Internal Assessment Test 2 – July 2024

Solution

Sub:	Introduction To Cyber Security (Open Elective Course)					Sub Code:	21CS653	Branch:	ECE, ME
Date:	10.07.2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	VI		

1

Scheme:

a) List any 4 distinct phishing techniques used by Phishers to launch Phishing attacks and explain them in brief (1-2 lines each) ***(4 marks, one for each technique)***

b) b) List any 5 "Phishing countermeasures" and explain them in brief (1-2 lines each) ***(5 marks, one for each technique)***

c) What is a "teardrop" DoS attack? Answer in brief (one line). ***(1 mark)***

Solution:

a) Various phishing techniques are listed below

- *URL manipulation: URLs are misspelled or with a difference of 1-2 letters. Phisher creates and registers a domain name in the name of this "manipulated or wrong web site". When users make a mistake in typing the name, they land onto the wrong web site.*
- *Filter Evasion: Phisher uses graphics (e.g. images) to avoid anti-phishing filters of browsers. Web browsers have inbuilt anti-fishing filters which the Phisher bypasses. This results in victim being trapped.*
- *Website forgery: Phisher redirects users to website designed by Phisher/hacker by altering browser address bar through Javascript commands*
- *Flash fishing: Phisher exploits limitations of "Anti-Phishing" toolbars (which are installed to check website content for signs of Phishing)*
- *Social fishing: Phishers entice the netizens (users) to reveal sensitive data by means of social media, email, phone etc (and a combination thereof)*

➢ ***Sending email*** *as if it is sent by a bank asking to call them back citing false security breach*

➢ *"Smishing": Criminal offense conducted by using social engineering techniques similar to Phishing. (Named derived from "SMS phISHING" (but could be other text messages as well).*

-
- *Phone fishing: Phone calls to entice users to reveal their personal information, Use of fake caller ID to make it look genuine*
- *Vishing uses (most often) features offered by VoIP (Voice Over IP) to gain access to personal and finanacial information (Voice + Phishing)*

- *Mishing: Combination of Mobile phone and Phishing attacks conducted using mobile phone*
-
- *Spear Phishing: Phishing message sent to a particular organization, group (of employees)*
- *Whaling: A specific form of phising targeting executives from the top management of a company to reveal confidential information*
- ➢ *It involves more extensive reconnaissance (gathering information) about the target rather than the target being enticed to be a victim of Spear Phishing attack*
- ➢ *E-Mails sent in the whaling scams are designed to masquerade as a critical business E-Mail sent*
- *e.g. Whaling attack on CEOs where a forged "official looking FBI email" was sent to collect password information*
- *Some new types of techniques*
- *Quishing: QR code Phishing*

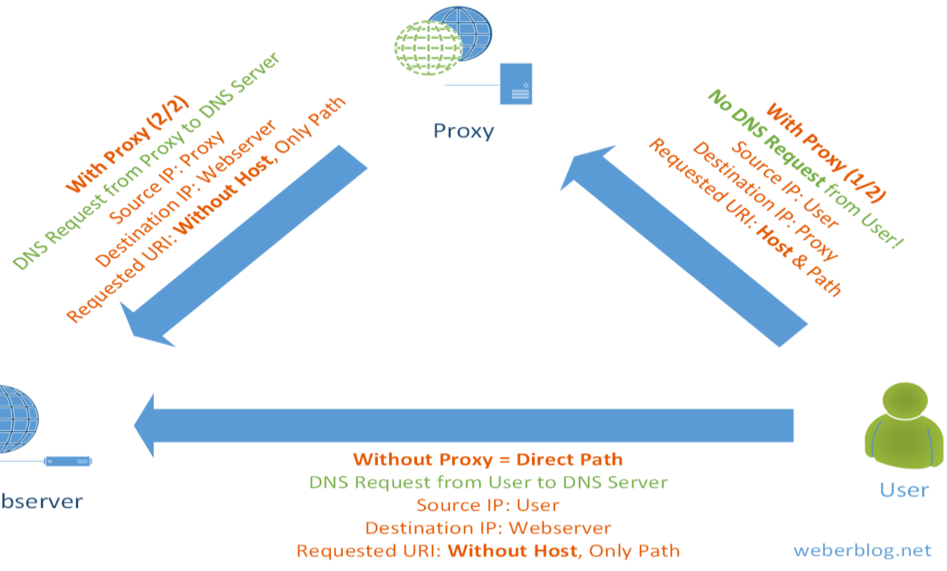
Phishing countermeasures
Keep Antivirus up to date
Do not click on hyperlinks in e-mails
Take advantage of anti-spam software
Ensure HTTPS (secure HTTP)
Use anti-spy software
Get educated
Firewall
Use backup system images
Secure Hosts file
Protect against DNS Pharming attacks
Do not enter sensitive or financial information in pop-up windows

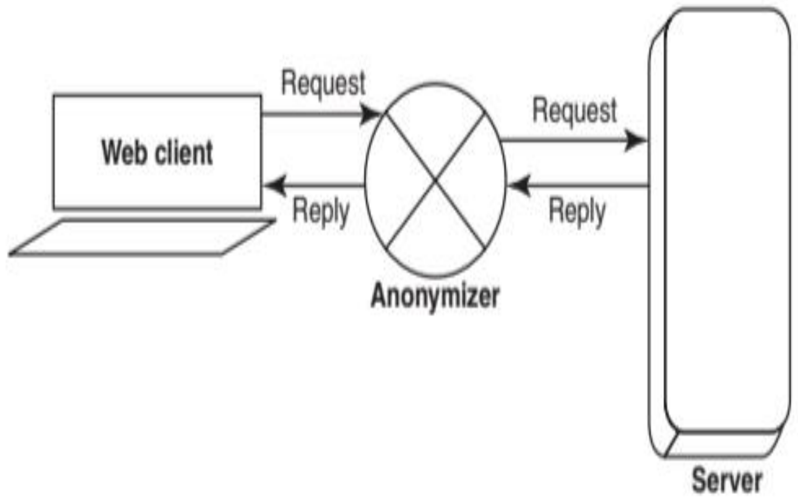
c) Teardrop attack:
Fragmented packets are forged to overlap each other, so as to confuse receiving host during reassembly. A bug in TCP/IP fragmentation reassembly code may crash various O.Ss

2

a) What is a Proxy server? How does it work? Explain with a sketch. ***(3 marks)***
b) List 4 important benefits of a proxy server for "client computers" which connect to it. ***(4 marks)***
c) What is the benefit provided by Proxy server to "hacker computers"? ***(1 mark)***
d) What is the difference between forward proxy and reverse proxy? ***(2 marks)***

a) ***Proxy:*** *A server/computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers*
A client connects to the proxy server, requesting some service, such as a file, connection, web page etc
The proxy server evaluates and forwards the request to actual server
Response from the server is sent back to client


Proxy
With Proxy (2/2)
DNS Request from Proxy to DNS Server
Source IP: Proxy
Destination IP: Webserver
Requested URI: Without Host, Only Path
With Proxy (1/2)
No DNS Request from User!
Source IP: User
Destination IP: Proxy
Requested URI: Host & Path
Webserver
User
Without Proxy = Direct Path
DNS Request from User to DNS Server
Source IP: User
Destination IP: Webserver
Requested URI: Without Host, Only Path
weberblog.net

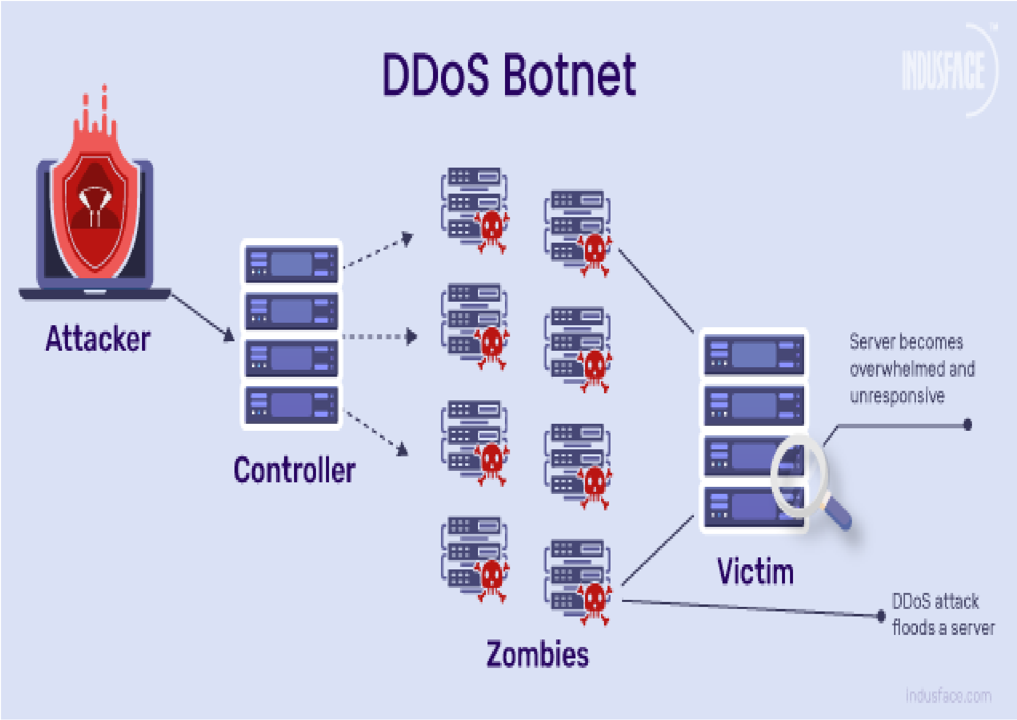


b) *Benefits provided by Proxy: Any 4 of the following*
Proxy server helps keep the systems shielded (for security purposes). In case of attack, first proxy gets attacked
Speeds up access to a resource using caching (e.g. Caching web pages from a web server). But proxy also introduce one extra hop for traffic compared to direct internet connection.
Specialized proxy servers are used to filter unwanted content such as advertisements
Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address
Proxy can help in protecting identity of users online.

c) *But for a hacker or attacker, Proxy server can allow an attacker to hide ID of his/her computer.*

d) *Reverse proxy is a server that sits in front of one or more web servers, intercepting requests from clients.*

	Reverse proxy can provide protection from attacks *Helps in load balancing. (distribute incoming traffic)* *Improves fault tolerence if any of the servers fails* *Forward proxy is on the client side, getting traffic from client machines and forwarding to internet.*
3	a) What is a DoS attack? What does DoS attack target? ***(2 marks)*** b) What is DDoS attack? Explain with a sketch. What is the difference between DoS and DDoS? ***(4 marks)*** c) List any 4 types of DoS attacks with a brief (1-2 lines) description of each ***(4 marks)*** ***Solution:*** ***A) A denial-of-service (DoS) attack is an attempt to make a computer resource (i.e. information systems) unavailable to its intended users. The goal of DoS is not to gain unauthorized access to system. But to prevent legitimate users of a service from using it*** ***A DoS attack may target any of the computer resources*** ***Flood a network with traffic, thereby preventing legitimate network traffic*** ***Disrupt connections between two systems, thereby preventing access to a service*** ***Prevent a particular individual from accessing a service*** ***Even CPU utilization, disk space, services like Database, Email etc*** ***B) DDoS (Distributed denial-of-service) attack is somewhat similar to DoS*** ***The attack is "distributed" because the attacker is using multiple computers*** ***An attacker may use your computer as well, to attack another computer (without your knowledge).*** ***In DDoS, a large number of zombie systems are synchronized to attack a "primary victim".*** ***The zombie systems are called "secondary victims" and have been already compromised before the attack*** ***A secondary system may be compromised with a Trojan, allowing the attacker to download a zombie agent*** ***Attackers can also break into zombies using automated tools that exploit flaws in programs listening for connections from remote hosts*** ***Botnet is the popular medium to launch DoS/DDoS attacks*** ***BotNet = RoBot + Network***


DDoS Botnet
INDUSFACE
Attacker
Controller
Zombies
Victim
Server becomes overwhelmed and unresponsive
DDoS attack floods a server
indusface.com

C) Various types of DoS attacks.
**** (Ping) Flood attack***
Attacker sending the victim an overwhelming number of ping packets

- ***Ping of death attack (exploiting bugs in TCP/IP stack)***

Sending oversized ICMP packets to the victim system crashing it
Some systems freeze, reboot after receiving these packets

- ***SYN attack (TCP SYN flooding in a client – server scenario)***

Attacker (client) initiates TCP connection to victim (server) with a SYN
Victim replies with SYN-ACK
But Client (attacker) does NOT send back an ACK
This causes Server (Victim) to allocate memory for pending connection and wait filling up buffer space for SYN message

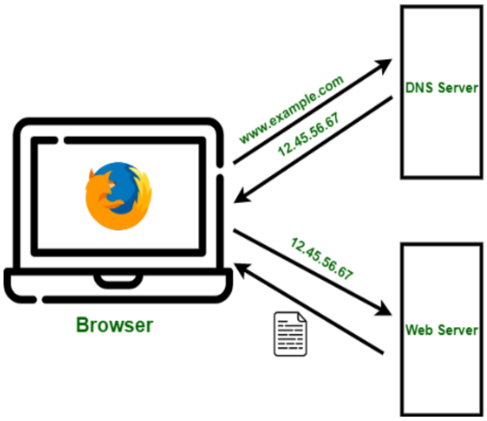
- ***Teardrop attack: Fragmented packets are forged to overlap each other, so as to confuse receiving host during reassembly***
- ***A bug in TCP/IP fragmentation reassembly code may crash various O.Ss***
- ***Smurf attack: A DoS attack which generates significant network traffic on a victim network***
- ***ICMP echo request to a network broadcast address***
- ***On a multi access broadcast network, hundred of machines might reply to each packet creating “magnified DoS attack of ping replies”***
- ***Nuke: An old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets***
- ***PDos: Permanent damage to firmware or hardware***

There could be few more such examples/cases. If students write them, they will be

	considered.
4	a) What are the 3 basic stages of computer forensic investigation? Write a one-line explanation about each of them ***(3 marks)*** b) What important information is revealed by “backed up data” when carrying out forensic investigation? In case of loss of data or applications during Cyberattack, is it always desirable to retrieve data from latest back up? Explain in brief. ***(3 marks)*** c) What are the technical expertise areas/characteristics required by a Cyber Investigator? List any 4 of them with one line explanation of the importance of each. ***(4 marks)*** ***a) Three basic stages of computer forensic investigation*** *a. Acquisition: Acquisition is the act or process of gathering information and evidence.* *b. Authentication: Authentication is a process of ensuring that the acquired evidence is the same as the data that was originally seized* *c. Analysis: is the process of examining and evaluating information* ***b) Backup media should also be connected, because analysis of back up media may show that an incident began earlier than expected. Back up data (e.g. logs) may give some valuable information about the attack, when it started etc. But if a virus infected data was backed up, you do not want to restore it after investigation is done. So “which back to restore from”, depends on the status of that backup*** ***c)*** **Skills required: Cyber investigator needs to be skilled in multiple expertise areas.** ***Operating systems, Networking protocols, Hardware interfaces, Opening and accessing Hardware, Understanding of how computers process and store info, Applications (from web servers to Databases, Enterprise applications…,) Operations of devices like Routers and Switches.***
5	a) What is Steganography? How is it different from Cryptography? ***(3 marks)*** b) What is Steganalysis? What is Text Steganography? ***(3 marks)*** c) What is DNS and what does it do (explain with a sketch)? What is DNS hijacking? ***(2 marks)*** d) What is “chain of custody” when documenting evidence? What does “break in chain of custody” indicate? ***(2 marks)*** ***Solution:*** ***a) Steganography is hiding of information in text files, images, audio/video files using steganography.*** ***Cryptography is not same as Steganography*** ***In Cryptography, everyone knows that a message has been sent, but they can’t find out what it means.*** ***But Staganography tries to hide even the fact that the message was sent (or is present in a file)*** ***In Cryptography, message is encrypted. In Steganography, message is (more likely) NOT encrypted.*** ***b) The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it.*** ***Automated tools are used to detect such steganographed data/information hidden in the***

image and audio and/or video files

C) DNS stands for Domain Name Service. When a PC or laptop (or any other client system) is trying to communicate with a server, it queries DNS server to get IP address corresponding to that domain name. So DNS provides mapping from Name to IP address.



In case of DNS hijacking, users get wrong/hacked IP addresses for their DNA queries. This is done by Cybercrimicals hackers, who either 1) Get control of DNS server and modify DNS entries or 2) redirect DNS requests to a wrong DNS server (hacker's DNS server), which provides wrong data to users.

d) A chain of custody refers to continuity of the evidence, one can trace the route that the evidence has taken from the moment it was collected until the time it is presented in court and also every person whose hands it has passed through, and when and where it was transferred from one person to another.

<u>Any break in the chain of custody shows the possibility that the evidence has been tampered with</u>

6

a) What are the misconceptions about Cybercriminals? List any 3 of them. ***(1.5)***
What are typical categories of Cyber victims? List any 3 of them **(1.5)**

(Total 3 marks, only listing)

b) What is Digital evidence? What is Duplicate digital evidence and how does it help? ***(2 marks)***

c) When collecting Digital evidence, what decides the order in which the data should be collected? Why data collection commands should be ideally executed from a special CD? ***(3 marks)***

d) What is "ping"? What information does it provide? What is "ping of death" attack? ***(2 marks)***

Answers:

a) Common misconceptions:

All cybercriminals are "nerds"—bright but socially inept
All cybercriminals have very high IQs and a great deal of technical knowledge
All cybercriminals are male, usually teenage boys
All teenage boys with computers are dangerous cybercriminals
Cybercriminals aren't "real" criminals because they don't operate in the "real world."
Cybercriminals are never violent.
All cybercriminals neatly fit one profile

Cyber victims:

Categories of Cyber-victims or typical profiles of Cyber-victims

- ***People who are new to the Net (Internet)***
- ***People who are naturally naive (sometimes including the young and the elderly)***
- ***People who are disabled or disadvantaged***
- ***The desperate, who are greedy, are lonely, or have other emotional needs***
- ***Pseudo-victims who report having been victimized but actually were not***
- ***People who are simply unlucky enough to be in the wrong (virtual) place at the wrong time***

c) ***Digital evidence: Information of value to a criminal case that is stored or transmitted in digital form***
Duplicate digital evidence refers to an accurate digital reproduction of all the data objects contained on an original physical item
Duplication avoids the risk of original evidence getting affected (e.g. corrupted) or tampered with.

- ***When collecting digital evidence, "volatility" decides the order in which data is collected.. Evidence should not get lost or destroyed before it is collected and stored.***
- ***Commands should be ideally executed from a special CD and not from the "victim computer" because these commands on the victim computer themselves could be infected or corrupted and create undesirable effects. So using commands from Cyber analyst's CD is best option.***

d) ***"ping" is a commonly available diagnostic utility, that is used to check/test/verify if a particular destination IP address exists/is reachable by using ICMP protocol. Ping checks if the other (remote) computer is reachable. It also provides information on "response time" (essentially "round trip time" for ICMP packets). It also indicates how many packets were lost (giving idea of reliability of the link).***

Ping of death: Exploits bugs in TCP/IP stack. Hacker sends oversized ICMP packets to the victim system crashing it.
Some systems freeze, reboot after receiving these packets