OSI LAYER BASED ATTACK

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

OSI LAYER BASED ATTACKS

Today nearly every digital technology requires a network to communicate. Cell phones, Gadgets, Laptop, Desktop, tablets etc. There are several advantages of using the network model however, while using the technology at an edge it causes several disadvantages. Here disadvantages comes under different categories of attack occurred on each layer of OSI reference model.

In this presentation attacks are categorized layer wise and on each layer of OSI model there description are also mentioned along with Attack Risk and Skill Set required.

APPLICATION LAYER

Attack(s) Name	Attack(s) Details	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
Ddos	DDoS is a type of DOS attack where multiple compromised systems, targets a single system	LOIC, HOIC, Slow Loris, Anonymous Ddos	Windows / Linux	Low	High
Buffer Overflow	An anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations	Metasploit Framework	Linux	Medium	High
Cookies Manipulation	cookie manipulation arises when a script writes controllable data into the value of a cookie.	Temper Data, Hack bar (Firefox)	Windows / Linux	Medium	High
SQL Injection	An injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server	Havij, SQLMAP	Linux	Medium	High

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

APPLICATION LAYER(CONT'D...)

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
Parameter Tempering / Horizontal Cross Site Scripting	Parameter tampering is a form of Web-based attack in which certain parameters in the Uniform Resource Locator (URL) or Web page form field data entered by a user are changed without that user's authorization	Firefox plugins , Burp suite	Windows / Linux	Medium	High
Hidden Fields Manipulation	An attacker exploits a weakness in the server's trust of client-side processing by modifying data on the client-side, such as price information, and then submit it to the server	Firefox plugins , Burp suite	Windows / Linux	Low	High
Cookie Poisoning	Cookie poisoning attacks. are a process involving the manipulation and forging of cookies, designed to achieve illicit access to web applications.	Firefox plugins , Burp suite	Windows / Linux	High	High

PRESENTATION LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS required	Skill(s) Required	Attack Risk
Fake Certificates	A self signed or customized certificate used to mask instead of original certificate	Burp Suite	Windows / Linux	High	High
MiTM	An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.	ARP Spoofing, Eternal, ARP Poisoning, Wire shark	Windows / Linux	Medium	High
SSL Pinning	Technique used to ensure whether the Organization has binded their certificate key with the server	Burp Suite	Windows / Linux	Medium	High

SESSION LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
RTP Packets Interception	An Attack where the real-time media that is being transferred forms the 'RTP Payload' sniffed by a malicious user	ARP Spoofing, Ettercap, ARP Poisoning, Wireshark	Windows / Linux	High	High
NETBios Enumeration	Enumeration is used to gather the below Usernames, Group names Hostnames Network shares and services IP tables and routing tables Service settings and Audit configurations Application and banners SNMP and DNS Details	Netbios Enumerator / Super Scan	Windows	Medium	Medium
Session Hijacking	Attack is used to gain unauthorized access to information or services in a computer system.	Burp Suit, Hackbar	Windows / Linux	Medium	Medium
SSH Downgrade	SSH Downgrade attack by poisoning the ARP Cache of Hosts on a LAN.	Anonymous Login	Windows / Linux	Low	High

TRANSPORT LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
TCP Flooding	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.	TCP Flooding	Linux	Low	High
UDP Flooding	"UDP flood" is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams	UDP Flooding	Linux	Low	High

NETWORK LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
IP Spoofing	A hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network.	IP Spoofing	Windows / Linux	**Low**	**High**
ARP Spoofing (Man in the Middle)	A type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.	ARP Poisoning	Windows / Linux	**Low**	**High**
Packet Sniffing	An Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network.	WireShark	Windows / Linux	**Low**	**High**
ICMP Flooding	a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests	Yersinia	Linux	**Low**	**High**

NETWORK LAYER(CONT'D)

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
Smurf Attack	The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.	Smurf6	Linux	Low	High

DATA LINK LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
MAC Spoofing	Taking over someone identity already appeared on the network, MAC spoofing is duplicating the mac address of the original source and send data over the network	SMAC, mac hanger, Change Mac Address	Windows / Linux	Low	High
MAC Flooding	Broadcasting multiple MAC Addresses along with multiple source and destination MAC request.	Macof	Linux	Low	High
DHCP Starvation	DHCP starvation deals with the Client hardware address (CHADDR) - 16 Bytes, it tries to lease all of the DHCP addresses available in the DHCP scope	Yersinia	Linux	Low	High
DNS Spoofing		Cain n Abel	Windows	Low	High

DATA LINK LAYER (CONT'D...)

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
WIFI DE authentication	Sending SYN packet to the WIFI (SSID) by utilizing its MAC address and targeting the SSID for DE authentication	Airreplay-NG	Linux	Medium	High
802.1x Raw Packets	Sending 802.1x Raw packet over the network in order to compromise availability	Yersinia	Linux	Medium	Medium

PHYSICAL LAYER

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
RAM Data Extraction	Extracting data from including confidential information of Stored passwords from the memory, extracting passwords, email address from the memory	DumpIT	**Windows**	**Low**	**High**
Misusing of Infrared Technology	Infrared enabled devices are prone to be compromised by using a Mobile Application having infrared technology enabled in it.	SURE, PEEL Remote	**Android**	**Medium**	**High**
Mira Casting	Mira cast enabled devices allow an attacker to compromise SMART TV and published vulgar material from a ranged difference	Mira Cast	**Android**	**Medium**	**Mediuem**
Plugging a Portable Router	In an environment where DHCP and automated IP Assigning is in place , a portable router can extend the connection of the Physical network and can be used by the attackers.	Virtual Router, Portable AP	**Windows, Linux**	**Medium**	**Medium**

PHYSICAL LAYER (CONT'D...)

Attack(s) Name	Attack(s) Description	Tool(s) used	OS Required	Skill(s) Required	Attack Risk
Frequency Interception	Intercepting Different frequencies using SDR (Software defined radio) to intercept unencrypted communication	RF Analyzer	**Android, Windows**	**High**	**High**
Creating Physical Switching Loop	Using a LAN cable connected to two ports of the same switch can cause switching loop.	Straight Through cable	**None**	**Low**	**High**

THANK YOU