AUTHENTICATION BASED ATTACKS

Authentication Steps:

Identification Step: Present an identifier to the system, could be a security principal.

Verification Step: Is there something that validates or verifies the identity or security principal presented.

Authentication systems:

- Windows: Credential providers, Windows 10
- Linux: Plugable Authentication Modules (PAM)
- CAS, SSO

Authenticaton Factors:

- Something you know: Password, PIN, Security Questions
- Something you have: Smartcard, Physical Token
- Something you are: Fingerprint, Iris
- Something you do: Voice pattern, Handwriting

Threats for Authentication Factors

- Threats to something you know:

Password authentication: Phishing Poor password management techniques, key logging, other eavesdropping.

Password based attacks: Password cracking, rainbow tables password storage attacks.

Secret Questions: Easy to obtain answers

- Threats to something you have:

RFID copying

- Threats to something you are:

Facial recognition systems may fooled with a print of your face. False positive or false negatives.

- Overall security issues:

Eavesdropping, replay, malware, denial of service, host and client based attacks.

NETWORK AND SYSTEM BASED ATTACKS

- First known virus is creeper.
- Three categories of malwares are viruses, trojans, worms

Common Types of Attacks

1.Active Atacks (much common)

Attacker has ability to see/manipulate real-time traffic: sniffing, eavesdropping, spoofing, denial of service.

- Sniffing

  Reading monitoring or capturing full packets from a device. Well known tools are wireshark,tcpdump.

- Eavesdropping

  Similar to sniffing but sometimes without the full packets usually used in 1to1 communications. Well known tools used wireshark, tcpdump ,ettercap. Most network attacks are in form of sniffing, eavesdropping is a form of it. It is serious threat If done incorrectly, it can result in a noticeable change in connection which can be detectable.

- Spoofing

  Pretending to be someone/something that you are nor. Well known tools used: ettercap. May only work on non enterprise systems. Enterprise systems have detection mechanisms. It is not complex because of software. ARP spoofing, you can get in the middle of two way conversation and say the router of the gateway is not the source of information, I am the source of information. So you eavesdropp, spoof and manipulate the traffic. Dynamic ARP Inspection can be used to prevent ARP spoofing.

- Denial of Service

  It is an attack on the availability of a service by blocking or overwhelming communication or resources to that service. System resources are network bandwidth, CPU, memory, application resources are web server, DNS server etc.

  Effects the ability to use resources. Well known tools are botnets, HOIC, LOIC etc. It need high level resources to attack, so it is not common.

  Ping attack: Multiple pings either overwhelm the server or overwhelm the connection. Can be prevented by disabling ping replies or responses either in software on the server or through firewall rules.

  SYN attack: Send a half open SYN packet to the server. Multiple half open queries overwhelm software resources typically in open sessions. Can be prevented with session timeout rules. Very effective attack, but most operating systems can handle it.

Flooding attack: Send various requests to overwhelm resources. Depending on what the software is on the other side is how the attack is successful. It can be prevented with application memory handling or firewall rules.

Reflection or Recursion attack: Sends requests on behalf of another system. Server asks another server that is not well protected to ask something on behalf of it. Can be prevented by disabling recursion or at least lock down recursion to inside the network. DNS or NTP could be used for this kind of attacks.

Defenses: Firewalls or operating systems rules are good defences, also backups are useful for stop denial of service attacks

2.Passive Attacks

Attacker can read data and use the data for other purposes: stems for sniffing traffic, compromised data. Most passive attacks stem from previous active attacks. Attacker uses the information obtained form sniffing or eavesdropping.

Password attacks: unencrypted password reuse

Replay attacks: using tokens or cookies from traffic stream

Protection form Network based Attacks

- Keep up to date on network security patches
- Utilize enterprise grade hardware
- Segment your network
- Protect network equipment

Wireless based Attacks

SSID (Service Set Identifier)

Channel bonding uses two of the frequencies together to get a higher speed.

The base station serves up an SSID, or the access point for example. So, for example, at the university we have two actual SSIDs. One is called the UCCS-Wireless and the other one is called UCCS-Guest.

Threats to Clients:

- Connecting to a spoofed SSID: attacker or owner can sniff traffic
- Connecting to unsecured SSID (open): attacker could perform a man in the middle attack

- Denial of service: sending disconnects. Can kick all other clients off

Threats to infrastructure

- Signal interference: too many AP sor SSIDs
- Spoofing SSIDs
- WPS: wifi protected setup
- Backdoors

SSID is secured with Wireless Equivalent Privacy WEP. Encryption is not built into Open SSIDs

CLOUD SECURITY

SaaS: Software as a service: software on your device

PaaS: Platform as a service: operating system

IaaS: Infrastructure as a service: computer itself with hardware like servers.

Others: Network, data

Cloud Components are;

- Rapid
- Flexible architecture
- Resource pooling
- Resource measuring

DATABASE SECURITY

Database is a structured collection of data.

Database Access Control

- Grant
- Revoke

Database Access Rights

- Select
- Insert
- Delete/Drop
- Update

Role Based Access Control RBAC

Role based access control is used to increase security; database owneer, administrator, system administrator

Database Security Threats

SQL Injection

Goal is to extract information from database. One of the most common types of attact, exploited through insecure web applications.

Inference

Attacker can use queries to infer database structure or content, occurs when too much access is given to a user.

Encryption

Database encryption is usually not performed. Attacker may be able to grap unencrypted data if encryption is not performed.

COMMON VULNERABILITIES

Missconfiguration

Incorrectly configuring software safe guards, usually in web applications, #5 of OWASP.

- Disabling default accounts – wireless
- Not setting update schedule – Windows, Linux
- Removing setup files – Wordpress (Must be removed)
- Closing open ports – Linux (Must be closed)
- Using insecure ports -LDAP
- Not setting a password
- Unnecessary services – Linux
- Default certificates – Lenovo

Operating Systems

Kernel – Ring 0 (most priviledged)

User Level – Ring 3 (least priviledged)

Some OS have rings 1 and 2

Most OS have just 2 rings 0 and 3.

Securing OS

- Use least privilege.Rooting escaletes privileges the users.
- Remove unnecessary services, apps and protocols
- Use antivirus
- Use best practices
- Hardening guides – CIST, NIST, NSA

Buffer Overflow

If data is overwritten through poor programming, other code can be injected causing other program or operating system access. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

How buffer overflows are found:

- Testing or fuzzing
- Reverse engineering of code
- Looking at program execution
- Once vulnerability is foundi the attacked can put their own data in

Shell code is code that is used by an attacker to usually gain access to a part of the operating system. It is used in the buffer that overwritten. An attacker must understand how to use shellcode and what the underlying architecture is in order to exploit. It can launch remote sessions, reverse remote sessions, tear down other defenses.

Common defences

Compile time:

Stack protection- stack guard

Safe library use

Run time:

Memory randomization – Randomize the memory locations

OS memory protection – EMET

WEB BASED APPLICATION RISK AND THREATS

OWASP TOP 10 (Open web application security project)

Designed to education about secure software. Every year top 10 list represented.

A1- INJECTION

Injection flaws have been at the top of the list for years. Covers:

- SQL

- Command
- XXE
- LDAP

Attacker sends untrusted data to system that interprets the data.

A2- BROKEN AUTHENTICATION AND SESSION MANAGEMENT

User sessions can be hijacked. Information that can be stolen or accessed. Poor authentication coding methods allow attackers to gain access.

- Session ID
- Usernames
- Passwords
- Accound information
- Cookies

A3- CROSS SITE SCRIPTING

Attacker execute scripts via a browser. The appliation uses untrusted data in the constrocution without validation or escaping. Can inject viruses or get session id

A4- BROKEN ACCESS CONTROL

Attacker use insufficient security measures to bypass authentication mechanisms. Change in account parameters values to allow access.

A5- SECURITY MISCONFIGURATION

A6- SENSITIVE DATA EXPOSURE

Data exposure can happen a number of differrent ways. Can be used in conjunction with other methods. Encrypting data may prevent this problem.

A7 – INSUFFICENT ATTACK PROTECTION

A8- CROSS SITE REQUEST FORGERY

A9- USING THE COMPONENTS WITH KNOWN VULNERABILITIES

A10- UNDERPROTECTED APIS

DATA BREACHES

Different ways information comes out; watchdog agency, law enforcement, compay themselves.

What has been compromised; financial data, social security numbers, usernames, passwords, health data