Report

For this lab, your team must submit a report with the following information:

1. **What services did you disable on your Linux machine? What are their normal uses?**

➔ Based on list of processes which were listening and TCP/UDP ports, I choose the ‘master’ – postfix and the ‘dovecot’ processes to disable

```
team@nslabu:~$ sudo netstat -tulpn
[sudo] password for team:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      1067/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      1067/dovecot
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      894/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1209/master
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      1067/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      1067/dovecot
tcp6       0      0 :::110                  :::*                    LISTEN      1067/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      1067/dovecot
tcp6       0      0 :::22                   :::*                    LISTEN      894/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1209/master
tcp6       0      0 :::993                  :::*                    LISTEN      1067/dovecot
tcp6       0      0 :::995                  :::*                    LISTEN      1067/dovecot
udp        0      0 0.0.0.0:36795           0.0.0.0:*                           1095/openvpn
udp        0      0 0.0.0.0:68              0.0.0.0:*                           822/dhclient3
```

The normal use of ‘master’ process is to run Postfix daemons to send or receive messages via the network, daemons to deliver mail locally, etc. These daemons are created on demand up to a configurable maximum number per service.
And the dovecot is the email server for linux systems. It supports the mbox,maildir formats and allows modifications of mailboxes and indexes.

2. **Simple TCP/IP Services provides the Daytime service. How could the UDP version of this service be used in denial of service attacks against third parties? How could this service be used in conjunction with the UDP echo service to create a datagram loop?**

➔ The Daytime service uses UDP on port 13.UDP server sends the data and time to the host which requested it in the form of the datagram. This version of daytime service is vulnerable to Denial of Service attack. There is a chance by a third party to use any of the available trouble shooting tool to generate a huge number of UDP datagram packets with the daytime service information by spoofing addresses. This huge inflow of datagrams to the UDP server will exhaust the system resources and bandwidth which leads to DoS to the intended users.

Echo service send the datagrams received from the source back to the source. So when the Daytime service is used along with Echo, a datagram loop is established, wherein the UDP server sends the date and time datagram to the host and since the host uses Echo service, it redirects it back to the UDP server and this repeats for each datagram sent by UDP server. This to and fro transmission of the datagrams between the UDP server and system which has requested Daytime service will cause a loop to be established and it is difficult to resolve this issue.

3. **What kinds of information could an attacker obtain anonymously from your Windows 2003 Server if NULL sessions were fully enabled?**

➔ A null session is an anonymous connection with no authentication information. If the NULL sessions were fully enabled, an attacker can gain one or more of the following information of the Windows system since any user created will have the same permissions as of the other users and has accessibility to many of the critical information.

- Can connect to IPC $ of the server and can access the computer's registry and can change registry's keys.
- Can obtain user IDs, groups, administrators and share names using enumeration
- Can fetch details of the password updated dates, last login dates and account policy which gives the attacker enough information to crack the windows passwords of the users.
- Can also obtain information of the drives.

4. **When using SYN cookies, if the defending system doesn't store state about SYNs that were replied to previously, what's to stop an attacker from just sending an ACK outright to start a connection?**

➔ If the defending system doesn't store states about the SYNs, it can still stop the attacker from just sending the ACK outright to start a connection. System will have the details in the connection table where it can check if the received ACK response from attacker is correct or not by decrypting the ACK message. The table store the details of the source address, destination address, source port and destination ports. It verifies whether these details in the received ACK matches the ones in the table. If it already exists, it means that there is an open connection already and avoids the attacker in starting a new connection with the details it has. So there won't be SYN flood on the server.

5. **What kinds of negative impacts do SYN cookies have on TCP connections?**

➔ Negative impacts:

- The size of the Sequence number field is fixed to 32, so this might hamper higher performance of the TCP options.
- The TCP window scaling does not work in this case and becomes less efficient to heavy networks.
- Selective ACK does not work. So the data recipient cannot inform the source about the data segments that have reached successfully and ask the server to retransmit only the lost segments. This makes TCP connection less efficient.
- The attacker can watch the series of SYN cookies being sent, can guess the next cookie in the sequence and spoof the connection from that host.
- Server can only have 8 unique MSS values as only 3 bits define MSS

6. **What SYN flood mitigation settings did you apply to your Windows server? Why did you choose these settings?**

➔ Settings applied to the Windows server
Maximum HTTP requests per minute per IP address -> Set to 700

Maximum TCP connect requests per minute per IP address-> 700
Maximum concurrent TCP connections per IP address - >200

I chose these settings because if any attacker tries to do a SYN attack, he will try to send a huge number of TCP connect requests to the server and exhaust the server resources. Applying the above mentioned settings will help the server to keep the resources idle for actual connections and ensure that the DoS attack does not happen, thereby making all the resources available.