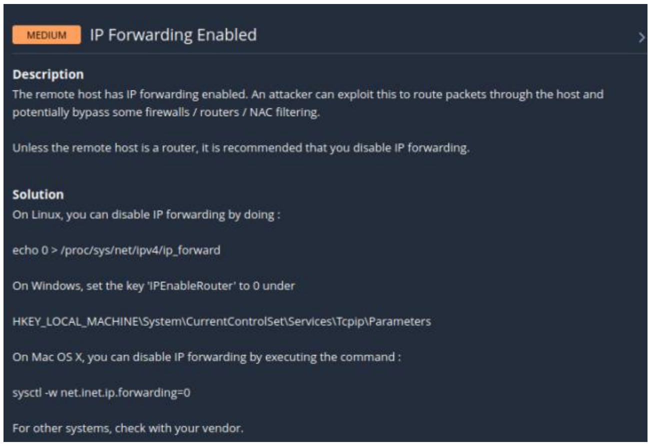
```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Host #3: [redacted] (Database)

- Operating System: Oracle Virtual Box, QEMU, Bay Networks embedded
- Software versions
    - Bay Networks Baystack 450 switch → version 3.1.0.22
- Open ports:
    - 3306/TCP → mysql → version: MYSQL 8.0.22
        - Protocol: 10
        - Version: 8.0.22
        - Thread ID: 1265
        - Capabilities Flag: 65535
        - Status: Autocommit
        - | Salt: \x12L\x04Rh\x1B`FK@p#r \x19k\#R3
        - |_ Auth Plugin Name: mysql_native_password
        - Some Capabilities:
            - Support41Auth
            - IgnoreSigpipes, FoundRows
            - SupportsLoadDataLocal
            - IgnoreSpaceBeforeParenthesis
            - ConnectWithDatabase, SwitchToSSLAfterHandshake
            - DontAllowDatabaseTableColumn
    - 443/TCP → https → version: Apache httpd 2.4.41
- Traceroute:
    - Hop 1:
        - RTT: 2.91 ms
        - Address: [redacted]
    - Hop 2:
        - RTT: 3.17 ms
        - Address: [redacted]
- Vulnerabilities discovered
    - Total Vulnerabilities: 12

        - 1 Medium
        - 11 Info
    - Important vulnerabilities:
        - IP Forwarding Enabled:
            - Risk factor: Medium
            - CVSS v3.0 Base Score 6.5



IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

On Mac OS X, you can disable IP forwarding by executing the command :

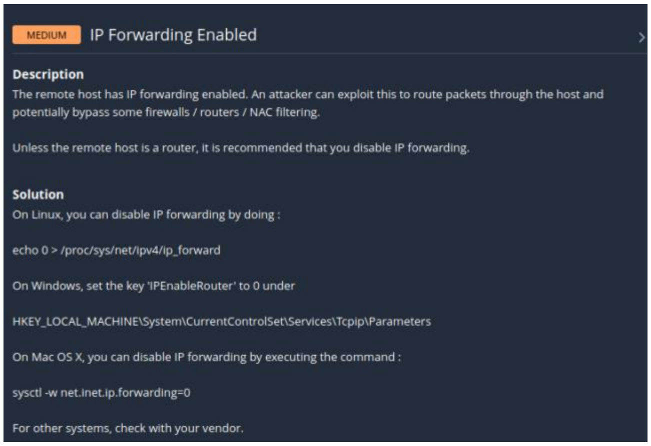
```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Host #4: [redacted]

- Operating system: Oracle Virtual Box
    - Linux
- CPE:
    - Linux_kernel
- Software versions
    - Bay Networks Baystack 450 switch → version: 3.1.0.22
- Open ports
    - 23/TCP → telnet → version: Linux telnetd
- Traceroute:
    - Hop 1:
        - RTT: 9.96 ms
        - Address: [redacted]
    - Hop 2:
        - RTT: 10.03 ms
        - Address: [redacted]
- Vulnerabilities discovered
    - Total Vulnerabilities: 12
        - 2 Medium
        - 10 Info
    - Important vulnerabilities:
        - IP Forwarding Enabled:
            - Risk factor: Medium

        - CVSS v3.0 Base Score 6.5



IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

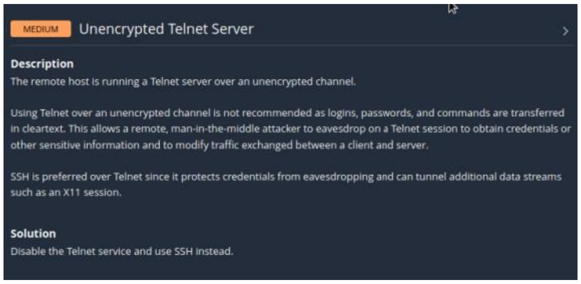
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

    - Unencrypted Telnet Server:
        - Risk factor: Medium
        - CVSS v3.0 Base Score 6.5



Unencrypted Telnet Server

Description

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

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

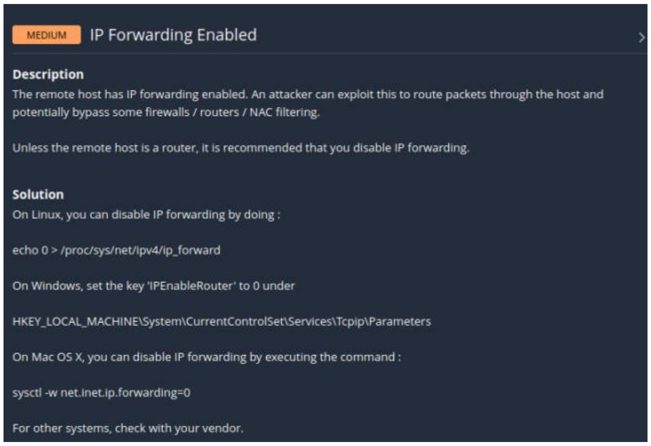
Solution

Disable the Telnet service and use SSH instead.

Host #5: [redacted]

- Operating system: Oracle Virtual Box
    - Linux
- CPE:
    - Linux_kernel
- Software versions
    - Bay Networks Baystack 450 switch → version: 3.1.0.22
- Open ports
    - 23/TCP → telnet → version: Linux telnetd
- Traceroute:
    - Hop 1:
        - RTT: 4.51 ms
        - Address: [redacted]
    - Hop 2:
        - RTT: 4.61 ms
        - Address: [redacted]
- Vulnerabilities discovered
    - Total Vulnerabilities: 12
        - 2 Medium
        - 10 Info

- Important vulnerabilities:
  - IP Forwarding Enabled:
    - Risk factor: Medium
    - CVSS v3.0 Base Score 6.5



IP Forwarding Enabled

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

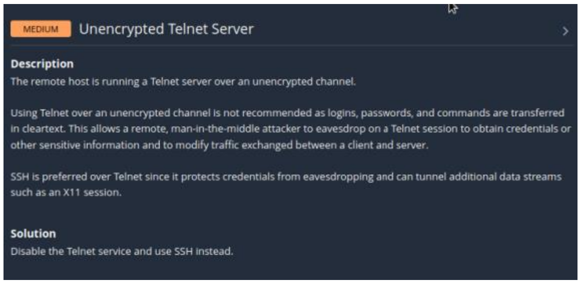
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

On Mac OS X, you can disable IP forwarding by executing the command :

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

  - Unencrypted Telnet Server:
    - Risk factor: Medium
    - CVSS v3.0 Base Score 6.5



Unencrypted Telnet Server

Description

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

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Host #6: [redacted]

- Operating system:;
  - Agfa DryStar 5500 printer, D-Link DP-300U, DP-G310CPE:
  - Hamlet HPS01UU print server, TAHOE 8216 power management System
- Traceroute:
  - Hop 1:
    - RTT: 7.13 ms
    - Address: [redacted]
  - Hop 2:
    - RTT: 7.50 ms
    - Address: [redacted]
- Vulnerabilities discovered
  - Total Vulnerabilities: 5
    - 1 Medium
    - 4 Info
  - Important vulnerabilities:
    - IP Forwarding Enabled:

            - Risk factor: Medium

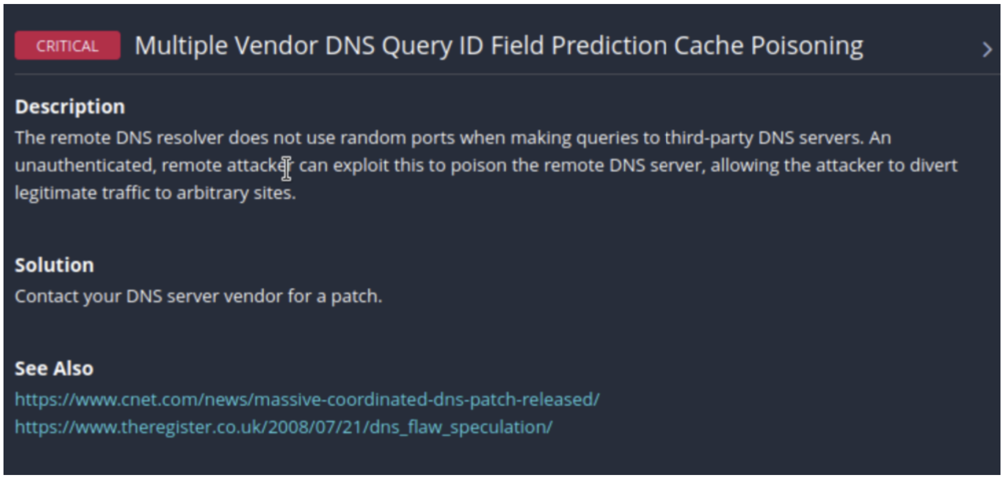
Host #7: [redacted]

- Operating system: Oracle Virtual Box
    - Linux
    - Unix
- CPE:
    - Linux_kernel
- Device Type: bridge | general purpose | switch
- Software versions
    - Bay Networks Baystack 450 switch → version: 3.1.0.22
- Open ports
    - 21/TCP → ftp → version: vsftpd 3.0.3
    - 22/TCP → ssh → version: OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
        - Host Key:

          | 2048 4b6fe94a8e5b2b4d123494489bfc051a (RSA)
          | 256 3761b8e907af1cf16a4994eade19cfb4 (ECDSA)
          |_ 256 5cc2487e04511dba89a1ca4a55904fe6 (ED25519)
    - 23/TCP → telnet → Linux telnetd
    - 53/TCP → domain → version: ISC BIND 9.10.3-P4-Ubuntu
    - 80/TCP → http → version: Apache httpd 2.4.18
    - 3128/TCP → squid-http → version: Squid http proxy 3.5.12
- Traceroute:
    - Hop 1:
        - RTT: 3.94 ms
        - Address: [redacted]
    - Hop 2:
        - RTT: 3.99 ms
        - Address: [redacted]

- Vulnerabilities discovered
    - Total Vulnerabilities: 50
        - 1 Critical
        - 2 Medium
        - 47 Info
    - Important vulnerabilities:
        - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
            - Risk Factor: Critical

    - CVSS v3.0 Base Score: 9.1



CRITICAL Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Description

The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

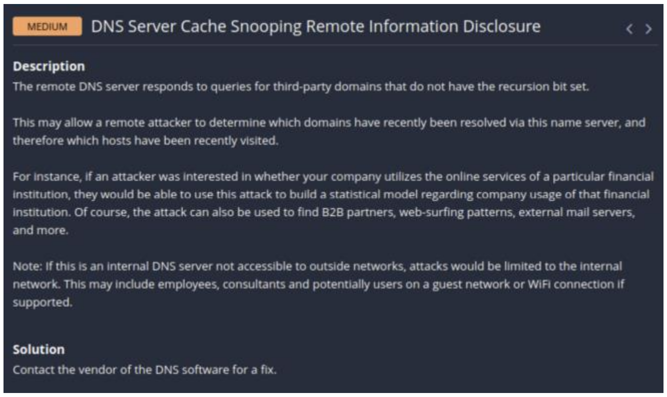
Solution

Contact your DNS server vendor for a patch.

See Also

https://www.cnet.com/news/massive-coordinated-dns-patch-released/
https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

- DNS Server Cache Snooping Remote Information Disclosure:
    - Risk factor: Medium
    - CVSS v3.0 Base Score 5.3



MEDIUM DNS Server Cache Snooping Remote Information Disclosure

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

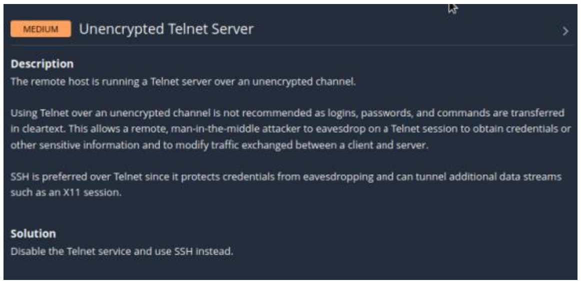
For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution

Contact the vendor of the DNS software for a fix.

- Unencrypted Telnet Server:
    - Risk factor: Medium
    - CVSS v3.0 Base Score 6.5



MEDIUM Unencrypted Telnet Server

Description

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

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Host #8: [redacted] (Printer)

- Operating system: Oracle Virtual Box
  - Oracle Virtual Box
  - Kodak ESP C310 printer
- Open ports
  - 445/TCP → Microsoft-ds
  - 631/TCP → ipp
  - 3306/TCP → MySQL
  - 8080/TCP → http-proxy
- TRACEROUTE (using port 80/tcp)

  HOP RTT ADDRESS

  - 1 3.97 ms [redacted]
  - 2 ... 6
  - 7 995.75 ms [redacted]
- Vulnerabilities discovered
  - Total Vulnerabilities: 5
    - 1 Medium
    - 4 Info
  - Important vulnerabilities:
    - IP Forwarding Enabled:
      - Risk factor: Medium

Other hosts discovered on [redacted]/16

Host #9: [redacted]

- Open ports
  - 80/TCP → http
  - 443/TCP → https

Host #10: [redacted]

- Open ports
  - 22/TCP → ssh
  - 80/TCP → http
  - 443/TCP → https

Host #11: [redacted]

- Open ports
  - 111/TCP → rpcbind
  - 80/TCP → http
  - 443/TCP → https
  - 445/TCP → Microsoft-ds

Host #12: [redacted]

- Open ports
    - 22/TCP → ssh
    - 2049/TCP → nfs

Host #13: [redacted]

- Open ports
    - 80/TCP → http
    - 443/TCP → https
    - 21/TCP → ftp
    - 22/TCP → ssh
    - 111/TCP → rpcbind
    - 2049/TCP → nfs
    - 3309/TCP → mysql

Host #14: [redacted]

- Open ports
    - 53/TCP → domain
    - 88/TCP → Kerberos-sec
    - 135/TCP → msrpc
    - 389/TCP → ldap
    - 445/TCP → Microsoft-ds
    - 464/TCP → kpasswd5
    - 593/TCP → http-rpc-epmap
    - 636/TCP → ldapssl
    - 3268/TCP → globakcatLDAP
    - 3269/TCP → globakcatLDAPssl

Commands Used

- nmap -A "ip address"
- nmap -O "ip address"
- nmap -sT "subnet"
- nmap -sS "subnet"
- nmap -Pn "subnet"
- ping "ip address"
- dig "ip address"

Tools Used

- Nessus
- Google Search Engine

3. Conclusion

During this pen test, we have discovered 8 main hosts having many of their ports opened. The vulnerabilities discovered ranged from simple Information to medium and Critical. We've found servers, web servers, one database, and printers on the network.