Adrian Menezes
9624
TE comps B

Cybersecurity Assignment - 1

Q1] The TCP/IP protocol stack consists of 4 core layers

(i) Applicatn layer :- Topmost layer in the TCP/IP state is the applicatn layer. Responsible for providing network services directly to end-users or app programs.

(ii) Transport layer:- Responsible for end to end communicatn & transfer reliability betn two devices

(i) TCP - connectn oriented protocol to ensure data reliable transmissn

(ii) UDP :- Connectn protocol that provides a light weight way to transmit data.

(iii) Internet layer :- core routing & addressing fn of TCP/IP starts.

(iv) Link Layer :- Also known as Interface layer deals with physical & data link aspect of N.C

Q2] ~~Explain~~ IP addressing and routing are fundamentals processess in computer network that enables data transmissn :.

IP Addressing:- (i) IP Address Assignment:- Every device on a network is assigned a unique IP address, IP address can be assigned manually or dynamically.

(ii) Subnetting:- Divided into subnets for efficient management.

(iii) Default Gateway:- Devices with subnets need to know where to send data when destinatn isn't within their local network

Routing :- Routing tables :- Routers, the device responsible for directing data across network

Packet forwarding :- when device wants to send data to another

Routing protocol helps in efficient data transmiss^{n} by path orga
Redundancy & Failover, laoad balancing, scalability & adaptability

Q3] Ethical Hacking also known as penetrat^{n} test or white hat hacking involves authorized & controlled efforts to identify & address vulnerability.

a) Planning & preparat^{n} :- Define scope, obtain proper authorizat^{n} & Establish rules of engagement.

b) Reconaissance :- By collecting informat^{n} & Network scanning to discover open ports etc.

c) Vulnerability :- Identify vulnerability, applicat^{n} & network configurat^{n} & prioritize vulnerabilities.

d) Exploitat^{n} :- Exploit vulnerabilities to demonstrate potential impact

e) Documentation : About successful exploits.

f) Reporting : Create a detailed report.

g) Remediat^{n} : work with the organizat^{n}

h) Documentat^{n} & follow up :- Maintaining proper records & getting continuous improvements.

Q4]

TCP/IP	OSI model
1) No. of layer = 4	1) No. of layer = 7
2) Developed by US defence	2) Developed by ISO
3) Link, Internet, Tranport, App layer	3) Physical, Tranport, data link, sess^{n} presentat^{n}, App layers
4) widely used	4) less popular, commonly used
5) Directly associated with HTTP, DNS, FTP	5) Not directly associated with specific protocol
6) Easier to grasp	6) More complex

Q5) • Gathering & Recon in security Assessment :

- Essential in security checks exposing
- Ethical hacking ~~p~~phase collects data for attack
- Data includes, network, informat^{n}, aiding multiple vector.

• Footprinting :- Passive & Active :

Passive : Gather public data (websites, news)

Active : Intrusive methods (hacking, social Engg)

- Recon Obj :- Attackers choose vulnerable targets, explore exploits
  - Any org member can be initial target
  - single entry point is enough to begin
- Exploiting Recon Data :- Data used for targetted attack, SE
- Preventing Recon Attacks :- strong security policies, controls needed

Q6)

Vulnerability Assessment	Penetratn Testing.
1) Indentifies vulnerabilities in system	1) Simulates real-world attacks to exploit vulnerabillties
2) Scans & identifies potential weakness	2) Actively exploits vulnerabilities to assess real-world impact.
3) less intrusive, identifies ~~vulnerab~~ vulnerabilities	3) More aggressive, tests how vulnerabilities can be exploited
4) Nessus, Oen, VAS, Qualys	4) Meetasploit, Nmap, Burp suite

Q7) Key characteristics of social Engg (SE) Attacks :-

→ Manipulatn of Human psychology :- SE, attacks exploit human emotn & behaviour sush as trust, fear, curiosity & authority to manipulate into taking action, that benefit the attacker

→ Pretexting :- Attackers create fabricated scen~~er~~arios or pretexts to deceive victims into divulging sensitive informatn or performing action they wouldn't normally do

→ Impersonatn :- Attackers impersonate legitimate individuals or entities often using fake emails

→ Urgency :- Attackers create a sense of urgency to pressure victims into making hasty decis^{n}

→ scarcity : By creating a percep^{tn} of limited availability, attackers entice victims to ack quickly without careful considerat^{n}

→ Baiting: Attackers offer something enticing like a free software download that ~~contains~~ tricks victims into compromising their security

Q8) ~~W~~ Malware stands for malicious software designed to exploit devices, networks or services .it includes viruses, worms & Trojans.

⇒ Viruses : Replicates by modifying other programs & inserting its own code successful replicat^{n} results in infect^{n} of the affected areas.

⇒ worms : Independent Malware program that self-replicates to spread to other computers

⇒ Trojan Horses (Trojan): spread through SE, tricking users into executing disguised attachments

⇒ Impact & Risks :: Malware can steal sensitive data, disrupts networks & damage or destroy data

⇒ Protect^{n} Measures :- Implement strong security measures, such as firewalls & antivirus software.