Automated Attack & Penetration Tools

Mangal

*Vulnerability is a defect in software design like coding error, drag, design flaws. Not all vulnerabilities are addressed. Vulnerability assessment tools help to detect such vulnerabilities.

Why attack and penetration tools are important

* Helps analyze overall security & degree of security of assets
* Use of these tools can help answer the following questions
  - More / few security countermeasures to be implemented?
  - Organizations true security
  - Effect of security breach.

Situations in which tools must be used:

* Audits & reviews: To determine whether systems are properly patched, specific security policies & requirements are followed,
* Network evaluations: Scanning, vulnerability assessment scanning
* ~~Penetration~~ tests: Focused on finding exposed systems & vulnerable targets. Ethical hackers conduct these tests

Automated Exploit Tools (Vulnerability assessment tools)

Mongal
Date / /20

Metasploit:

- Open source tool
- Used by network security professionals to perform penetration tests, regression testing, etc.,
- Basic approach
  - * Select the exploit module
  - * Choose configuration options
  - * Select payload
  - * Launch exploit & wait for response.
- Three basic ways in which it can be controlled
  - * msfweb : Simple point & click interface
  - * msfconsole : Console-based interface
  - * msfcli : Command-line interface

Metasploit Web

* Allows user to run Metasploit through web browser
* Windows System : Start → Programs → Metasploit → MSFWEB ⟹ Takes you to command prompt with many web variables that can be entered in web browser
* Three options in Metasploit

Mangal
Date / /20

- Exploits: Default option. Contains list of exploits. Select the exploit ~~you need~~ and all information about the exploit gets displayed

- Payloads: Defines payload type. Metasploit has 106 payloads. Only certain code can work for specific exploits.

Configuration page details series of requirements and optional fields for exploit & payload.

- Sessions: Serves as staging point in all ongoing open sessions. Two options on Session page: Session Break shuts down the session to remote system using an interrupt & prompting user to end session via command shell; Session kill to open a dialog box prompting the user to kill the session immediately.

Metasploit Console

* Provides the user control over delivery of exploi
* 4 command line options
  - -h Display the help screen
  - -s Read & execute a command
  - - Display option information
  - -q Dont display start screen upon startup.

* 9 steps to execute an exp

Mangal 20

[showencoders setg encoder] — Listing default encoder & nop/generator

[showexploits] — Display available exploit modules (Information transferred from temporary to global env)

— Select a module

— Display appropriate target platform (Main mode → exploit mode)

~~[sho~~] — Set options (exploit & advanced)

[show payloads] — Set payload

— Check functionality (Returns no of FPs & FNs)

— Launch exploit.

Metasploit

Framework engine ⟷ Info exchange ⟷ Exploit environment

(Global & temp variables)

Metasploit Command Line Interface

- msfcli has no access to OS
- Can be run as script with another program
- 5 steps in executing
  - Select exploit module
  - Select platform
  - Select payload
  - Select payload & exploit options
  - Execute exploit

Updating Metasploit

- /msfupdate -u -f

Mangal
Date / /20

Exploit Tree

- Categorizes all available exploit code (Repository)
- User of the project can mirror the contents of ExploitTree project & keep a copy on local system that can be updated when database is revised.

CoreImpact

- Point & Click automated exploit tool.
- Uses step-by-step approach to penetration testing
- Exploit mode: Browse files, set the victim's system as source & open mini cmd prompt on victim's system
- Advanced mode: User takes control of victim's system.
- Pivoting: Use compromised machine to compromise another

CANVAS

- Written in Python portable to Windows & Linux.
- More advanced than Metasploit but needs license
- Add targets manually

Determining which tools to use

Mangal
Date / /20

* System level scanners
* Disruption factor (Which processes must be put on hold)
* Intrusive scans can disrupt network / computer systems as part of operation
* Mostly automated (generates report after scan)

Defeating malware

Malware - Software that is harmful to computer
Includes virus, worm, trojans & Spyware.

Evolving Threat

* Computer virus in 1984
* Brain Virus - Basit & Amjad (1986 - Pakistan)
* Israeli writer (Amnon Jackont) - Section of his book released in Internet - Keystroke logging (Trojan)

Viruses & Worms

* Large category of malicious code
* Can display messages / ~~work~~ make programs work erratically

Viruses

* Early viruses - market developers as skilled coders/ destroy data

Windows OS

* Brain virus targeted floppy disk's boot sector & infected 360K floppy disks.
* Virus code was made to reside in first 512 bytes of boot sector & rest in 6 different areas of floppy disk
* When system is booted, the boot sector is checked by DOS.
* Lehigh virus kept track of count of infected files. When it reached some count, it wiped out those data from floppy disk.
* Mac OS infected with MacMag that drew world image on computer screen & Scores virus that prevented users from saving the data.
* Damage caused by Linux viruses is less in comparison with Windows viruses. Since Linux is opensource, there are no of programs operating in it & it is difficult to find the dominant one.
* Three ways of propagation of virus.
  - Master boot infection: Attacks boot record of floppy disks / hard drives
  - File infection: Relies on user to execute a file. Renames the program & makes the format to appear different.
  - Macro infection: Infects application and virus instructions are executed when application is clicked.

Date / /20

* If viruses spread quickly and [illegible] fast infection [illegible] If
as possible, they are called ~~they~~ is (are) called as
they limit the rate of infection,
sparse infection viruses.

* Some viruses load themselves into RAM instead of
living exclusively in files. They are called RAM
resident files.

* Viruses that are hard to detect by anti-virus software
Multipartite virus uses more than one propagation
method. Ex: NATAS infects boot sectors and program
files. Polymorphic viruses can change their signature
every time they replicate and infect a new file.

* Three components of a polymorphic virus: encrypted
virus body, decryption routine & mutation engine

* Process of polymorphic infection
  - Decryption routine gains control over computer, decrypts
  virus body & mutation engine
  - This routine ~~controls~~ transfers computer control to virus
  - Virus replicates itself & mutation engine in RAM
  - Virus invokes mutation engine which generates
  new decryption routine
  - Virus encrypts virus body & mutation engine
  - Virus appends new components to a new
  program

* Since two infections are different, virus scanner cannot detect

Mangal
Date / /20

* Stealth viruses hide their presence from both OS & AV
  dy - hiding change in file date & time
  - hiding increase in infected file size
  - encrypting themselves

* Virus hoax

Worms

* Do not attach to a host file but self-contained & spreads across the network automatically

* Melissa virus - Spread through email. Enticed users with a file containing UN & Pwd to access contents of websites ~~Those who used it were~~ Emails to 50 users from their inbox were sent automatically causing overwhelming network traffic. Normal.dot template file in Windows was installed & files infected when transmitted through ~~the~~ email gets to compromise systems

* ILY virus using VBS

* Anna Kournikova Virus created using a tool called VBS Worm Generator

* Code Red Worm attacked one computer & targeted other systems

* Nimda, Slammer, Sasser, MyDoom

Detecting & Preventing

Mangal
Date / /20

Integrity of programs to be checked ~~during~~ MD5
email attachments

Sheep dip system — To screen suspect programs & is connected to a network only under controlled conditions. Can be used to examine suspected files, incoming messages & attachments

Prevent viruses using 5 steps

- Install AV
- Keep AV up to date
- Don't open attachments from stranger.
- Keep system patched
- Send attachments as PDF

Others: Don't use mail program like MS Outlook.

Antivirus

* Norton * McAfee

AV uses following techniques to check files & applications for virus

- Signature scanning: Check beging & end of EXE files
- Heuristic scanning: Check for irregular/unusual instructions
- Integrity checking: Checksum & hash on EXE files
- Activity blocking: Runs when system is on. Prevents virus from infecting other file.

Trojans – Programs that pretend to do one thing but perform another malicious act.

Mangal
Date / /20

Infections

* No free lunch
* Email – Check attachments. Social engineering
* Physical access – Copy Trojan Horse to system through USB port / CD-ROM drives
* Instant messaging (IM) & Internet Relay Chat (IRC)

Symptoms

* Varying levels – unstable to complete system failure
* Total control of the system with the hacker

Well-known Trojans

* NetBus – Easy innovator that targeted Windows 9x. Redirect IP from port to another IP address via server machine
* Back Orifice 2000 – Backdoor access tools that supports encryption to perform communication between client & Server

Mangal
Date / /20

Subseven: Changes its signature & difficult for antivirus tools to detect
Has two parts
- Client program that hacker runs on his machine
- Server that must be installed to victim's computer.

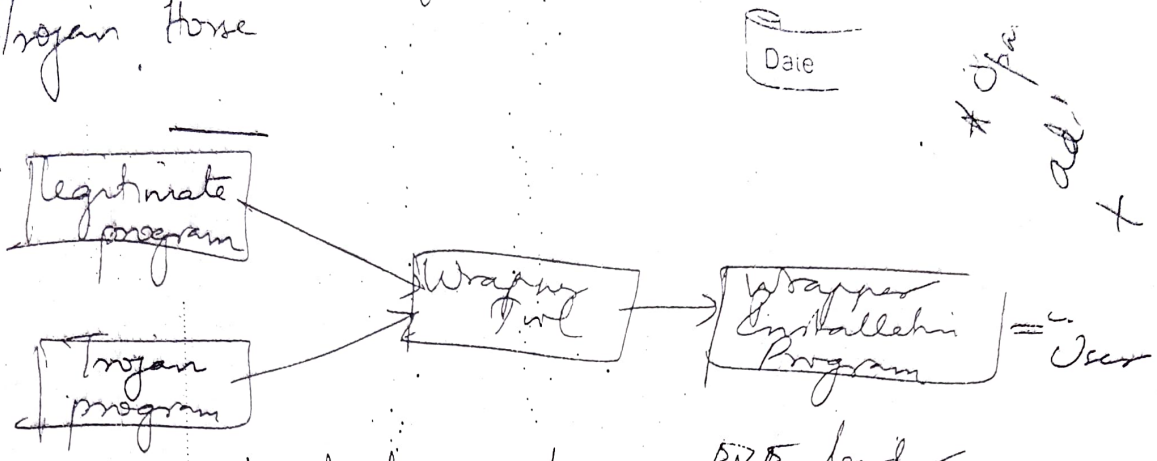
Modern Trojans

* Does not focus on monetary benefits
* Brazilian music industry targeted by Trojans in 2006 & 2007
* Phishing schemes to trick users to download & install customised Trojans — Make victims enter bank account information which is sent to thieves.
* Trojans that steal password. Hackers can design Trojans to send them back the stolen passwords

Distributing Trojans

* Wrapper can make Trojans slip past users defense like Antivirus
* Wrapper - Program to combine 2 or more executables into a single packaged program

* After installation of executable, wrapper Trojan Horse



* Wrapper aka binder, packager, EXE binder ...
* Some programs get joined using wrapper. Others bound 3/4/5 or more programs.
* Examples of wrappers
  - eLiteWrap — SaranWrap
  - TrojanMan — Teflon Oil Patch

Rootkits

* Collection of tools that allow an attacker to take control of a system
* Once rootkit is installed, attackers come & go
* Contain log cleaners that remove traces of attackers presence from log files
* 2 types
  - Replaced binaries in Linux — Can be detected because of changed size of Trojaned binary

zibots – Program ...
addresses from Internet in order
to build mailing lists for sending spam

Mangal
Date 1/1/20

* Munging to foil spambots ← Email address deliberately modified so that a human reader can decode it but a spambot cannot.

Phishing

Fake website similar to real one can ask for credentials of user's account information & ~~use it~~ these details could be used by attacker.

Firewall

Design goals

1) All traffic must pass through firewall
2) Only authorized traffic defined by local security policy will be allowed to pass
3) Immune to penetration (Trusted system + Secure OS)

4 techniques to control access & enforce security policy

* Service control: Type of services that can be accessed
* Direction control: Direction in which particular service requests may be initiated & allowed to flow through firewall
* User control: Service access based on user

* Behavior control: Controls how particular services are used.
Eg: Spam filtering in email to a particular extent

Capabilities within scope of firewall

* Defines a single choke point that keeps unauthorised users out of protected network, prohibits vulnerable services, provides protection against IP spoofing & routing attacks
* Provides location for monitoring security related events
* Convenient platform for Internet functions (N/w address translator, N/w management functions)
* Platform for IPSec.

Limitations

* Cannot protect against attacks that bypass the firewall
* Does not protect against internal threats
* Cannot protect against transfer of virus infected program

Types of firewalls

1) Packet filtering router: Appl to each incoming IP packet & forwards. Filtering rules based on
- Source IP address
- Source & destn
- IP protocol f
- Interface

* More sec
* Disadvantage

* Packet filter – List of rules based on matches to fields in IP/TCP header.
Match to rule → Take necessary action.
No match – Take default action
Cases for discarding & forwarding.

Mangal
Date / /20

Stateful Inspection Firewalls

Packet filtering → Vulnerability that can be exploited by unauthorised users.

* Tightens up TCP traffic by creating a directory of outbound TCP connections. An entry for each currently established connection. Now, incoming traffic to high numbered ports for those packets in the profile of directory

Application-level gateway

* Proxy server
* TCP segments are relayed based on valid user ID & authentication information when user contacts the gateway
* Supports specific features permitted by N/w administrator
* More secure than packet filters. Easy to log & audit all incoming traffic at application level.
* Disadvantage – Additional processing overhead over each connection

Circuit - level gateway

* Does not permit end-to-end TCP connection. Sets up 2 TCP connections - one between itself and TCP user on inner host and one between itself and TCP user on outside host
* Relays TCP segments from one connection to other without examining the contents
* Can incur processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data
* Example:- Socks package
  * Socks consists of server, client library & socks-ified versions of several standard client programs.

Bastion Host

* Executes secure version of OS
* May require additional authentication before providing proxy service:

Each proxy

* Configured to support some of application's command set & access permitted to only some of the host systems
* Maintains detailed audit information & each proxy module is a small software package designed for network security.