Ethical hacking

→ Structured threats
  ↳ Preplanned and focus on specific target.
  ↳ organized effort to breach a specific network or organization.
  ↳ These people know s/m vulnerability and can develop script to ~~use~~ use this knowledge

→ External threat
  ↳ individual or organisation

Attacks : Use variety of tools, scripts and

DoS attack → Denial of service attack (common)

4 classes of attack
① → Reconnaissance
② → Access
③ →
④ →

① attack is kind of info. gathering on network s/m and services. This enable attacker to discover vulnerabilities.

② is the ability for an unauthorized person gain access to s/m.

③ implies that an attacker disables or corrupts networks, S/ms, or services with the intent to deny service to intended users.
DoS attacks involve either crashing or slowing down a S/m so that it is unusable.

④

Threat actor

Categories
↳ Script kiddies
↳ Hactivist
↳ Organised crime
↳ Nation States APT
↳ Insiders
↳ Competitors.

Threats to a S/m
→
→
→
→

Malware is any software that is in

Types
→ Worms, viruses, Rootkit,

Worms → self-replicating code

Viruse → Malicious code that replicates by attaching to executable code

Trojan → claim to do one func^n and do another

Spy Spyware

Adware

Rootkit

Backdoor

Logic bombs

Ransomware

Malware attacks

↳ Kooter

↳ WannaCry

↳ Zeus or Zbot

↳ Ghost

↳ Mirai

★ Types of attacks
- OS attack
- Misconfiguration attack
- Shrink wrap code attacks
- Application level attack

VAET →

→ The attacker must be able to exploit a weakness or vulnerability in a system.

Types of Attack
- Eavesdropping
- Identify Spoofing
- Snooping attack
- Interception
- Replay attack
- Data modification attacks
- Repudiation attack
- DoS Attack
- DDoS Attack
- Password guessing attack.

[Some more].

OS Attack
→ Identify which os the target uses

OS vulnerabilities
- Buffer overflow vulnerabilities
- Bugs in os
- Unpatched OS.

[exploit-db.com]

Application level attack

There is a dearth of time to perform complete testing before releasing products.

- Phishing
- Session hijacking

Shrink wrap code attack

Code can attack into an open source code / public code

Misconfiguration attack

- User haven't updated the OS, so it has different configuration
- Attacker use this to attack the user

☆ Ethical Hacking

Why?

To identify vulnerabilities

Defens in depth (OSI layer)

Data
↓
App
↓
Host
↓
Internal Network →

Scope
Risk assessment, auditing, counterfraud, best practices and good governance.
- Identify risks and highlight the remedial actions.
Limitation = _____
What do Ethical Hackers do?
-
-

Skills of

- Platform
- Network
- Computer expert
- Security
- Technology

Vulnerability research.

What is penetration testing?

Why penetration testing?

EC-council lab credentials: ilab, ASpen

Sudhap2503@gmail.com

Ethical@123

Footprinting

→ Whois Database.

whois.domaintools.com

Enter domain name and get information about the website.

DNS lookup

Command prompt → nslookup

Default server and address will appear.

www.kloth.~~com~~ net /services/nslookup.php ← DNS lookup

yougetsignal.com ← Reverse IP domain check.

dnsrecon -r 162.241.216.0 - 162.241.216.25

↓ denotes range

↓ reverse lookup.

hackthissite.org.

Enumeration

Enumeration is the process of extracting usernames

→ Involves attacker creating active connections with a target s/m and performing directed queries.

[Total 7 labs for enumeration]

NBIOS Enumeration

1 → Using windows command prompt

2 → NSE Script

3 → NBIOS enumerator (something like that)

1 → Using command prompt

nbtstat -a 10.10.10.10 } All computer available on IP address.

nbtstat -c } NetBios Name Cache list

net use } Get information about target

2 →

From : Target

To : Our Sm IP

2 →

Use Ennmap Software

Type command nmap -iV -v - script something.nse IP address

-sU } → UDP Scan

[parrot Security password → toor.] [lab]
SNMP Enumeration → Get N/w resource name.

Scanning

- TCP Scan
- Stealth Scan

Nmap S/m IP
Eg Nmap 127.0.0.1
1000 port
list down the open port

- Xmas Scan
  URG, ACK, RST

- FIN Scan
  In fin Scan, attacker send a TCP fram with only FIN flag (Check)

- NULL Scan
  RFC 793 → TCP transport layer to send msg.

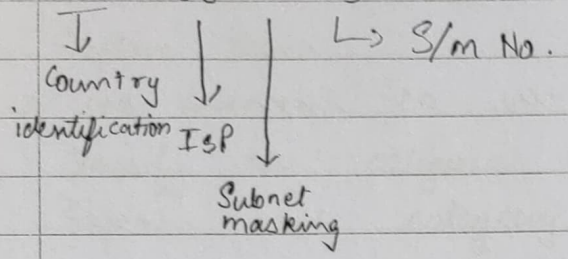
- IDLE Scan
  Sync Ack
  Port open or close.

- ICMP Echo Scanning / List Scan
  ⇒ Internet control message protocol.
Ping Ip-System
ICMP

- SYN/FIN Scanning using IP Fragmentation.

IP Fragmentation

192.168.34.25



- UDP Scanning
- Inverse TCP Scanning
- ACK flag Scanning
  Stateful firewall Scanning.
  → All ~~to~~ trafic in n/w is scanned
  → Ports, rules Stateless

Scanning : IDS Evasion Techniques

Scanning Tool : ~~Nmap~~
→ Nmap
→ NetScan Tools Pro

Scanning countermeasures
→ Latest service pack
→ Antispoofing rules
→

Banner Grabbing

OS fingerprinting
Method to determine the OS running on a remote target S/M.
Types:
→ Active
→ Passive

Telnet used for active banner grabbing
ID Serve → tool
GET REQUESTS
Netcraft

Banner grabbing countermeasures
Disabling or changing banner.
Hiding file extensions.

Q1 What are the different attack vectors through which the attacker can attack the Info. S/M. Explain them.

Q2 Classify the categories of Info security threat. Explain each category in detail.

Q3 What is hactivism? Explain it.

Q4 Enumerate diff. phases of hacking. Explain each in detail

Q5 What is footprinting? Explain the following terminologies:-
a) Open Source or passive Info gathering
b) Anonymous footprinting
c) Organisational footprinting
d) Active Info gathering
e) Pseudonymous footprinting
f) Internet footprinting.

Q6 Why do attacker need footprinting? What are the objective behind it

Q7 Explain website footprinting

Q8 Explain DNS footprinting

Q9 How is footprinting done through Social Eng. Explain

Q10 Explain any 5 footprinting tools

Q11 What is a virus? What are the characteristic of virus? What are the stages in life cycle of a virus

Q12 What is vulnerability scanning? How can we detect it?

Vulnerability scanning

VC identifies vull vulnerabilities and weakness of a s/m

Nessus Tool.

Robot.txt → Tell which site they can crawl.

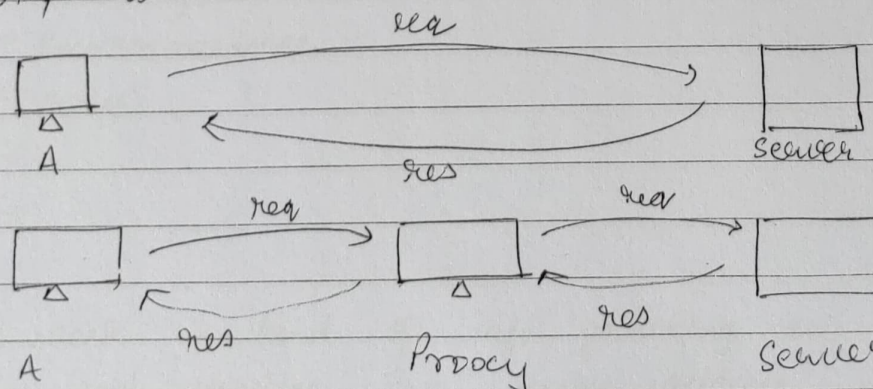
SAINT Tool.

Draw N/W Diagrams

LAN surveyor

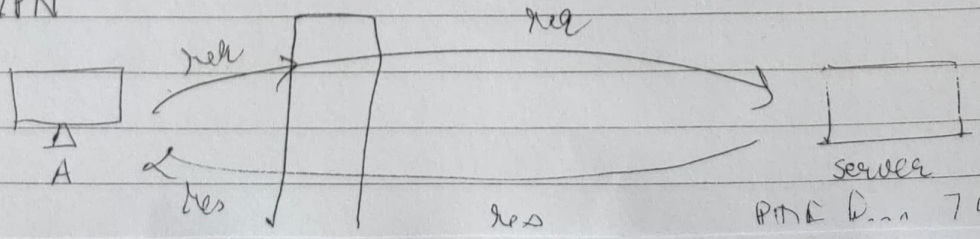
Repare Proxies

Proxy is a network computer that can serve as an intermediary for connecting with other computers



Tunnelling

VPN



Page 75.