Network Security

TA-2

Dhaval kumar Vijaykumar patel Enroll:- 032200300002034

Date:- 26th June 2023

Q-1)

(a) Explain Oscar Methodology in detail.

→ The "OSCAR" methodology consists of five phases or stages that are followed in sequence. while managing the life-cycle of the network forensic investigation. The methodology is usually referred to as the "oscAR" methodology.

(i) O → Obtain Information
(ii) S → Strategize
(iii) C → Collect Evidence
(iv) A → Analyze
(v) R → Report

(i) O obtain Information

Collection of any information that is related to system environment and incident under investigation. Gather as much as information about the network and the incident. The goal is to understand the network infrastructure, its components, and the context of the incident.

a) The incident

An investigator begins by gathering the following incident related information.

- Description of the case
- The time and Date of case
- Identification of people involved
- Identification of the data and system components involved

- Identification of any process or actions performed since incident discovery
- Identification of process for manging the incident
- Identification of any legal concerns
- deadlines for the investigation and Recovely for the data

b) The environment

The investigator should study the technical and organizational environment in which the incident took place. The investigator should try to assess the following

- The deployed business model
- Legal concerns
- The topology and architecture of the network
- network evidence resources
- The organizational Infrd. and Communication systems
- The process and procedure for the incident response
- logs, system configuration, network traffic capture
-

(ii) Strategize

once the investigator has a clear understanding of the network and the incident, they develop a strategic plan for the investigation This involve.

- define scope
- objective of investigation
- identify potential source of evidence
- determine tools and techniques required

- allocating resource effectively
- potential risks
- need for collaboration with other teams or external entities.

(iii) Collect evidence

Collection of Relevent evidence from various source. Also Document each evidence and Preserve in a efficient way. The evidence could be network traffic, data from logs, storage devices, etc.

(iv) Analyze

↳ once evidence collected it is analyse using various techniques and tools.

→ find correlation of evidence and incident
- Timeline
- Identify data source
- Network traffic pattern
- reconstruct event
- decrypting data
- and other technique to extract valuable information

(v) Report

↳ It is very ~~imopo~~ important to document all result and step into a professional and convincing report.

↳ clear and concise summary of the investigation.

b) What would you do if nmap port scans are blocked by network security administrator? How would you gather host information in such case?

→ If nmap port scans are blocked, we can gather host information by just scans with bypass host discovery. Host discovery we ping, but server firewall do not response to ping Request. This command forces the host without waiting for a reply.

nmap -Pn -F <IP>

This command will return information on every host, their latency, MAC, and also any description associate with this address.

This can be a powerful way of spotting suspicious hosts connected to our network.

Also we can by pass the firewall Rules using Exotic scan Flags, Source port manipulation IDS attacks IP, ID, Idle scanning, etc..

c) With reference to 802.11i, describe the operation of TKIP and CCMP protocols.

→ TKIP (Temporal key Integrity protocol)

↳ TKIP is an encryption protocol included in IEEE 802.11i standard for wireless local area network (WLAN). It was designed and implemented to provide more ~~security~~ secure encryption ~~than the~~ ~~word~~ than the WEP encryption protocol.

↳ TKIP operates by using a 128-bit encryption key called the temporal key that dynamically changes for each packet transmitted

3 major componant.

- 64-bit message integrity check (MIC)
  ↳ used to verify the integrity of Packet
- Packet sequencing control
  ↳ Runs with key Hierarchy function. TKIP employes key ~~he~~ hierarchy structure, which includes a pairwise Transient key (PTK) for securing communication between two device and a Group Temporal Key (GTK) for securing multicast and broadcast traffic within a network

↳ Per-Packet Key ~~hiding~~ mixing
↳ TKIP combines the original WEP key with a unique initialization vector (IV) and a per-packet key identifier to generate a unique encryption key for each packet. This helps mitigate the weakness of WEP's static key.

CCMP (Counter mode with cipher Block chaining message Authentication code Protocol)

→ CCMP is an advanced encryption protocol to replace TKIP
- CCMP operates using the AES Algorithm.
- It combine encryption and Authentication functionalities in a single protocol.
- CCMP operates in two main steps.
  - The counter mode (CTR) - encryption
  - The cipher Block chaining message Authentication code (CBC-MAC) - authentication and integrity

CTR mode:
↳ encryption the packet payload with a unique counter value and a drive by encryption key

CBC-MAC ~~mode~~:
↳ for authentication and integrity. It generates a cryptography hash of the packet using the AES, ensuring that the packet has not tempered.

d) Three TAP in network forensics.

↳ Network TAP
↳ Aggregation TAP
↳ Regeneration TAP

→ TAP stands for Traffic Analysis Point.
TAP is device or software that allows us to monitor and access data that is transmitted over a network

↳ Network TAP
Each network port has a corresponding monitor port. The network ports will be labeled A and B, with their corresponding monitor port also labeled with A and B.
↳ This can be single passive monitor tool or a network packet Broker (NPB). which then sends the copied traffic on to several network monitoring tools, such as traffic analyzer, capture system IDS, etc.

↳ Aggregation TAPs
↳ Aggregation TAPs connect MANY network ports to ONE monitoring port. This means that network traffic analyzed. This is useful when that single monitoring tool has a limited number of ports.

↳ Regeneration TAPs

That crucial network segments traffic could than be monitored by an IDS, recorded for later forensic examination, captured for future use, or analyzed for performance issues.

Q. 2

a) (i) Security and Incident Response

↳ organization monitor network forensic data to check security of the network, infra., systems and sensitivity of information. By monitoring organization can detect and prevent security breaches, unauthorized access, malware infection, etc.

(ii) Compliance and Regulatory Requirment:

many compliance and Regulatory Required a monitoring network activity To match the requirment and standard organization need to monitor network forensic data.

(iii) Network performance:

monitoring network forensic data can help in maintaining network performance and troubleshooting By analyzing network traffic pattern, band width, latacy, packet loss, organization can identify and resolve the network bottlenecks, optimization network configuration, more productivity and efficient functioning of critical systems and applications.

b)

5

OSSEC, open source security (OSSEC) Host-based Intrusion Detection system (HIDS). It is widly used open-source security tool design to provide real-time monitoring, log Analysis, file integrity checking, and active responce capabilities on host systems. It helps organizations to detect and respond to security incidents.

Pupose :-

IDS :- detect and Alert on potential Intrusions
Log Analysis
File integrity checking
Active Response

usage :-

monitoring and detection
Log analysis and correlation
File integrity monitor
compliance monitor
Incident Responce

d) OSINT refer to collection, analysis and utilization of publicly available information from open source.

Purpose:

Threat Intelligence

OSINT tool gather information from a wide range of open sources like public website, social media, forums, article etc. This information can used to identify potential threats, threat vector and monitor the digital landscape for IOCs, or security risks.

Vulnerability Assessment:

help to identify potential vulnerability in systems, networks, or applications. by analysing public information related to software versions, security patches, known vulnerabilities etc.

Digital Footprints Analysis:

Mapping organization's digital foot-prints by collecting information about public-facing, domain names, etc.

Investigation and Attribution:

help uncover digital footprints, identify aliases, track online activities, and gather evidence that can be used in legal proceedings or incident response efforts.

usage!

Information gathering
Data Analysis and correlation
Threat hunting
Incident Response
Risk assesment

9.3

(a) (i) VPN vs VLAN

VPN → virtual Private Network

↳ VPN helps to stay private when we online. Provide on network connection while using public network.

↳ We encryption to encrypt our internet traffic data. to hide our online identity

↳ VPN client connect to wifi → ISP. here VPN client encrypt by protocols.

↳ establishment of VPN tunnel. to connect VPN server.

↳ VPN server connects to our website server and decrypt our messages.

VLAN Virtual (LAN)

VLAN is a virtual connection between devices or department ~~or~~ of two or more then one or two local area network. More then one local area network connected virtually into one logical network.
It is design to intract with each other through data link as they share the same physical location in same broadcast domain.

~~example~~
↳ The Two different department of a organization could have systems on the same physical LAN. but it might be easier to manage the system if both ~~—~~ department logically each had it's own network virtual LAN.

(ii) Avalanch Effect
When a small chang in input the output is entirely change. It is called Avalanch effect

example

& Hsh functions

Hsh of → ~~0~~00123
SHA1 → 9bcea448 3a00ga 15aa 64 994 fc18 3c5819 009e135

Hsh of → 000<space>123
SHA 1 → 0ed94ac37c 07232b2 ebd259 ~~—~~ 6315d 0b96 71b607
b3

(iii) Attack Surface vs Attack vector

Attack surface

Attack surface is a combination of all potential entry points, vulnerabilities, and areas that could compromise and attacker could target to gain unauthorized access, network or application.

example

- Open network port
- Service accessible over the internet
- API
- Dependencies
- Network protocol and communications channels

Attack vector

Attack Vetor is method or path of procedure that tricks users into give information or doownlod malware.

example

→ Phishing email or social engineering technique
→ Exploit vulnerabilities
→ Brute-forcing
→ ~~Attack~~ MITM men-in-the-middle Attack.

(iv) Buffer overflow

To understand let's first see what is Buffer. Buffer is a temporary area for data storage.

When software try to write data in buffer but it write so many data that leads to exceed its allocated size.

It's call Buffer overflow.

It can lead to system crashes, overwriting adjacent memory size and area.

(v) Evil Twin

Evil Twin attack is a rogue wi-Fi access point that seems like legitimate IP. It tricks users to connecting to that AP, that allows attackers to intercept network traffic steal information, or launch further attack

(b) (i) tcpdump

tcpdump is a command-line packet Analyzer tool used for capture and analyze network traffic in real-time.

Pcap (Packet capture)

Pcap is a common file format used for storing network packet capture data.

Role-based Access control (RBAC)

↳ security model that provide granular access control based on predefine role and permission. In RBAC, access rights are assigned to roles and users are then assigned to specific roles based on their job responsibilities or organizational roles.

Key components

Roles
Permissions
Users
Access-control policies
Scalability and manageability
Security and compliance

(ii) SOC (Security operational center)

↳ centralized unit within a organization that is responsible for monitoring, detecting, analyzing and responding to cybersecurity incidents.

Functality:-

Threat monitoring and detection

↳ SOC continuously monitor the organization network, system, and endpoints for suspicious activity

Incident Response

↳ If any incident occurs SOC is started response accordingly

Security event analysis:

↳ SOC analysis security events to determine the nature of incident, Impact and response actions.

Threat hunting:

Searching for indicator of compromise.

Vulnerability Management:

SOC search for vulnerability and conduct assessment.