Interview data

Monday, November 27, 2023 12:26 PM

Network attack based on OSI LAYER :

OSI LAYER	Activity	Attack vector
7 Application layer	• User interface and software application • Web browsing, email communication, file transfer • Protocols like HTTP, SMTP, FTP	1. Malware injection 2. Phishing attacks 3. Application-level ddos attacks
6 Presentation layer	• Data encryption & decryption • Data compression & Expansion • Viewing compressed files	1. Data encoding/decoding vulnerabilities 2. Malicious code injection 3. Format strings attacks
5 Session layer	• Establishes, manages, and terminates connections • Manage session state • Video conferencing	1. Session hijacking 2. Brute force attacks 3. Session fixation attacks
4 Transport layer	• Ensure end to end data delivery • TCP and UDP Protocols • Error correction	1. Man in the middle 2. SYN/ACK Flooding 3. TCP/IP Vulnerabilities
3 Network layer	• Routing and addressing • Ipv4 and ipv6 routing protocols (like OSPF) • Subnet Configuration	1. IP Spoofing 2. Routing table manipulation 3. DDOS attacks
2 Data link layer	• Frames and error Detection/Correction • Ethernet, Wi-Fi and bridging	1. MAC address spoofing 2. ARP spoofing 3. VLAN hopping
1 Physical	• Physical medium and electrical /optical signaling • Ethernet cables, fiber optics and … • Radio waves in wireless links	1. Physical tampering 2. Wiretapping 3. Electromagnetic interface

Application :	Exploit
Presentation :	Phishing
Session:	Hijacking(XSS attacks, Session side jacking, Malware)
Transport:	Reconnaissance(TCP session hijack, Fraggle, SYN flood, Land attack)
Network:	MITM(Smurf attack, Ping of death, Teardrop)
Data link:	Spoofing (MAC spoofing, MAC flooding, VLAN hopping)
Physical:	Sniffing

Type of DNS attacks :

Volumetric Attacks:	A high volume of requests get sent from different devices to a target device, **focusing on the bandwidth**. UDP FLOOD
Protocol Attacks:	Exhausting a server's resources **by focusing on the protocols.** SYN FLOOD
Application Layer Attacks:	Focusing on the application layer of the server, these attacks are more sophisticated and difficult to detect. PING OF DEATH

Which difference between Layer 2 and 3 OSI MODEL ?

The Data Link Layer (Layer 2) is the second layer of the OSI model and is responsible for the reliable transfer of data between adjacent network nodes. It provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer 1. Layer 2 switches operate at this layer and **use MAC**

addresses and ARP to forward data packets between network segments.

The Network Layer (Layer 3) is the third layer of the OSI model and is **responsible for the delivery of data across multiple networks**. It provides the functional and procedural means of transferring variable-length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport Layer 1. Layer 3 switches operate at **this layer and use IP addresses to forward data packets between network segments**

WEB PENETRATION

Broken Access Control:	This category moves up from the fifth position and focuses on risks related to access control flaws.
Cryptographic Failures:	This category shifts up one position to #2 and focuses on failures related to cryptography which often leads to sensitive data exposure or system compromise.
Injection:	This category slides down to the third position and includes risks related to injection flaws.
Insecure Design:	This is a new category for 2021, with a focus on risks related to design flaws.
Security Misconfiguration:	This category moves up from #6 in the previous edition and focuses on risks related to misconfiguration.
Vulnerable and Outdated Components:	This category moves up from #9 in 2017 and focuses on risks related to using components with known vulnerabilities.
Identification and Authentication Failures:	This category is sliding down from the second position and includes risks related to identification failures.
Software and Data Integrity Failures:	This category is new for 2021 and focuses on risks related to software and data integrity.
Server-Side Request Forgery:	This category is new for 2021 and focuses on risks related to server-side request forgery.
Security Logging and Monitoring Failures:	This category is new for 2021 and focuses on risks related to security logging and monitoring failures

Security Misconfiguration:

-Weak Password Attack
    Default Passwords
    Brute force / Dictionary Attack
    Spray Attack
-Prevent Stack trace errors
-Prevent Verb tampering
-Implement HTTP Only
-Force Browsing

SQL Injection

1. In-Band Sqli
2. Union Based
3. Error Based

XSS:

XSS Exploit Requirements

1. Vulnerable Website
2. With User Interaction / Without User Interaction
3. Attacker Website

XSS Types

1. Reflected

2. Stored
3. Blind
4. DOM (Fully Client Side)
5. Self XSS

Exploitation

1. XSS Exploit Targets
2. Session Hijacking
3. Trustable Phishing
4. Run Malicious Scripts

Exploitation Types

1. Hijack Session Remotely
2. Inject External Script

For web penetration testing beef project will be helpful

Command & Code Injection

Interactive Shell

1. Blind Shell
2. Reverse Shell

Data Exfiltration

1. Using Http
2. Using DNS
3. Using Ping

XXE:

An XML External Entity (XXE) attack is a **type of attack against an application that parses XML input** .
It occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.
XXE injection is a web security vulnerability that allows an attacker to interfere with the way an application processes XML data.
Successful exploitation of XXE injection allows an attacker to view files from the application's server and interact with any external or backend systems that the application can access.
There are various types of XXE attacks, including exploiting XXE to retrieve files, performing SSRF attacks, exfiltrating data out-of-band, and retrieving data via error messages.

Broken Access Control

Insecure Direct Object Reference (IDOR) is a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. **This vulnerability allows attackers to bypass authorization checks and access unauthorized resources .**
IDOR vulnerabilities are most commonly associated with horizontal **privilege escalation**,
but they can also arise in relation to vertical privilege escalation .
There are many examples of access control vulnerabilities **where user-controlled parameter values are used to access resources or functions directly**.
One such example is **when a website uses the customer number as a record index in queries that are performed on the back-end database**.
If no other controls are in place, an attacker can simply modify the customer_number value, bypassing access controls to view the records of other customers .

HTTP parameter pollution
http://example.com/?color=red&color=blue
ASP/IIS => red,blue
PHP/Apache => blue
Python/Zope => ['red', 'blue']

Forensic:

Sysmon

Event ID 1:	**Process Creation:** This event is generated when a process is created .
Event ID 2:	**A Process Changed a File Creation Time:** This event is generated when a process changes the creation time of a file .
Event ID 3:	**Network Connection:** This event logs TCP/UDP connections on the machine .
Event ID 4:	**Sysmon Service State Changed:** This event is generated when the Sysmon service state is changed .
Event ID 5:	**Process Terminated:** This event is generated when a process terminates .
Event ID 6:	**Driver Loaded:** This event is generated when a driver is loaded .
Event ID 7:	**Image Loaded:** This event is generated when an image is loaded into a process .
Event ID 8:	**Create Remote Thread:** This event is generated when a process creates a remote thread in another process .
Event ID 9:	**Raw Access Read:** This event is generated when a process opens a handle to a device object and requests read access to the device .
Event ID 10:	**Process Access:** This event is generated when a process opens another process .
Event ID 11:	**File Create:** This event is generated when a file is created .
Event ID 12:	**Registry Event** (Object create and delete): This event is generated when a registry key or value is created or deleted .
Event ID 13:	**Registry Event** (Value Set): This event is generated when a registry value is set .
Event ID 14:	**Registry Event** (Key and Value Rename): This event is generated when a registry key or value is renamed .
Event ID 15:	**File Create Stream Hash:** This event is generated when a file stream hash is created .
Event ID 16:	**Sysmon Configuration Change:** This event is generated when the Sysmon configuration is changed .
Event ID 17:	**Pipe Event** (Pipe Created): This event is generated when a named pipe is created .
Event ID 18:	**Pipe Event** (Pipe Connected): This event is generated when a named pipe is connected .
Event ID 19:	**Wmi Event** (Wmi Event Filter activity detected): This event is generated when WMI event filter activity is detected .
Event ID 20:	**Wmi Event** (Wmi Event Consumer activity detected): This event is generated when WMI event consumer activity is detected .
Event ID 21:	**WmiEvent** (Wmi Event Consumer To Filter activity detected): This event is generated when WMI event consumer-to-filter activity is detected .
Event ID 22:	**DNS Event (DNS query):** This event is generated when a DNS query is made .
Event ID 23:	**Service Configuration Change:** This event is generated when a service configuration is changed .
Event ID 24:	**Pipe Event** (Pipe Listening): This event is generated when a named pipe is listening .
Event ID 25:	**Driver Loaded (Boot)**: This event is generated when a driver is loaded during boot .
Event ID 26:	**File Delete Detected** (File Delete logged): This event is generated when a file is deleted .
Event ID 27:	**File Block Executable:** This event is generated when Sysmon detects and blocks the creation of executable files (PE format) .
Event ID 28:	**File Block Shredding:** This event is generated when Sysmon detects and blocks file shredding from tools such as SDelete .
Event ID 29:	**Image Load** (DLL): This event is generated when a DLL is loaded into a process .
Event ID 30:	**Image Load** (Driver): This event is generated when a driver is loaded into a process .

Windows Important Event ID :

4624:	Successful logon
4625:	Failed logon
4728:	Member added to security enabled global group
4732:	Member added to security enabled local group
4756:	Member added to security enabled universal group
1102:	log cleared
4740:	User account locked out
4663	Attempt made to access object

MITRE ATTACK Techniques:

1	Reconnaissance
2	Resource Development
3	Initial Access
4	Execution
5	Persistence
6	Privilege Escalation
7	Defense Evasion
8	Credential Access
9	Discovery
10	Lateral Movement
11	Collection
12	Command and Control
13	Exfiltration
14	Impact

TOP 10 MITRE ATTACK :

T1059:001:PowerShell:	Adversaries use PowerShell to execute malicious code, download and install malware, and steal data.
T1047: Windows Management Instrumentation:	Adversaries use WMI to execute malicious code, download and install malware, and steal data.
T1027: Obfuscated Files or Information:	Adversaries use obfuscation techniques to hide malicious code or data from detection.
T1218.011: Rundll32:	Adversaries use Rundll32 to execute malicious code, download and install malware, and steal data.
T1105: Ingress Tool Transfer:	Adversaries use various methods to transfer tools and files to compromised systems.
T1055: Process Injection:	Adversaries inject malicious code into legitimate processes to evade detection.
T1569.002: Service Execution:	Adversaries use services to execute malicious code, download and install malware, and steal data.
T1036.003: Rename System Utilities:	Adversaries rename system utilities to evade detection.
T1490: Inhibit System Recovery:	Adversaries use various methods to prevent system recovery.
T1036: Masquerading:	Adversaries disguise malicious code or data as legitimate files or processes to evade detection.

The Cyber Kill Chain :

is a framework that explains how attackers move through networks to identify vulnerabilities and exploit them. It covers seven stages: reconnaissance, weaponization, delivery, exploitation, installation, C2, and actions on objectives

Reconnaissance:	Attackers gather information about the target system, such as IP addresses, domain names, and email addresses.
Weaponization:	Attackers create a weapon, such as a virus or a Trojan horse, that can be used to exploit the target system.
Delivery:	Attackers deliver the weapon to the target system, usually through email, social engineering, or other means.
Exploitation:	Attackers exploit a vulnerability in the target system to gain access to it.
Installation:	Attackers install malware or other tools on the target system to maintain access and control.
C2:	Attackers establish command and control channels to communicate with the target system and issue commands.
Actions on objectives:	Attackers achieve their objectives, such as stealing data, disrupting services, or causing damage.

Best tools :
Process hacker - Browsing History View - Abuse IPDb - Cisco Talos - urlscan

Threat Hunt :

Detection Methods for the Pass the Hash Attack

Below, known Event IDs are added to detect a possible Pass-the-Hash attack :

Event ID 1 - Process Create.

● Key Description Fields: LogonId, ParentProcessId, ParentImage, CurrentDirectory, CommandLine, IntegrityLevel, ParentCommandLine, ParentCommandLine, UtcTime, ProcessId, User, Hashes, Image

Event ID 5 - Process terminated.

● Key Description Fields: UtcTime, ProcessId:, Image

Event ID 10 - Process accessed.

● Key Description Fields: SourceThreadId, TargetProcessId, GrantedAccess, SourceImage, TargetImage

Event ID 4624 - An account was successfully logged on.

● Key Description Fields: Account Name, Account Domain, Logon ID

Event ID 4663 - An attempt was made to access an object.

● Key Description Fields: Process ID, Access Mask, Account Domain, Object Name, Process Name, Object Type, Logon ID, Handle ID

Event ID 4672 - Special privileges assigned to new logon.

● Key Description Fields: Security ID, Account Name, Account Domain

Event ID 4688 - A new process has been created.

● Key Description Fields: Required Label, Account Domain, Source Process Name, New Process Name, Token Escalation Type, New Process ID, Source Process ID

Detection Methods for the Pass the Ticket Attack:

Below, known Event IDs are added to detect a possible Pass-the-Ticket attack:

Event ID 4768 - A Kerberos Authentication Ticket **(TGT)** was requested.

● Key Description Fields: Account Name, Service Name (always "krbtgt"), Service ID, Client Address

Event ID 4769 - A Kerberos Service Ticket was requested.

● Key Description Fields: Account Name, Service Name, Client Address

Event ID 4770 - A Kerberos Service Ticket was renewed.

● Key Description Fields: Account Name, User ID, Service Name, Service ID

Detection Methods for the Kerberoasting Attack:

It is possible to identify various signs of Kerberoasting by observing the Windows event log for unusual requests for ticket-granting service (TGS).

Event ID 4769 - A Kerberos Service Ticket was requested.

● Key Description Fields: Account Name, Service Name, Client Address

Event ID 4770 - A Kerberos Service Ticket was renewed.
● Key Description Fields: Account Name, User ID, Service Name, Service ID

Detection Methods for the Golden Ticket Attack :

Event ID 4769 - A Kerberos Service Ticket was requested.
● Key Description Fields: Account Name, Service Name, Client Address

Event ID 4624 - An account was successfully logged on.
● Key Description Fields: Account Name, Account Domain, Logon ID

Event ID 4627 - Identifies the account that requested the logon.
● Key Description Fields: Security ID, Account Name, Account Domain, Logon ID