Unit-3

Passive Information Gathering

Information Gathering – 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, ~~type of DB~~

Same tools used by attacker – browser & Internet connection

Starting at the Source

- Gather information at target's website (free info provided to clients, customers, general public) (About us)
- If likelihood of attacking a company is low, use acquired company to attack the primary target.
- Use locations on website. Attacks based on this includes dumpster diving, wardriving & wardialling
- Dumpster diving (dumpster Djiving): Only address of victim is known. Garbage available in the company (JP Morgan Chase) can contain personal financial data (Social Sec. Numbers, operation manuals, guides, passwords, addresses)

→ It is a technique used to retrieve info that could be used to carry out an attack on computer network.

- One can reduce the risk of dumpster diving by shredding old CDs, wiping hard drives etc. Mangal 120

- Wardriving (war driving) Act of finding & marking locations & status of wireless networks.

NY suburb refused use of open wireless connection by public. Others can access your network to launch attack on someone else. Reduce this risk by turning on encryption & physically protecting access points

- Wardialling (war dialling) Act of automatically scanning telephonic nos using modem. Large organizations have exchange no that can be scanned using wardialler. This will have systems with modem connected that may have weak/no authentication.

Some Wardialling tools include

- ToneLoc :-
- THCScan
- Demondialler

Corporate board of directors, list of key employees details

... spoofing, alternative

Scrutinizing key employees

Mangal
Date /20

If key employees' location is available, ~~one~~ on drive to that location & check to see if they have some wireless connectivity. Tools are available to find addresses & also to map IP address to location.

Electronic Dumpster Diving

- Process of looking for obsolete, obscure or old electronic data.
- Internet Archive - home to Wayback Machine. 85 B web pages are archived. To prevent this, define robots.txt
- Disgruntled employees may also leak information (bad temper). They can post information in www.internalmemos.com. Some info is available for free & others for premium.

Analyzing Web Page Coding

Code of every web page is analyzed. Details like email addresses, links to other sites, notes/comments, hidden fields, information about web applications or programs used, design of site must be examined.

This can be done using site-ripping tools. Such tools can make a duplicate copy of the website that can be stored on your hard drive.

Other tools - Teleport Pro, Wget, Instant Source

* Hidden fields are poor programming practice. They hold details of some price that can be changed when being retrieved.
* An attacker can use price information, modify it & pass it to web application. Can lead to problems if invalidate
* Another issue is hidden fields that accept negative values. Can lead to negative balance in bank accounts

Exploiting Web Site Authentication Methods

Common authentication types include
- basic
- forms based
- message digest
- certificate

Basic authentication can be done by exclusive ORing Passwords sent can be XORed with stored values after converting it to binary form of its ASCII equivalent. The resulting value is sent over HTTP. This is a very weak form of encryption

Forms based authentication uses cookie issued to a client Once authenticated, web application generates a cookie / session state variable. This cookie is reused on subsequent visits. Even passwords can be stored in a cookie

Message digest uses MD5 algorithm. It uses username, password & nonce value to create an encrypted value that is passed to the server. Nonce makes it more resistant to cracking & makes sniffing attack useless.

Certificate based authentication
signature of certified authority

Mangal
Date / /20

Mining Job Ads & Analyzing Financial Data

An attacker can collect details of technologies used in an organization by looking at the job ads posted by them in many websites.

Also, financial health of an organization can be used by an attacker.

When one company acquires another, their websites will be merged. During this phase, there will be less security and attacker can gain access to details

Using Google to mine sensitive operation

Google collects sensitive data that must not be revealed to outsiders

Filetype - Searches only within text of particular type of file

Inurl - To search only within specified URL of document

Link - Search within hyperlinks of specific term

Intitle - Searches term within title of document

allintitle

site:python

Exploring domain ownership

IANA (Internet Assigned Numbers Authority) - Responsible for preserving the central coordinating functions of global Internet for public good.

- Manages domain name & addresses.

WHOIS database

- Tool to query info an organization entered when they registered its domain (Can be queried by domain name/IP)
- Internet Corporation for Assigned Names & Numbers (ICANN) collects WHOIS information from domain holders.

- Ex: WHOIS information for smu.edu.

Fields: Registrant (South Methodist University)
Administrative Contact
Technical Contact

Names - Social engineering
Email - Spoofing
Phone nos - Wardialling

Regional Internet Registries Oversees the regional distribution of IP addresses within geographical regions of world.

- Responsible for subdelegating IP addresses to ISPs and end users.

* Managed by IETF (Internet Engineering Task Force)

Mangal
Date / /20

* Designed to aid in network diagnostics and to send error messages.
* Any network device using TCP/IP can send, receive or process ICMP messages.
* ICMP messages have no priority & do not flood the network.
* Some devices consider them as interruptions. So they may be lost / discarded.
* ICMP messages cannot be sent in response to other ICMP messages. Not sent in case of multicast/broadcast/invalid address.
* In case of traffic fragmentation, ICMP message is sent only for first fragment.
* Common type of ICMP message is ping (designed to verify 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 number of hosts, ping sweep is performed.
* Programs that perform ping sweep typically sweep through range of devices to determine which ones are acha

*Drawbacks: Does not identify services in the system — Pings only one system

Date 1/a/20 Mangal

*** Port Scanning

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

TCP/IP basics

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 — three way handshake for establishing connection
* TCP header has 1 byte field for flags.
  - ACK (Acknowledgement)
  - SYN (Seq Nos)
  - URG (To indicate priority data)
  - FIN (Normal shut-down)
  - RST (Abnormal session)
  - PSH (Data delivery without waiting for buffers to fill)

* Terminates session using 4 step Shutdown

Date / /20

Common Scan Types

- TCP Full Connect Scan – Full connection (easily detected)
  Open ports SYN/ACK
  Closed ports RST/ACK
- TCP SYN Scan – Half open
- TCP FIN Scan – Shuts down
  Used on UNIX devices
- TCP NULL Scan – Sends a packet with no flags set
- TCP ACK Scan – Finds Access Control List (ACL)
- TCP XMAS Scan – Toggles flag values.

UDP

- based on speed.
- fire and forget protocol
- Does not issue responses.
- Gives less information in comparison with TCP scan

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 open ports

Idle scan – Uses an idle host to bounce packets off of and make scan harder to trace

Port Scanning Tools

Mangal
Date / /20

Nmap } Command-line
THC Amap }

Superscan } GUI tools
Look@LAN }
NetScan

OS Fingerprinting

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

Passive Fingerprinting

- IP addresses, active systems and open ports have been identified (determined by examining packets)
- Four commonly examined items
  1) IP TTL value - Unique TTL values on outbound packets
  2) TCP window size - Different values for initial window size
  3) IP DF option - Fragmentation different for differing 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 and IP fields

Mangal
Date :/ /20

Initial Time to Live } IP header
Don't fragment }
Overall SYN packet size }
TCP options } TCP header
TCP Window Size }

Active Fingerprinting

- User does not wait for random packets to analyze but voluntarily injects packets into network.
- Methods used in active fingerprinting

FIN probe
Bogus flag probe
Initial Seq No sampling
IPID Sampling

TCP Initial Windows
Ack value
ToS
TCP Options
Fragmentation Handling

OS Fingerprinting Tools

* Nmap
* For reliable prediction, 1 open port & 1 closed port is required.
* Xprobe2 - another active OS finger printing tool

Scanning Countermeasures

Mangal
Date 20

* Focusses on blocking unauthorized individuals from this information
* Intrusion detection – 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, connection is opened
* Securing routers & traffic through routers done using packet filters
* Packet filtering configured through ACLs.
* ACLs allow/block traffic based on header information
* ACL makes decision based on
  - Source IP address
  - Destination IP address
  - ~~TCP flags~~
  - Direction
  - Source Port
  - Destination Port
  - Protocol
  - Interface

Enumerating Systems

* Process of counting by an attacker before launching an attack – Enumeration
  - SNMP
  - Routing devices
  - Vulnerable services.
  -

SNMP Services

Mangal
Date / /20

- TCP/IP standard for remote monitoring & management of hosts, routers & other nodes on network
- Enables administrators to do the following:
  - * Manage network performance
  - * Locate & resolve network problems
  - * Support better network management
- SNMP uses two components - manager & agent. Manager sends & updates request & agent responds
- Management Information Base (MIB) organized in tree structure (contains object property definitions)
- SNMP v1 (Limited security)
  SNMP v3 (Data encryption & authentication)
- Two community strings
  - First string - View configuration of device
  - Second string - Read/write (Changing configuration)

SNMP Enumeration Tools

* Attacker can use default community strings
* Gain access to usernames (half way for attack)
* Use insecure modes of SNMP
*
* 1) Attacks scans port 161 (SNMP)
  2) Uses community strings
  3) Attempts to login
  4) Escalates privilege

SNMP Enumeration Countermeasures

- Turn off that port when not
- Upgrade to SNMPv3
- Different community strings

Routing Enumeration

Routing devices

- Routing protocol routes packe
on routing table
- Can be done statically (for small networks), dynamically based on parameters like bandwidth, cost, delay, distance, load & reliability
- Some dynamic routing protocols — RIP, BGP, IGRP, OSPF

Router Enumeration Tools

- Using browser (Google hacking). Items that you find
  - * Usernames
  - * Encrypted passwords
  - * IP addresses of routers
  - * Access lists
  - * Routing tables.
- Autonomous System Scanner (ASS). Works in d mode
  - * Passive — Listens to routing protocol packets
  - * Active — Discovers routes by queying more (more accurate)
- ASS works with all versions of RIP but not OSPF since it employs link state routing
- To detect OSPF, use SNMP or Wireshark.