Ruchi Pawar

Overview Of Transport Layer:

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment.

Transport Layer Protocol:

- UDP (User Datagram Protocol)
- TCP(Transmission Control Protocol)
- SCTP (Stream Control Transmission Protocol)

UDP:

UDP is one of the simplest transport layer protocol which provides non sequenced data transmission functionality.

UDP is consider as connection less transport layer protocol.

This type of protocol is referred to be used when speed and size are more important than reliability and security.

It is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data received from the upper layer.

User datagram is the packet constructed by the UDP protocol.

TCP:

TCP stands for Transmission Control Protocol.

TCP is a connection-oriented transport layer protocol.

TCP explicitly defines connection establishment, data transfer, and connection tear down phases to provide connection oriented service for data transmission.

TCP is the most commonly used transport layer protocol..

SCTP:

SCTP stands for Stream Control Transmission Protocol.

SCTP is one of the connection oriented tranport layer protocols.

It allows transmitting of data between sender and receiver in full duplex mode.

This protocol makes it simpler to build connection over wireless network and to control multimedia data transmission.

Types Of Reconnaissance attacks:

There are three types of reconnaissance attacks. These are social, public, and software. Let's discuss these types in detail.

Social reconnaissance attacks

In this type of attack, a hacker uses social engineering to gather information about the target. Users share a lot of personal and business information on social networking sites. A hacker can use social networking sites to gather information about the target. For example, if the target is a company, the hacker can use social networking sites to reveal information about the company's employees.

A hacker can use honey trap techniques to lure an employee. Once the employee accepts the friend request of the hacker, the hacker starts the next step. In the next step, the hacker convinces the employee to reveal information about his business. For example, the hacker may provide technical support to the employee on his project. Or the hacker may offer some monetary reward for disclosing information about the company.

To reduce social reconnaissance attacks, a company must train its employees about what information they cannot share with others within and outside the company. Employees should never share sensitive information on any social platform. If an employee

shares any confidential information with unknown persons or outside users, the company must take appropriate action against the employee.

Public reconnaissance attacks

In this type of attack, a hacker collects information about the target from public domains. Companies share location and business model information on their websites. A hacker can use this information to determine the location of the target. From this information, a hacker can also determine what kind of infrastructure the target uses. For example, most web hosting companies share information about their servers and security equipment. Companies share this information to attract new customers and gain the trust of existing customers. Hackers can use this information to find vulnerabilities in the company's network.

To mitigate public reconnaissance attacks, companies should not share confidential information on public platforms. For business requirements, if a company wants to share information about its infrastructure, instead of sharing exact hardware information, it should share generic information. Generic information will fulfill the business requirement. From generic information, a hacker can't guess the product information. For example, if a company uses the Cisco Firepower 4100 Firewall, it may publish that we use the Cisco Firewall.

Software reconnaissance attacks

In this type of attack, a hacker uses software tools to gather information about the target. Operating systems and software

packages include many tools and utilities for debugging and troubleshooting. A hacker can use them to collect information about the network and its resources. For example, a hacker can use the **nslookup** command to perform a DNS lookup. The **nslookup** command resolves an IP address from a fully qualified domain name. Once the hacker knew the domain name of the business, the hacker can use the who is database to reveal detailed information about domain owners, mail servers, contact information, authoritative DNS servers, etc.

In the next step, the hacker can use the **ping** command. The **ping** command sends packets to the target host. If the target host is live, the host replies to the packets. Reply packets verify that the target host is live. The following image shows the sample output of the **ping** command.

Case Study Of Reconnaissance attacks :

This case study chains together several of the items learned within the chapter to perform a successful scan of a network. This case study trails Evil Jimmy the Hacker as he scans a small company called Little Company Network (LCN). He uses DNS to gather information before moving onto NMap for some scanning as he attempts to start his diagramming of the network.

The scene is set as LCN rejects Evil Jimmy for a position. He is skilled in penetration testing, and because LCN obviously did not even read to the end of his rèsumè, Jimmy plans to make use of his skills in an unauthorized manner. Jimmy knows the DNS names of his target LCN.com, so he plugs his laptop into the

wall and begins his attack. Knowing that preparation is vital to a successful outcome, Jimmy starts by making a plan and gathering his tools. The following steps illustrate the execution.

1. Evil Jimmy heads straight for the company website and uses the Wget tool to download the entire website. He can later browse this information at his leisure to look for e-mail addresses, address information, and any other details about the company that might later prove useful.
2. Evil Jimmy uses SamSpade to discover the company address, contact, and registration information posted for the website at the time it was created. The following example displays these output details from SamSpade.

```
Registrant:
LITTLE COMPANY NETWORK
    100 NW JOHN OLSEN PLACE
    HILLSBORO, OR 97123
    US
    Domain Name: LCN.COM
    Administrative Contact, Technical Contact:
            Little Company Network jbates@LCN.COM
            100 NW JOHN OLSEN PL
            HILLSBORO, OR 97123
            US
            503-123-5555 fax: - 503-123-5555
```

```
16.          Record expires on 11-Apr-2005.
17.          Record created on 10-Apr-1997.
18.          Database last updated on 20-Mar-2005 17:16:56
   EST.
19.
20.          Domain servers in listed order:
21.
22.            NS1.SECURESERVERS.NET
       NS2.SECURESERVERS.NET
```

23. Using his Visual Route tool, Jimmy gets a general idea of where the web server is. As Figure 5-30 shows, the web server is in Seattle, Washington, so the address in Oregon is probably the office address with the web server being hosted elsewhere in Washington..

Figure 5-30 Visual Route Results

24. Armed with company address information, Evil Jimmy drives right over to the company office and plugs into the network to do a little scanning. (In the real world, this might or might not take place, but for the example, it works great.)

Note

Wireless access is becoming increasingly viable as a way into a company network without ever needing to physically "touch" their network.

25. Now that Jimmy has local network access, he can ping sweep the network. Using Pinger, Jimmy discovers several computers across the network. Figure 5-31 displays the computers on the network that respond to standard ICMP requests.

Figure 5-31 Pinger Results

26. Next, Jimmy begins port scanning computers to help enumerate details of which programs are running on each computer. Also, Jimmy uses the NMap **–O** switch to detect which operation system is running. The following example shows the output information:

```
C:\>NMap -sS -O 192.168.200.21,100

Interesting ports on Desk1 (192.168.200.21):
(The 1658 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
```

34. 135/tcp open msrpc
35. 139/tcp open netbios-ssn
36. 5713/tcp open proshareaudio
37. MAC Address: 08:00:46:F3:14:72
38. Device type: general purpose
39. Running: Microsoft Windows NT/2K/XP
40. *OS details: Microsoft Windows XP SP2*
41. NMap finished: 2 IP addresses (2 hosts up) scanned in 3.203 seconds
42.
43. Starting NMap 3.81 (http://www.insecure.org/NMap) at 2005-03-21 21:07
44. GMT
45. Standard Time
46. Interesting ports on WEB1 (192.168.200.100):
47. (The 1652 ports scanned but not shown below are in state: closed)
48. PORT STATE SERVICE
49. 23/tcp open telnet
50. 53/tcp open domain
51. 135/tcp open msrpc
52. 139/tcp open netbios-ssn
53. 445/tcp open microsoft-ds
54. 1025/tcp open NFS-or-IIS

```
1026/tcp open  LSA-or-nterm
1029/tcp open  ms-lsa
1031/tcp open  iad2
1433/tcp open  ms-sql-s
1434/tcp open  ms-sql-m
MAC Address: 00:50:56:EE:EE:EE
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows 2003 Server or XP SP2
```

64. Jimmy is finished scanning and leaves the building just as the networking team commences the search for the intruder. Fortunately for Jimmy, it took several minutes for the team to detect the scan before they could start searching for the guilty hacker.
65. Back in the comfort of his home, Evil Jimmy starts to collate the information into an easy-to-read diagram that displays computer addresses, services open, and operating systems on each.

To mitigate software reconnaissance attacks, an administrator can use the following techniques: -

Can disable all unused ports on servers.

Can use the masking service to hide sensitive information on the **who is** database.

Can use NAT to hide the internal structure of the network.

Can use software or hardware firewall to filter all specious traffic.

That's all for this tutorial. In this tutorial, we discussed what reconnaissance attacks are and how they work in detail.

Transport Layer Innovations for Future Networks

Call for Papers

The communication technologies used for Internet connectivity have radically changed since the 1980s, when the current design of the TCP/IP stack was introduced. Most of the traffic will soon be generated by mobile devices, connected to different generations of wireless Local Area Networks and cellular networks, which now can provide to end users a multi-gigabit-per-second data rate. Mobile devices are more and more heterogeneous, and support connectivity over different interfaces and networks. Similarly, the capacity of fixed and

backhaul networks has dramatically increased, thanks to advances in optical communications.

Submission Guidelines

Manuscripts should conform to the standard format as indicated in the Information for Authors section of the Manuscript Submission Guidelines. Please, check these guidelines carefully before submitting since submissions not complying with them will be administratively rejected without review.

All manuscripts to be considered for publication must be submitted by the deadline through Manuscript Central. Select the “April 2021/Transport Layer” topic from the drop-down menu of Topic/Series titles. Please observe the dates specified here below noting that there will be no extension of submission deadline.