SDS Page No.
Date / /

MOD-2

2.1 ✓ Anonymity
✓ Censorship circumvention

2.2 ✓ Intro. to foot printing
✓ Info. gathering methodology
✓ Vulnerability scanning
✓ Whois lookups
✓ Dimitry

2.3 Port scanning with Nmap,
Nessus,
Netcat,
Maltego

SDS | Page No. | Date

Anonymity

- Situation in which, the acting persons identity is unknown, the person is not reachable, non-identifiable or not trackable.
- Thus, reducing the account of the actions performed by him.

→ In osi model → Applicatn, Anonymity, Presentation, session, transport, Network, Data link layer & physical
This is the pattern followed,

→ Here Anonymity layer has function → to hide the source destination & contents of internet flows from eavesdropper.

→ Challenge here is to define & quantifying anonymity, building system for deanonymizatn. & maintaining performance.

* Threats to anonymity

1) As our IP address is directly linked to us, Internet service providers (ISPs) can store our data for several years & law enforcement can use these records in court as evidence. (use these as legal documents).

2) Our browsers can be tracked via cookies, html tags, etc, leading to declaration of our data to public (data leak).

3) Browser fingerprinting,
Tracking down our activities on browser, can leak or can be used to identify us.
Done by checking the websites we visits & tracking our login's & types of link we visit.

4) Wireless traffic can be trivially intercepted,
Wireless traffic such as that transmitted over wifi can be intercepted by malicious actors using tools like Airsnort & Firesheep
w/o encryption, this traffic can be intercepted & read & analysed, potentially compromising ~~your~~ anonymity

* Reasons for Anonymity

1) To protect the privacy
→ Anonymity shields us from being tracked by other third party applications:
↳ done to create targeted advertisements eg
→ Anonymity allows individual to browse sensitive content w/o fear of being identified.

2) Protection from Prosecution
→ In some places, freedom of speech is not practiced at a good extent & the certain opinions from people may lead them to legal actions.
→ Anonymity provides this layer of protectn for them, & thus can access the information that may be controversial or illegal.
→ eg: downloading copyrighted material w/o legal consequences.

3) Preventing chilling actions
→ Anonymity enables individual to voice their opinions on unpopular & controversial topics, w/o revealing them. Thus reducing risks of legal consequences.

fingerprinting → consequences → on the info collected, these malicious actor can create a fake profile of the person whose info is collected.

SDS Page No. Date / /

* Data that is generally masked /anonymized

1) Personally identifiable information (PII), info that can directly identify an individual & their personal info.

2) OS & Browser information, these data can be used to create a unique 'fingerprint', that may identify the orginal person

3) language information, basically revealing the background of a person, may sometime reveal the location of person.

4) IP address, IP is already an unique identifier, that can be tracked down also revealing users activities.

5) Amt of data sent & received, volume of data exchange may sometime reveal the users intentions towards some thing.

6) Traffic timing, timing of data transmission can provide insights into users behaviour & about their activities.

* Achieving anonymity

1) Use of Proxy Chains →

- ProxyChain allows us to use SSH, TELNET, FTP etc other internet applications from behind HTTP (HTTPS) & SOCKS (4/5) proxy servers.
- Proxying refers to the technique of bouncing internet traffic through multiple machines to hide the identity of og. machine.

→ P.C. is a tool generally used by hackers,

[we have a list of proxies here (proxies → machines)]

→ Proxychains can be mixed up with different proxy type in a list

→ also supports chaining methods/options like random, that takes a random proxy in the list stored in a configuration file.

OR

chaining proxies in exact order.

→ also supports a dynamic option, that excludes dead or unreachable proxies.

2) Use of VPN ⇒

- A virtual private network (VPN) extends a private network across a public network & enables users to send & receive data across shared or public networks as if the computing devices are directly connected to private network.

→ VPN is created by virtual point-to-point connection using dedicated protocols over existing networks.

→ From a user POV, resources available within the private network can be accessed remotely

this creates a simple basic level of security.

3) Use of TOR networking ⇒

- TOR directs internet traffic through a free, world-wide overlay network consisting of more than 7 thousand relays to conceal a users location from anyone who's conducting a network surveillance.

→ TOR uses onion routing to anonymize one's network traffic. Onion routing is done by implementing encryption in app. layer of comm. protocol, nested like layers of onion.

→ TOR encrypts the data, including destinations port & IP address & sends it via a virtual circuit that has random selection of TOR Relays.

→ Each relay decrypts the layer of encryption. & at end the entirely decrypted data is sent to its destination w/o revealing the IP address.

Here back tracking is like peeling slices of onion, but each slice i.e. tor relay provides user with anonymity.

But it makes the req. slow to execute.

Censorship

- A legal control or suppression i.e. restriction of what can be accessed, published or viewed on internet.

Done via various filtering techniques & site blocking.

* Areas of censorship

a) Copyrights ⇒ concept that grants creators of the original work, exclusive rights to their creations.

→ The copyright laws are intended to protect the og. work of creator & providing creator with control over how the creation can be distributed.

b) Defamation ⇒ communication of false statements, statements with intent to harm reputation. Censorship acts as removal of defamatory content to prevent harm to reputation.

c) Harassment ⇒ Involves offensive behaviour that is intended to disturb, upset or intimidate individual or group of people STS or Defamation (censorship ---).

d) Obscene material ⇒ statements or acts that are inappropriate based on moral, religious, cultural or traditional standards of society.

→ May include explicit content or content that may spread hate.

→ (censorship .... etc)

* Technical Internet censorship method

1) Internet Protocol (IP) address blocking

→ Involves blocking specific IP's & not allocating them access to online services.

→ This can be circumvented by using VPNs or Proxy servers.

2) DNS filtering & redirection

→ altering the DNS responses to block access to specific domains or redirect to alternate website.

→ can be circumvented using alternative DNS servers or VPNs.

3) URL filtering

→ Blocking access to specific URL's, done at network level, using firewalls or web proxies.

4) Packet filtering

→ inspecting the data packets sent over a network & blocking packets that meet certain criteria.

used to block access to certain type of content

Doing this may impact network performance.

SDS | Page No. | Date / /

5) Network disconnection

→ completely cutting of internet access or specific network services.

→ Generally used during political unrest or to suppress.

6) Portal censorship & search result removal

→ controlling access to internet protocols or search engines & removing or censoring search results that may be objectionable.

* Non Technical internet censorship

a) Diff. publishers, authors, ISP's may receive formal & informal requests to remove, alter or block access to specific site or content.

b) civil lawsuits → publisher, authors ~~or~~, ~~ISPs~~ ISPs may face civil law suits claiming the content published by them may affect / violate the rights.

c) Access to internet may be limited due to restrictive licensing policies or high costs, lack of necessary infrastructure, all because of restricting licensing policies, connectivity issues,

d) confiscation & destruction of equipment → in some cases, org may confiscate & destroy equipments used to access info. May lead to activism. coz of suppression.

OpenNet Initiative (ONI):

→ Main goal is to monitor & report on internet filtering & surveillance practices by nations.

→ Project employees a no. of technical means and also international network of investigators, to determine govt. run filtering programs

Magnitude of censorship is classified as ⇒

a) pervasive → large portion of content is blocked.

b) substantial → no. of categories are subjected to medium level of filtering or many categories are subjected to 1000 level filtering.

c) selective → a small no. of specific sites are blocked or filtering targets a small no. of categories.

d) suspected → suspected but not confirmed whether site is blocked.

e) No evidence → No evidence of blocked website.

Circumvention

Refers to the methods or techniques used to bypass or overcome censorship.

Techniques are → VPNs, Proxy servers, TOR

- DNS Tunneling ⇒ by encrypting internet traffic within a DNS query, user can access blocked data o/o censorship filters.

SDS | Page No.
Date / /

Footprinting

- Footprinting is the part of reconnaissance process, that is used to gather info. about the target or network.
- Step where hackers gathers much information as possible to find ways to intrude into a target system or atleast decide what types of attacks will be more suitable.

→ Essential aspect of footprinting involves level of risk associated with org's publically accessible data.
→ On completion of footprinting, we obtain a blueprint of the security profile of target organisation.
(targets security system)

Types

a) Passive footprinting ⇒ gathering info about the target w/o direct interaction, mainly done when info. gathering activities are not to be detected by target.
Info collected includes →
⇒ finding info via search engines
⇒ performing people search using social networking skills
⇒ fetch infrastructure details of target organisation.
⇒ determine os of target
etc.

b) Active footprinting ⇒ gathering info about the target with direct interaction. Target may recognise the ongoing info gathering process.
Info collection includes →
⇒ querying published name servers of target.
⇒ Extracting meta data of published docs.
⇒ collect info. via email tracking.
⇒ perform whois lookup, social engg, traceroute.

* Info. obtained in Footprinting

By conducting footprinting across various network layers, you can gain info such as network blocks, specific ip addresses, etc.

a) Network info is gained by performing Whois analysis etc & info about domains, network blocks, IP addresses, etc are found.

b) System information is gathered by performing network footprinting, DNS footprinting, etc. & info about user, passwords, etc is gathered.

c) Organisation info is collected from passive footprinting, & in active FP. you can query targets domain name against Whois DB.

Info about, employees, location details, etc is collected.

* Threats to FP. include → social engineering (intentions are not clear here), Information leaks (easily found by hacker), Privacy loss, Business loss.

SDS Page No.
Date / /

Methods of information Gathering

3 methods → Footprinting,
Scanning,
Enumeration.

a) Footprinting (explain fp.).

b) scanning →

- Another essential step of footprinting is scanning, i.e. a package of techniques & procedures used to identify networks, hosts, ports etc.
- To find out the possibility of network security attack, pen tester use vulnerability scanning, using this technique, one can find vulnerabilities, missing patches, weak encryption algorithms.

three types of scanning

(i) Port scanning

→ Hackers & pen tester use this to search for open ports to get into the system.

→ Hackers need to identify the live host, firewalls, device attached to system, os used, etc.

→ Then hacker fetches IP address of victim organisation by scanning ports of UDP & TCP.

(ii) Network scanning

→ The three way TCP/IP handshake is exposed, a synchronised packet sent by client to start a connection, to which server responds with a syn/ack packet. to which client again responds by sending ack packet to server, thus connection is established

- while the syn packet is sent, the port is open & able to listen anything, thus can be used as an vulnerability & for that SYN Scan is done.

- ~~Test~~ When packet has PSH, FIN & URG flag, the target doesnt responds but an RST/ACK packet is sent if port is closed & no ~~Test~~ response if port is open → XMAS Scan

- FIN Scan is also same with FIN flag only.

- check the Ip addresses sequence no. & port scan response and send the syn packet to target using spoofed IP, IDLE Scan

- ~~II~~ Inverse TCP Flag Scan & ACK Flag Probe Scan.

(iii) Vulnerability Scanning

- Process of identifying vulnerabilities or weakness on a target system.
- Vulnerability scan can locate vulnerabilities w/o exploiting them. And is generally done by org's own employees, or that ~~can be expressively~~ authorised by company.

- Vulnerability scanning uses various tools →
  - → Nmap = to extract info like os, packet filters, firewall types,
  - → Angry IP scanner = scan for system in given IP range.
  - → Hping = network scanning tool & command line packet crafting
  - → superscan = TCP port scanner, used for pinging.
  - → Zenmap = to detect port scanning
  - → Net scan tools = set of tools to perform web sippers, etc.

SDS Page No.
Date / /

⇒ main objective of doing this is to find open ports, live hosts, services running on system, victim os.

c) Enumeration

- Enumeration process, where info is extracted from system like machine names, user names, network resource, shares & services.
- Here an active connection is established with system via hacker. & hacker tries to gain more target info. ~~about system~~ by performing direct queries.
- Thus penetration testing - enumeration phase is risky as you are directly contacting the target.

types of enumerations

i) NetBIOS enumeration ⇒ Network Basic I/O system (NetBIOS), attacker can perform DOS on remote machine.

ii) SNMP enumeration ⇒ SNMP is used for managing devices & works on client-server, thus network communicates with host-server machine
This SNMP req. can be access & manipulated. thus fetching information about shared devices, routers, etc.

iii) LDAP enumeration, ⇒ light wt. directory access protocol, A dir. service is used to store users record. The information transmits betn server & client & ~~hacker~~ LDAP handles remote queries to server & via this query sensitive info can be accessed like username, dept, etc.

iv) NTP enumeration → Network time protocol, if attacker queries NTP, it can enumerate the host list that is connected to NTP server

v) SMTP enumeration → simple mail transfer protocol, used to send mails through DNS & has commands like

Verify → to validate user,

EXPN → identify list of mails & deliver to aliases.

rect to → define msg's receiver.

using / exploiting these commands, attacker can find valid user on SMTP server.

vi) DNS Enumeration → DB to store domain names of IPs, DNS enumeration is possible when DNS primary server is requested by zone transfer & pretends like a client & may reveal sensitive info. about domain records.

vii) Windows & Linux / unix enumeration.

Who is Lookup

- A protocol used to find the owner of internet resources, like a domain, a server, an IP address
- Here just info. is been retrived from the dB about owners of stuff on internet

Details about any domain are stored in a DB & selected, when queried in whois lookup.

→ Helpfull in finding the info. about the target, various data like, IP add.; location, history, Registered country, company name, email, domain status etc can be found.

SDS | Page No.
Date / /

Dimitry → info gathering tool.

- Dimitry stands for Deep Magic Information gathering tool.
- A free-open source tool that is available on Github. and is used for gathering information.

- Dimitry is a command line tool, helpfull in gathering info, that can be used for social engineering.

Uses of Dimitry tool

- used to search target's subdomains.
- Find open ports on target system
- used to do a TCP scan.
- used to get email addresses associated with target domain.
- used with WHOis services, to get target information such as registered domains, name, address, contact info.
- used with NetCraft services to gather info. such as OS, webserver details, hosting service details, etc.

* Flags used in Dimitry

- (-o) choose location where o/p is to be written.
- (-i) perform whois lookup on target IP.
- (-w) perform whois lookup on host's domain name.
- (-n) retreive all Netcraft info for a specific target.
- (-s) used to search targets subdomain.
- (-e) search all emails associated with target.
- (-p) perform TCP port scanning

2.3

Port scanning using

a) Nmap

- Nmap is an security auditing (reviewing) tool used to enumerate target. Extensively used tool for reconnaissance.
- Used to probe the target network for active hosts, port scanning, OS detection, etc.
- Port scanning is one of the feature of Nmap, wherein too detects the status of the ports on the active host.

We can scan the set of ip addresses for open ports using nmap command.

nmap -sS range1 - range2 ⇐ command / range = ip add.

Types of port status ⇒

- open ⇒ given port is open and actively running a service.
- Filtered ⇒ port might be hidden behind firewall.
- closed ⇒ port is closed.

- They have TCP connect Scan (-sT),
  TCP SYN Scan (-sS)
  UDP Scan (-sU)
  TCP NULL Scan (-sN)
  TCP FIN Scan (-sF)
  TCP XMAS Scan (-sX).

SDS | Page No.
Date / /

b) Netcat

- The Netcat utility program supports a wide range of commands to manage network & monitor the flow of traffic.
- Netcat functions as a backend tool that allows for port scanning & listening

→ nc -z -v site.com will run a basic port scan for specified website / server. & o/p s a list of ports and their status.

→ when diagnosing a network issue, executing an netcat portscan will lend you all status of given ip address or domain.

we can scan a range of ports & a set of individual ports.

⇒ NetCat also provides with. File transfer, Backdoor shells, DNS lookup, Verbose scan, etc.

c) Maltego

- An open source intelligence & forsencis app. used during reconnaissance period.
- A platform developed to deliver a clear threat picture of the env. or the org.

→ It demonstrates the complexity & severity of single point failures in the existing infrastructure.

→ one of the best info. gathering tool & can query all types of data integration with WHOIS, TINEye, etc.

d) Nessus

- Primarily known as vulnerability scanner & not a port scanner, but can perform port scanning.
- When Nessus ~~scans~~ scans a system, it basically ~~scans~~ performs variety of tests to identify vulnerability & in which nessus performs port scanning.

→ In Port scanning → once the live hosts are identified, Nessus may conduct port scanning to know what ports are open to each host.

May use → SYN scanning, TCP connect scanning, UDP scanning } OFC Nmap.