Unit - 3 - Passive Information Gathering

* Information Gathering is the act of collecting data relevant to a specific goal.
* Attacker must know something about the target - domain name, IP address, physical address, location, phone no, etc.
* Tools used by attacker to gather → brower & internet connection

⇒ Starting at the Source :

* Gather info at targets website : free info provided to clients, customers, general public.
* Attacks based on location: Dumpster diving, warding, wardialling
* Dumpster Diving:
  - ↳ only address of the victim is known
  - ↳ Garbage available in the company can contain personal financial data like social security numbers, operation manuals, configuration guides, passwords, account numbers & passwords, etc.
  - ↳ it is a technique used to retrieve info that could be used to attack any computer network.
  - ↳ risk of dumpster diving can be reduced by shredding old CDs, wiping hard drives clean, etc.

* Wardiving :
  - ↳ act of finding and marking locations & status of wireless networks.
  - ↳ This risk can be reduced by turning on encryption & physically protecting the access points.
  - ↳ Others can use your network to launch attack on someone else.

* Wardialling:
↳ it is the act of automatically scanning telephone numbers using modem, usually dialing every telephone no. in a local area.
↳ Large organizations have exchange no. that can be scanned using wardialler.
↳ Wardialling tools:
- ToneLoc
↳ a program that looks for dial tones by randomly dialing numbers / dialing within a range. Ex.
↳ it can also look for carrier freq. of modem / fax.
- THC-Scan
↳ an older DOS-prog that can be used modem to dial ranges of nos. in search of a carrier freq. from a modem / fax.
- Demon Dialer
tool used to monitor a specific phone no. & target its modem to gain access to the system.

⇒ Scrutinizing Key Employees

* If the location of key employees is available, one can drive to that location to check if they have any wireless connections.
* Tools are available to find address & also to map IP addrs to the location.

Dumpster Diving [Electronic] **

* Process of looking for obsolete, obscure / old electronic data.
* Internet archive → home to Wayback Machine
  ↳ 85 billion webpages are archived.
  ↳ 'robots.txt' prevents this.
* Disgruntled employees may also leak info. They can post info in "www.internalmemos.com". Some info is available for free whereas the others for premium.

⇒ Analyzing Web Page Coding

* Code of every web page is analyzed.
* Details like email address, links to other sites, notes/comments, hidden fields, information of web applications/programs used, design of site must be examined.
  ↳ This can be done using site-ripping tools.
* Site-ripping tools can make a duplicate copy of the website that can be stored on hard drive.
* Other tools →
  (i) Teleport Pro : Windows website scanners; allows local reviewing.
  (ii) Wget : A command line tool for Windows and Unix; downloads the contents of the website.
  (iii) Instant Source : works with Internet explorer. Displays images, flash movies, & script files on webpage.
* Hidden fields are poor programming practice as they can be revealed when reviewed & they hold details of some price.
* Attackers can use this price information, modify it & pass it on to web application. It can lead to problems if info. is invalid
* Another issue → hidden fields that accept -ve values.
  ↳ It can lead to -ve balance in bank acc".

⇒ Exploiting Website & Authentication Methods.

* Common authentication types:
  - → basic
  - → forms based
  - → message digest
  - → certificate.

* Basic Authentication

→ done by Ex-OR (exclusive ORing)

→ Passwords sent can be XORed with stored values after converting it to binary form of the ASCII equivalent. The result is sent over HTTP.

→ very weak encryption..

* Form-based Authentication

→ uses cookie issued to a client.

→ Once authenticated, web application generates a cookie/session state variable. This ~~variable~~ cookie is reused on subsequent visits.

→ Passwords can also be stored on cookies.

→ Cookie Spy, Karen's Cookie Viewer.

* Message digest Authentication

→ uses MD5 algorithm.

→ uses username, password & nonce value to curate an encrypted value that is passed to the serve

→ Nonce value makes it more resistant to cracking & makes sniffing attacks useless.

* Certificate-based Authentication:

→ it is the strongest form of authentication.

→ Certificate contains a special type of authentication known as a publickey & signature of the certificate authority.

Mining Job Ads & Analyzing Financial Data

* attacker can collect details of technologies used in an organization by looking at the job ads posted by them in many websites.
* financial health of an organisation can be used by an attacker.
* when one company acquires another, their websites get merged. During this phase, the security is less & attacker can get access to internal details and information.

⇒ Using Google to Mine Sensitive Information

* Google collects data (sensitive) that must not be revealed to outsiders.
* Google Hacking Operators:
  1. Filetype: directs Google to only search within the text of a particular file type. [filetype:xls.]
  2. Inurl: directs Google to only search within the specified URL of a document. [~~link:www.domain.com~~ inurl: search-text]
  3. Link: directs Google to search within hyperlinks for a specific term. [link:www.domain.com]
  4. Intitle: directs Google to search for a term within the title of a document. [intitle: "Index of ...."].

⇒ Exploring Domain Ownership:

* Internet Assigned Number Authority [IANA] is responsible for preserving the central coordinating func of global Internet for the public good.
* Manages domain name & address.

⇒ WHOIS Database

* Tool to query info organization entered when they register the domain.
* can be queried by domain name / IP.
* ICANN collects WHOIS info from domain holders.
* Ex: WHOIS information for smu.edu.

  Fields: Registrant
  Administrative Contact
  Technical Contact

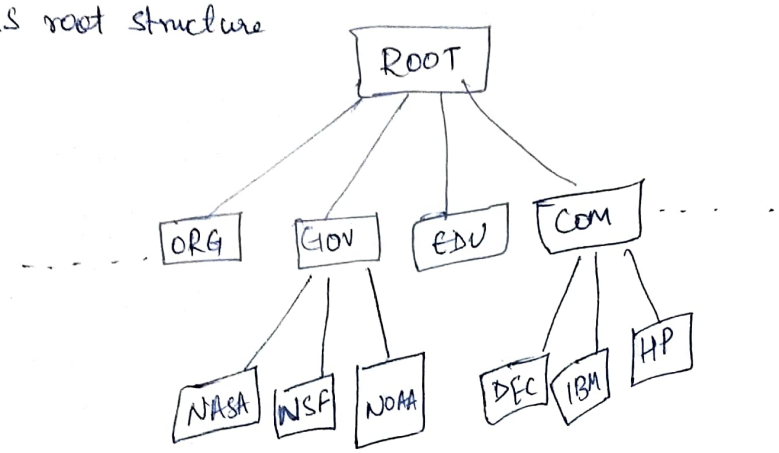
  Names: Social engineering.
  Email: Spoofing
  Phone no: Wardialling.

⇒ Regional Internet Registeries.

* oversees the regional distribution of IP addresses within geographical region of world.
* subdelegates IP addrs. to ISPs and users.
* managed by IETF
* aids in network diagnosis & send error messages.
* any network device using TCP/IP can send/receive or process ICMP messages.
* ICMP messages have no priority & don't flood network.
* Some devices consider them as interrupts, so they can be discarded
*

Domain Name Server

* Structured as a hierarchy.
* DNS cache
* DNS root structure



⇒ Web Server Location

* neoTrace
* VisualRoute
* Hping

⇒ Detecting Active System

* can involve more than just port scanning.
* alternative techniques → wardialing, wardriving, & using ICMP.

Wardriving

* act of driving around looking for open wireless access points.
* usual result is to find and identify the signal strength of approved access points & pinpoint rogue access point.
* modern networks should have a variety of security controls.
  - → Firewalls.
  - → VPNs
  - → Intrusion Detection System (IDS)
  - → Encryption.

* Wired Equivalent Privacy vs. Wi Fi Protected Access

* ICMP (Ping)

→ Internet Control Message Protocol
→ managed by IETF.
→ aids in network diagnostics & to send error messages
→ any network device using TCP/IP can send, receive or process ICMP messages.
→ ICMP messages have no priority & don't flood the network.
→ Some devices consider ICMP messages as interruptions & as a result they may get discarded
→ ICMP messages cannot be sent in response to other ICMP messages. They are not sent in case of multicast/broadcast/invalid addr.
→ In case of traffic fragmentation, ICMP messages are only sent for the first fragment.
→ Common type of ICMP message → Ping → verifies connectivity.
→ Ping works by sending an echo request to a system & waiting for target to send an echo reply back. If target is unreachable, timeout is returned.
→ To ping large no. of hosts, sweep is performed
→ Programs that perform ping sweep typically sweep through range of devices to determine which ones are active.
→ Drawbacks: doesnot identify services in the system; pings only one system at a time.

Port Scanning.

- process of connecting to TCP & UDP ports for the purpose of finding which services & applications are open on target device.

* TCP/IP basics:

→ 4 layer → network access layer, Internet layer, host-to-host layer and application layer.

→ Network Access layer - physical delivery of IP packets via frames.
[Ethernet, token ring, ATM, frame relay].

→ Internet layer - IP, ICMP, ARP, RARP, EGP, OSPF
IP - addressing, datagram, fragmentation, congestion control
ARP - IP to MAC addresses.

→ Host-to-Host layer - end to end delivery (TCP & UDP)

→ Application layer - FTP, Telnet, SMTP, DNS, TFTP, HTTP, SNMP

* TCP & UDP Port Scanning:

→ Robust communication - 3 way handshake for establishing conn.

→ TCP header has 1 byte field for flags
ACK - acknowledgement
SYN - Sequence nos.
URG - indicate priority data.
FIN - normal shutdown
RST - abnormal session
PSH - data delivery w/o waiting for buffer to fill.

→ Terminates session using 4 step shutdown.

→ UDP:
↳ based on speed
↳ fire & forget protocol
↳ doesn't issue responses.
↳ gives less information in comparison with TCP scan.

* Common Scan Types.

1. TCP Full Convert Scan – closed ports (RST/ACK). Open(
2. TCP SYN Scan – half open
3. TCP FIN Scan – shuts down (used on UNIX devices)
4. TCP NULL Scan – sends a packet with no flags set
5. TCP ACK Scan – finds access control list (ACL)
6. TCP XMAS Scan – Toggles flag values

⇒ Advanced Port Scanning

* FTP bounce scan – uses FTP server to bounce packets off of and make scan harder to trace.
* RPC scan – determines whether open ports are RPC.
* Window scan – similar to ACK scan but can determine the open ports.
* Idle scan – uses an idle host to bounce packets off of and make scan harder to trace.

⇒ Port Scanning Tools

Nmap, THC-Amap } Command line Tools.

SuperScan, Look@LAN, NetScan Tools } GUI Tools.

⇒ OS Fingerprinting

* OS in a system connected to a network can be detected in active/passive manners.
* Passive tools monitors network traffic without interacting with the target.
* Active tool interacts with the target, sends triggers, analyses responses and detects OS in more accurate way.

---

ssive Fingerprinting ★★

→ IP addresses, active systems & open ports have been identified (determined by examining patterns).

→ 4 commonly used examined items:
1) IP TTL value - unique TTL values on outbound packets.
2) TCP window size - diff. values of initial window size.
3) IP DF option - fragmentation is different for diff. OS vendors.
4) IP TOS option - type of service varies with vendors.

→ Linux based tool POf passively fingerprints source of all incoming connections.

→ POf looks at TCP & IP fields.

Initial time to live, Don't fragment } IP header

Overall SYN packet size, TCP options, TCP Window size } TCP header.

* Active Fingerprinting : ★★

→ User doesnot wait for random packets to analyze but voluntarily injects packets into network.

→ Methods used in active fingerprinting:

↳ FIN probe
Bogus Flag probe
Initial Sequence Number (ISN) sampling
IPID sampling
TCP Initial Window
ACK value
Type of Service.
TCP Options.
Fragmentation Handling

* OS Fingerprinting Tools:

→ Queso – first widely used tools (1990s).

→ Nmap.
  ↳ for reliable prediction, 1 open port & 1 closed port. is req

→ Xplore 2 – another active OS fingerprinting tool.

⇒ Scanning Countermeasures:

* Focuses on blocking unauthorized individuals from this info.
* Intrusion Detection System (IDS) types – host & network.
* Port knocking prevents active fingerprinting. Anyone wishing to use a particular service request access by sequencing a series of ports.
* Only when knocking sequence is correct during knock phase, a connection is opened
* Securing routers & traffic through routers is done using packet filtering. It is configured through ACLs.
* ACLs allow / block traffic based on header information.
* Decisions are based on:
  ↳ Source IP addr.
  Source Port
  Dest. IP addr.
  Dest. Port.
  TCP flags
  Protocol
  Direction
  Interface

Enumerating Systems

* process of counting by an attacker before launching an attack.

* SNMP Services

→ TCP/IP stardard for remote monitoring & management of hosts, routers, & other nodes on network.

→ Enables administrators to do the foll:
  ↳ manage network performance
  ↳ locate & resolve network performance
  ↳ Support better network management.

→ SNMP uses 2 components – manager & agent.

→ Manager sends & updates requests ; Agents responds.

→ Management Information Base (MIB) organized in tree structure contains object property definitions

→ SNMP V1 → has limited security
  SNMP V3 → has data encryption & authentication.

→ Two community strings:
  ↳ First string – is to view configuration of device.
  ↳ Second string – is to read/write (changing configuration)

* SNMP Enumeration Tools:

→ Attacker can use default community strings.

→ Gain access to usernames.

→ use insecure modes of SNMP.

→ available SNMP enumeration tools:

1) SNMPUtil – Win GUI.

2) SNScan – GUI

3) Solar Winds IP Network Browser. – GUI

4) SNMP Informant – agentool.

5) Getif – GUI (Win)

6) Trap Receiver and Trap Generator – Win32 GUI

→ SNMP fits into the enumeration process as follows.

1. Attacker begins by port scanning for port 161 (SNMP).
2. Attacker attempts to connect to SNMP-enabled devices using default community strings or by sniffing community strings.
3. Attacker uses the acquired information to attempt to log into an enumerated system.
4. Attacker escalates information

* SNMP Enumeration Tools:

→ Upgrade to SNMPv3
→ different community strings
→ Turn off the port when not in use.

* Routing Devices