

AN TOÀN MẠNG MÁY TÍNH

#02: CÁC KỸ THUẬT, GIAI ĐOẠN TÂN CÔNG CƠ BẢN

ThS. Lê Đức Thịnh, UIT

Nội dung

1. Các thách thức khi làm việc với an toàn thông tin
2. Các kỹ thuật tấn công, phòng thủ cơ bản
3. Hackers/Cibercrimes và động lực
4. Các giai đoạn của một cuộc tấn công

1. Các thách thức về an toàn thông tin



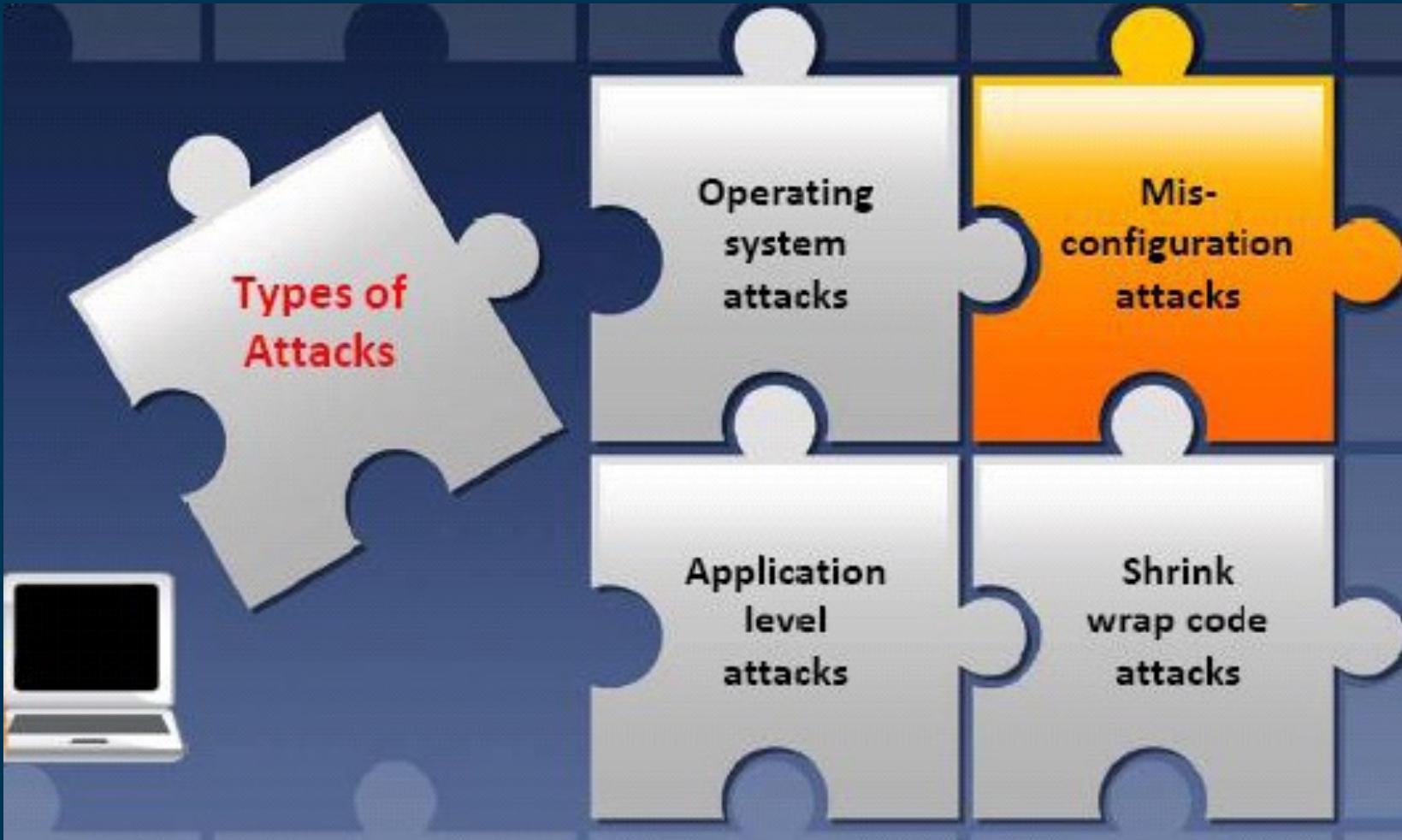
1. Các thách thức về an toàn thông tin (tt)



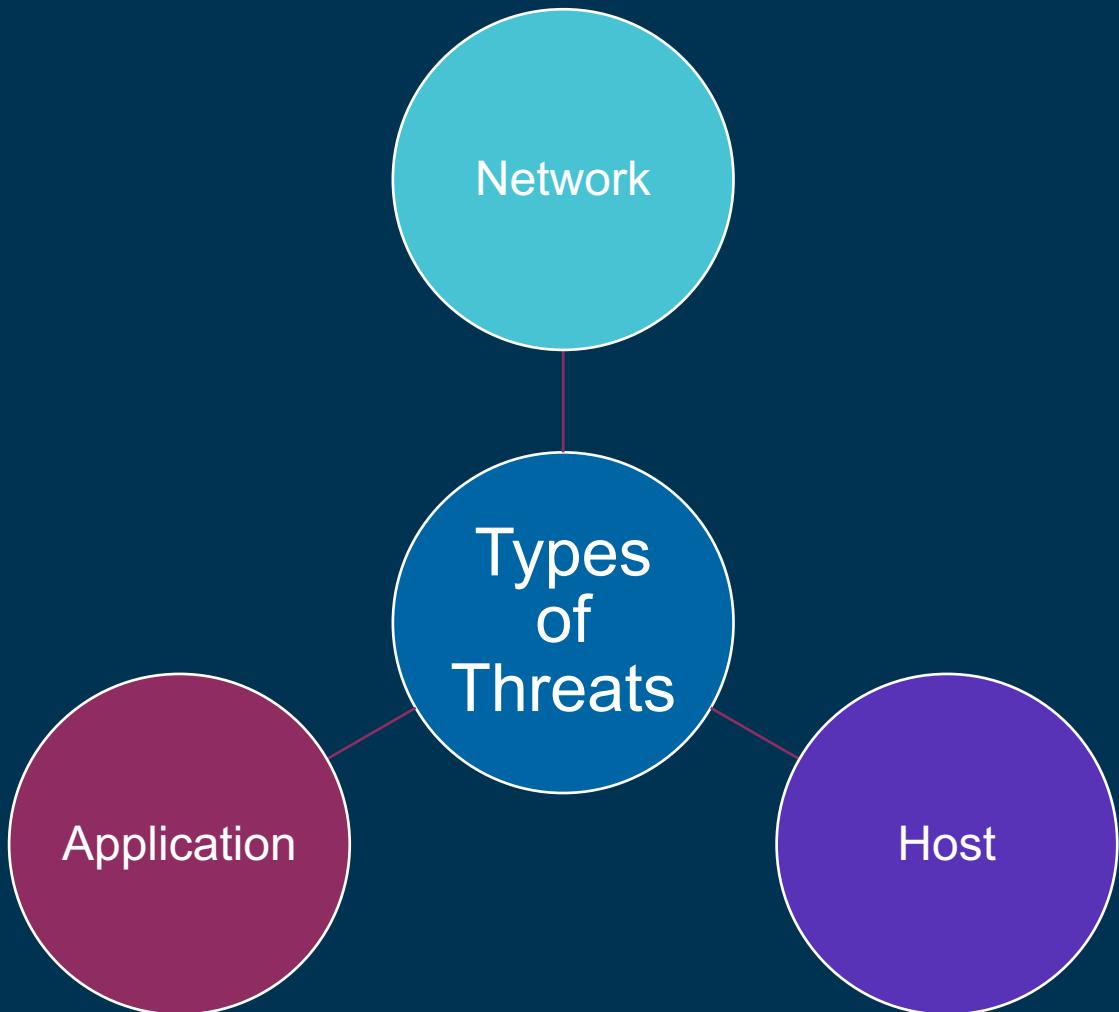
1. Các thách thức về an toàn thông tin (tt)



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

- **Network Threat:**

- Thu thập thông tin
- Sniffing và Eavesdropping
- Spoofing
- Session Hijacking
- Man in the middle
- DNS và ARP Poisoning
- DDoS
- Tấn công Password
- Firewall và tấn công IDS
- ...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

- **Host Threat:**

- Tấn công Malware
- Footprinting
- Tấn công Password
- Truy cập không được cấp quyền
- Tấn công vật lý
- Tấn công Backdoor
- DDoS
- Leo thang đặc quyền
- Thực thi mã tùy ý
- ...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

- **Application Threat:**

- Phishing
- SQL injection
- Buffer Overflow
- Lỗi cấu hình bảo mật
- Tấn công xác thực
- Xác thực dữ liệu/đầu vào không đúng
- Các cuộc tấn công xác thực và ủy quyền
- Định cấu hình sai bảo mật
- Xử lý lỗi và quản lý ngoại lệ không đúng cách
- Thông tin bị tiết lộ
- ...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

1. *Eavesdropping*

- Nghe trộm là một phương pháp cũ nhưng hiệu quả.
- Sử dụng một thiết bị mạng (router, card mạng...) và một chương trình ứng dụng (Tcpdump, Ethereal, Wireshark...) để giám sát lưu lượng mạng, bắt các gói tin đi qua thiết bị này.
- Thực hiện dễ dàng hơn với mạng không dây.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

1. *Eavesdropping*

- Không có cách nào ngăn chặn việc nghe trộm trong một mạng công cộng.
- Để chống lại việc nghe trộm, cách tốt nhất là mã hoá dữ liệu trước khi truyền chúng trên mạng.
 - Plaintext: văn bản gốc
 - Cyphertext: chuỗi mật mã
 - Key: khoá mã hoá hoặc giải mã

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

2. Cryptanalysis

- Là nghệ thuật tìm kiếm thông tin hữu ích từ dữ liệu đã mã hoá mà không cần biết khoá giải mã.
- Ví dụ: phân tích cấu trúc thống kê của các ký tự trong phương pháp mã hoá bằng tần suất.
- Phương pháp này thường sử dụng các công cụ toán học và máy tính có hiệu suất cao.
- Cách chống lại phá mã:
 - Sử dụng những giải thuật mã hoá không thể hiện cấu trúc thống kê trong chuỗi mật mã.
 - Khoá có độ dài lớn để chống Brute-force attacks.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Cơ chế chứng thực được sử dụng rộng rãi nhất là dùng username và password.
- Các phương pháp thông dụng bao gồm:
 - Guessing
 - Social engineering
 - Dictionary
 - Password sniffing

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Guessing: hiệu quả đối với các mật khẩu ngắn hoặc người dùng quên đổi mật khẩu ngầm định.
- 10 mật khẩu phổ biến nhất trên internet (theo PC Magazine):

1. Password	2. 123456
3. qwerty	4. abc123
5. letmein	6. monkey
7. myspace1	8. password1
9. blink182	10. the user's own first name

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Social engineering: là phương pháp sử dụng các kỹ năng xã hội để ăn cắp thông tin mật của người khác.
 - Mạo danh (Impersonate)
 - Lừa đảo (Phising) qua email, websites...
 - Thu thập thông tin từ giấy tờ bị loại bỏ
 - Tạo trang web đăng nhập giả...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Dictionary Attacks:
 - Chỉ những mật khẩu đã được mã hoá mới được lưu trên hệ thống máy tính.
 - Hệ điều hành UNIX và LINUX: mật khẩu đã được mã hoá với dạng mã ASCII của các user được lưu trong /etc/passwd (các versions cũ) và /etc/shadows (các versions mới hơn).
 - Hệ điều hành Windows NT/XP: tên user và mật khẩu của user đã được mã hoá được lưu trong registry của hệ thống với tên file là SAM.
 - Dictionary attacks: duyệt tìm từ một từ điển (thu được từ các file SAM...) các username và password đã được mã hoá.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Password Sniffing:
 - Là một phần mềm dùng để bắt các thông tin đăng nhập từ xa như username và password đối với các ứng dụng mạng phổ biến như Telnet, FTP, SMTP, POP3.
 - Để gây khó khăn cho việc Password Sniffing, có thể dùng những chương trình đặc biệt (như SSH trong HTTPS...) để mã hoá tất cả các thông điệp truyền.
 - Cain & Abel là một công cụ khôi phục mật khẩu trong hệ điều hành Microsoft và cũng là một công cụ password sniffing có thể bắt và phá mã các password đã được mã hoá sử dụng từ điển hoặc brute-force. Có thể download công cụ này tại <http://www.oxid.it/cain.html>.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số phương pháp chứng minh danh tính người dùng đang được sử dụng:
 - Sử dụng mật khẩu bí mật (secret passwords): phổ biến nhất. Sử dụng tên người dùng và mật khẩu của người dùng.
 - Sử dụng sinh trắc học (biometrics): sử dụng các tính năng độc đáo của sinh học như vân tay, võng mạc... nhờ việc kết nối các thiết bị sinh trắc học (khá đắt tiền, chỉ dùng tại những nơi yêu cầu bảo mật ở mức độ cao) vào máy tính như máy đọc dấu vân tay, máy quét võng mạc...
 - Sử dụng chứng thực (authenticating items): dùng một số giao thức xác thực như Kerberos...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số quy tắc bảo vệ mật khẩu:
 - Sử dụng mật khẩu dài kết hợp giữa chữ thường, chữ hoa, số và các ký tự đặc biệt như \$ # & %. Không dùng các từ có trong từ điển, các tên và mật khẩu thông dụng.
-> gây khó khăn cho việc đoán mật khẩu (guessing attacks) và tấn công sử dụng từ điển (dictionary attacks).
 - Không tiết lộ mật khẩu với những người không có thẩm quyền hoặc qua điện thoại, thư điện tử... -> chống lại social engineering.
 - Thay đổi mật khẩu định kỳ và không sử dụng trở lại những mật khẩu cũ để chống lại những cuộc tấn công từ điển hoặc mật khẩu cũ đã được nhận diện.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

3. *Password Pilfering*

- Một số quy tắc bảo vệ mật khẩu:
 - Không sử dụng cùng một mật khẩu cho các tài khoản khác nhau nhằm đảm bảo các tài khoản khác vẫn an toàn khi mật khẩu của một tài khoản bị lộ.
 - Không sử dụng những phần mềm đăng nhập từ xa mà không có cơ chế mã hóa mật khẩu và một số thông tin quan trọng khác.
 - Huỷ hoàn toàn các tài liệu có lưu các thông tin quan trọng.
 - Tránh nhập các thông tin trong các cửa sổ popup.
 - Không click vào các liên kết trong các email khả nghi.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Là phương pháp tấn công cho phép kẻ tấn công mạo nhận nạn nhân mà không cần sử dụng mật khẩu của nạn nhân.
- Các phương pháp phổ biến bao gồm:
 - Man-in-the-middle attacks
 - Message replays attacks
 - Network spoofing attacks
 - Software exploitation attacks

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

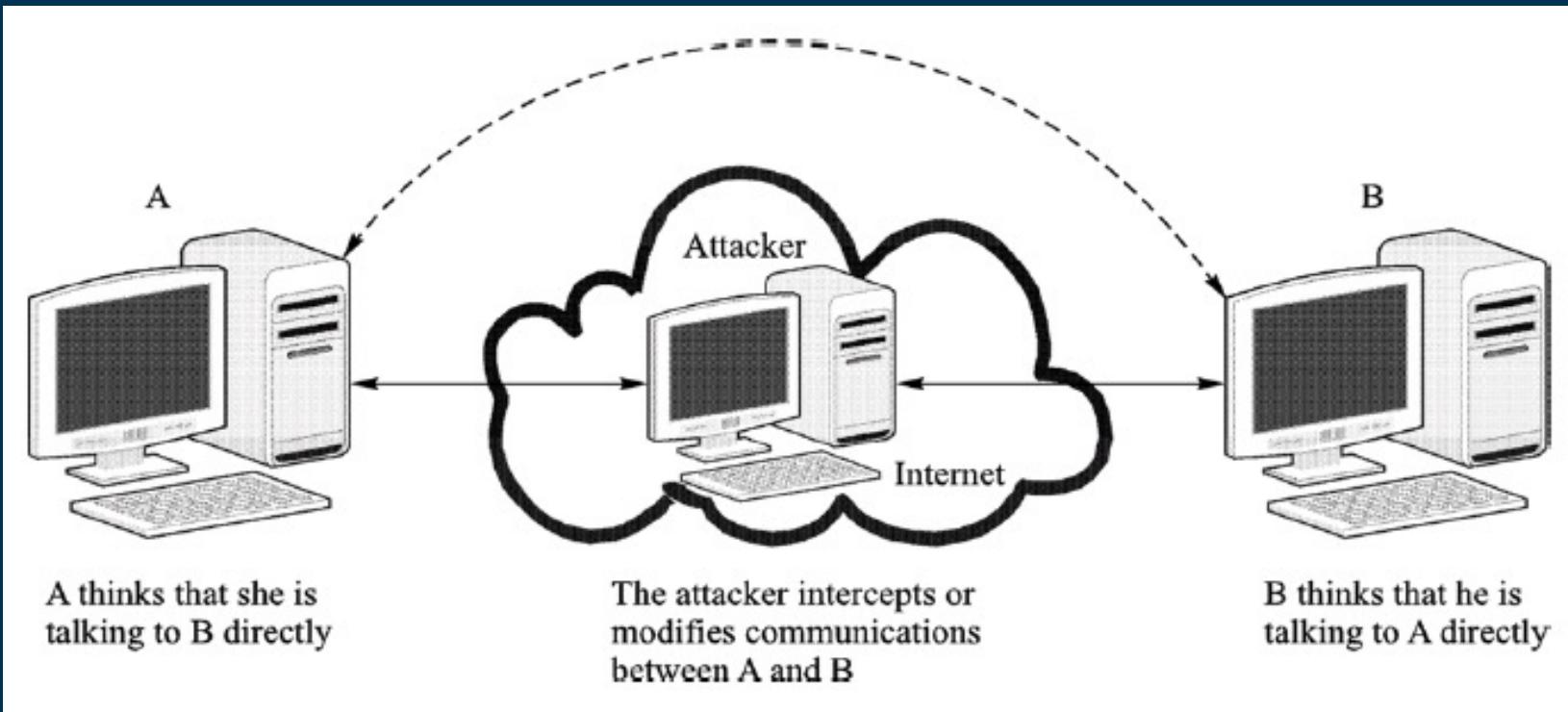
4. *Identity Spoofing*

- Man-in-the-middle attacks
 - Kẻ tấn công cố gắng dàn xếp với thiết bị mạng (hoặc cài đặt một thiết bị của riêng mình) giữa hai hoặc nhiều người sử dụng, sau đó chặn và sửa đổi hay làm giả dữ liệu truyền giữa những người sử dụng rồi truyền chúng như chưa từng bị tác động bởi kẻ tấn công.
 - Các người dùng vẫn tin rằng họ đang trực tiếp nói chuyện với nhau, không nhận ra rằng sự bảo mật và tính toàn vẹn dữ liệu của các gói tin IP mà họ nhận được đã không còn.
 - Mã hoá và chứng thực các gói IP là biện pháp chính để ngăn chặn các cuộc tấn công Man-in-the-middle. Những kẻ tấn công không thể đọc hoặc sửa đổi một gói tin IP đã được mã hoá mà không phải giải mã nó.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. Identity Spoofing

- Man-in-the-middle attacks



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

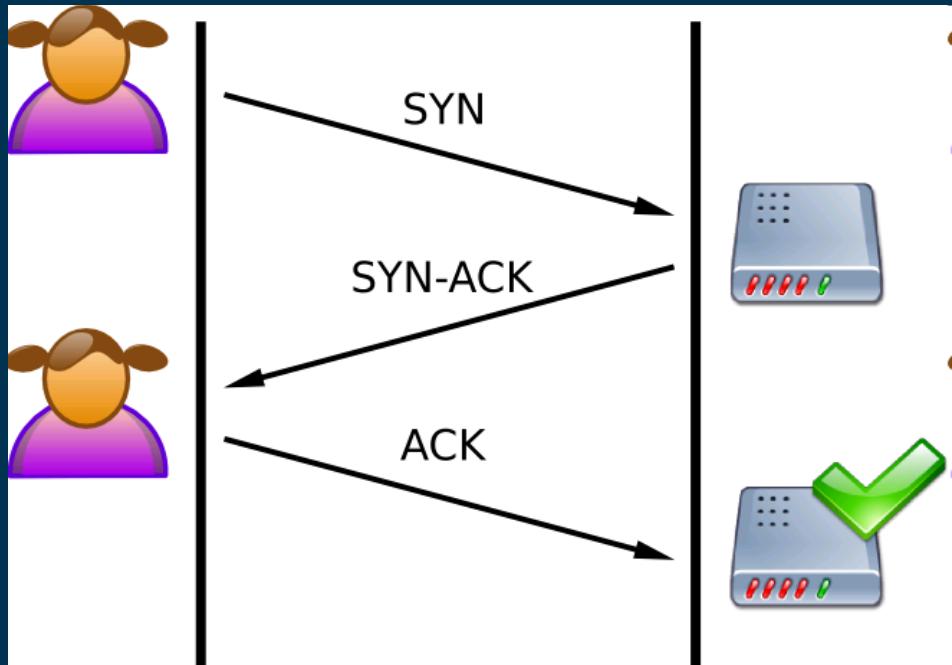
- Message replays:
 - Trong một số giao thức xác thực, sau khi người dùng A chứng thực mình với hệ thống là một người dùng hợp pháp, A sẽ được cấp một chứng thực (giấy phép) thông qua. Với giấy phép này, A sẽ nhận được những dịch vụ cung cấp bởi hệ thống. Giấy phép này đã được mã hóa và không thể sửa đổi.
 - Tuy nhiên, những kẻ tấn công có thể ngăn chặn nó, giữ một bản sao, và sử dụng nó sau này để mạo nhận (đóng vai) người dùng A để có được các dịch vụ từ hệ thống.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

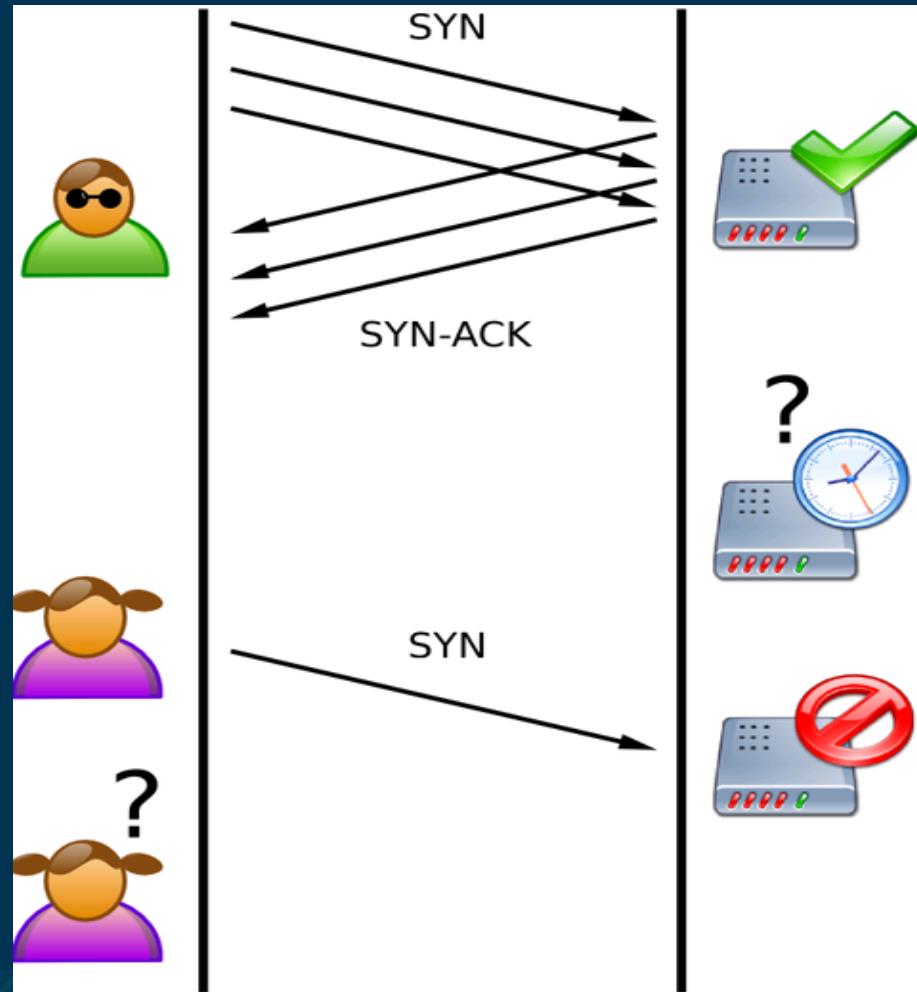
4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
 - SYN flooding: Trong một cuộc tấn công SYN flooding, kẻ tấn công lấp đầy bộ đệm TCP của máy tính mục tiêu với một khối lượng lớn các gói SYN, làm cho máy tính mục tiêu không thể thiết lập các thông tin liên lạc với các máy tính khác. Khi điều này xảy ra, các máy tính mục tiêu được gọi là một máy tính câm.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



A normal connection between a user and a server. The three-way handshake is correctly performed.



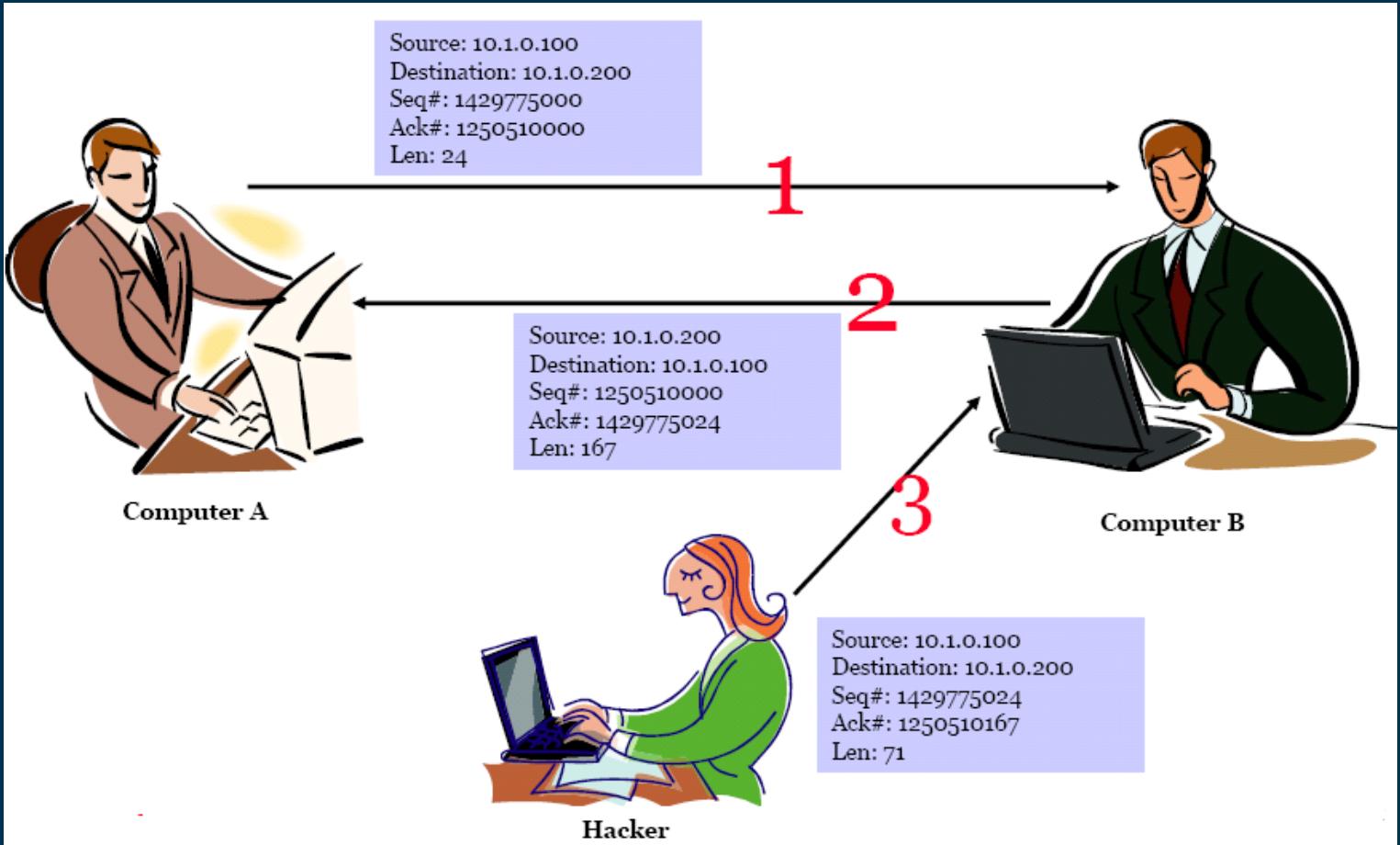
2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Network Spoofing: là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
 - TCP hijacking:
 - Là một kỹ thuật sử dụng các gói tin giả mạo để chiếm đoạt một kết nối giữa máy tính nạn nhân và máy đích. Máy nạn nhân bị treo và hacker có thể truyền thông với máy đích như hacker chính là nạn nhân.
 - Để ngăn chặn TCP hijacking, có thể sử dụng phần mềm như TCP Wrappers để kiểm tra địa chỉ IP tại tầng TCP (tầng Transport).

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

TCP hijacking



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

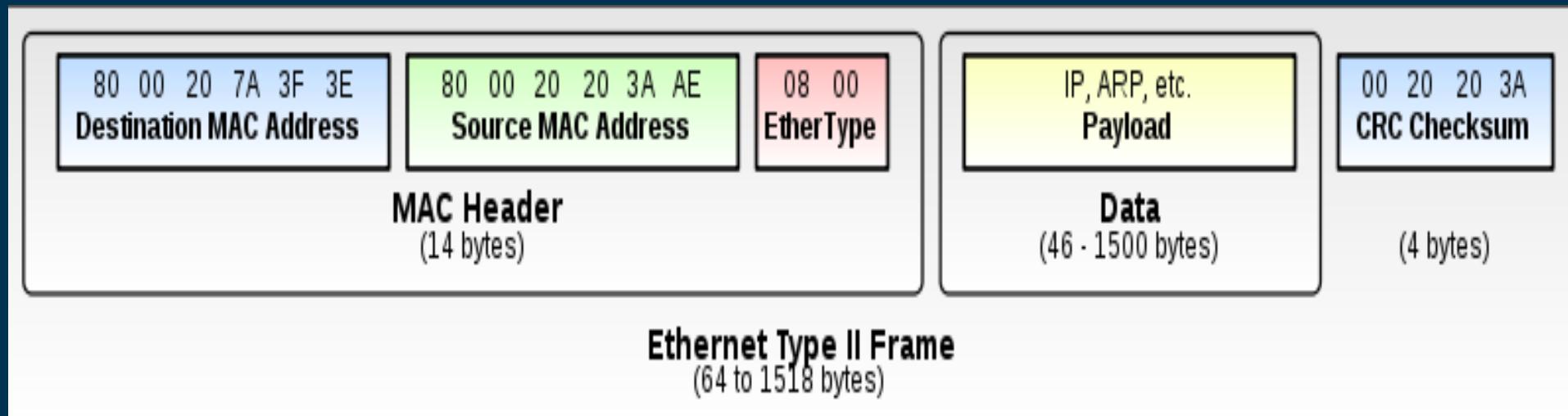
4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
 - ARP spoofing (ARP poisoning): ARP là một giao thức phân giải địa chỉ tại tầng liên kết có thể chuyển đổi địa chỉ IP đích trong header IP đến địa chỉ MAC của máy tính tại mạng đích. Trong một cuộc tấn công giả mạo ARP, kẻ tấn công thay đổi địa chỉ MAC đích hợp pháp của một địa chỉ IP đến một địa chỉ MAC khác được lựa chọn bởi những kẻ tấn công. Để ngăn chặn các cuộc tấn công ARP spoofing, cần phải tăng cường kiểm tra các tên miền, và chắc chắn rằng địa chỉ IP nguồn và địa chỉ IP đích trong một gói tin IP không được thay đổi trong khi truyền.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. *Identity Spoofing*

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
 - ARP spoofing (ARP poisoning):

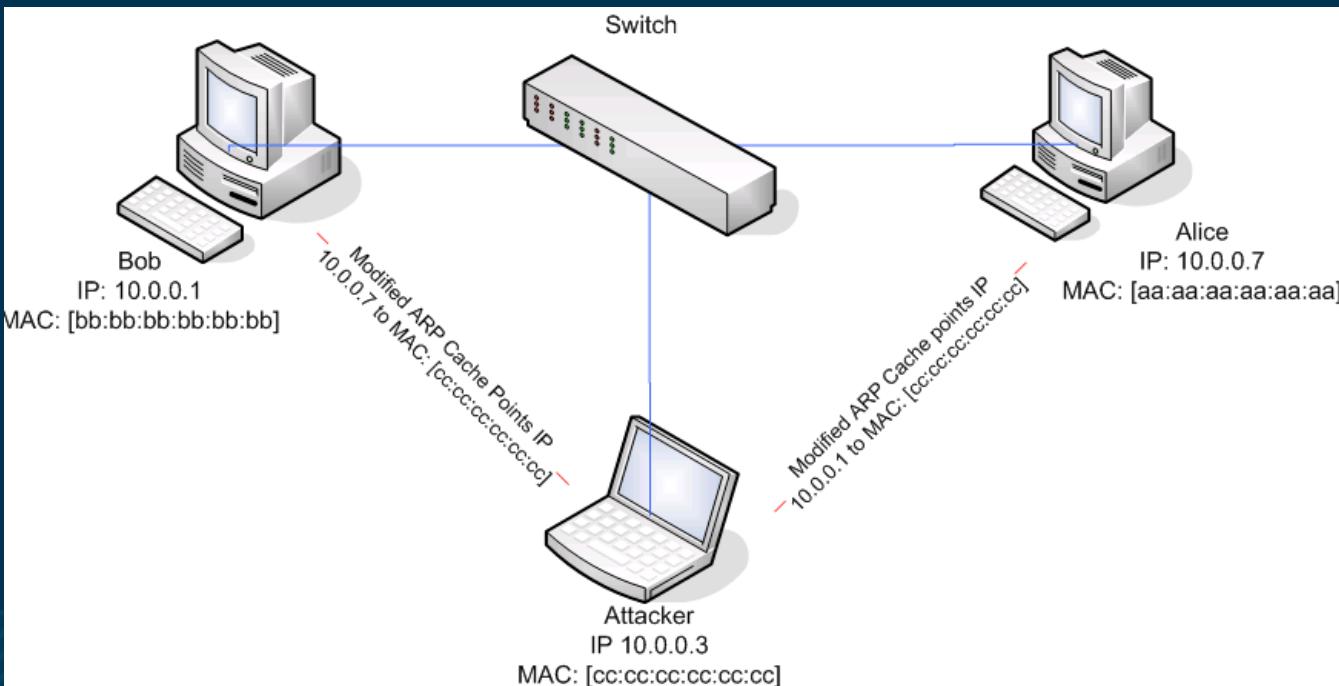


Một frame Ethernet tiêu biểu. Một frame giả mạo có địa chỉ MAC nguồn sai có thể đánh lừa các thiết bị trên mạng.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

4. Identity Spoofing

- Network Spoofing: IP Spoofing là một trong những kỹ thuật lừa gạt chính trên mạng. Bao gồm:
 - ARP spoofing (ARP poisoning):



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

5. *Buffer-Overflow Exploitations*

- Là một lỗ hổng phần mềm phổ biến. Lỗi này xảy ra khi quá trình ghi dữ liệu vào bộ đệm nhiều hơn kích thước khả dụng của nó.
- Các hàm strcat(), strcpy(), sprintf(), vsprintf(), bcopy(), get(), scanf()... trong ngôn ngữ C có thể bị khai thác vì không kiểm tra xem liệu bộ đệm có đủ lớn để dữ liệu được sao chép vào mà không gây ra tràn bộ đệm hay không.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

6. *Repudiation*

- Trong một số trường hợp chủ sở hữu của dữ liệu có thể không thừa nhận quyền sở hữu của dữ liệu để tránh hậu quả pháp lý. Người này có thể cho rằng chưa bao giờ gửi hoặc nhận các dữ liệu đó.
- Ngay cả khi dữ liệu đã được chứng thực, chủ sở hữu của dữ liệu xác thực có thể thuyết phục quan tòa rằng vì những sơ hở, bất cứ ai cũng có thể dễ dàng chế tạo tin nhắn và làm cho nó trông giống như thật.
- Sử dụng các thuật toán mã hóa và xác thực có thể giúp ngăn ngừa các cuộc tấn công bác bỏ.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

7. *Intrusion*

- Là kẻ xâm nhập bất hợp pháp vào một mạng với mục đích truy cập vào hệ thống máy tính của người khác, đánh cắp thông tin và tài nguyên máy tính hoặc băng thông của nạn nhân.
- Cấu hình sơ hở, giao thức sai sót, tác dụng phụ của phần mềm đều có thể bị khai thác bởi kẻ xâm nhập.
- Mở các cổng UDP hoặc TCP không cần thiết là một sơ hở phổ biến. Đóng các cổng này lại có thể giảm thiểu việc xâm nhập.
- IP scan và Port scan là những công cụ hack phổ biến thuộc dạng này và cũng là những công cụ giúp người dùng kiểm tra được các lỗ hổng trong hệ thống.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

- Mục tiêu của cuộc tấn công từ chối dịch vụ là ngăn chặn người dùng hợp pháp sử dụng những dịch vụ mà họ thường nhận được từ các máy chủ.
- Các cuộc tấn công như vậy thường buộc máy tính mục tiêu phải xử lý một số lượng lớn những thứ vô dụng, hy vọng máy tính này sẽ tiêu thụ tất cả các nguồn tài nguyên quan trọng.
- Một cuộc tấn công từ chối dịch vụ có thể được phát sinh từ một máy tính duy nhất (DoS), hoặc từ một nhóm các máy tính phân bố trên mạng Internet (DDoS).

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

- DoS có các hình thức cơ bản sau:
 - Smurf
 - Buffer Overflow Attack
 - Ping of death
 - Teardrop
 - SYN Attack
- Công cụ để thực hiện tấn công DoS có thể là Jolt2, Bubonic.c, Land and LaTierra, Targa, Blast20, Nemesy, Panther2, Crazy Pinger, Some Trouble, UDP Flood, FSMax...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

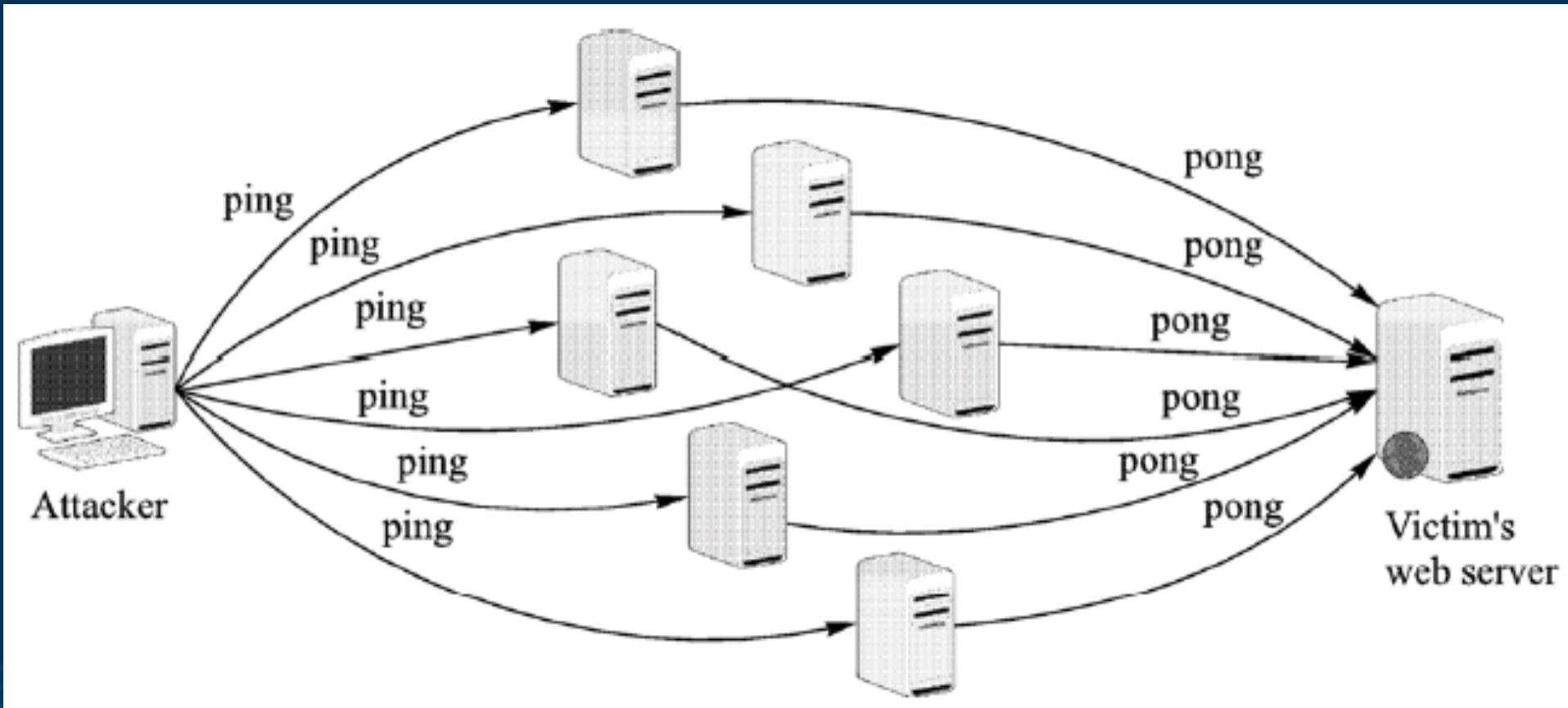
8. *Denial of Service Attacks*

- DoS: Smurf là một loại tấn công DoS điển hình. Máy của attacker sẽ gửi rất nhiều lệnh ping đến một số lượng lớn máy tính trong một thời gian ngắn trong đó địa chỉ IP nguồn của gói ICMP echo sẽ được thay thế bởi địa chỉ IP của nạn nhân. Các máy tính này sẽ trả lại các gói ICMP reply đến máy nạn nhân. Buộc phải xử lý một số lượng quá lớn các gói ICMP reply trong một thời gian ngắn khiến tài nguyên của máy bị cạn kiệt và máy sẽ bị sụp đổ.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. Denial of Service Attacks

- DoS:

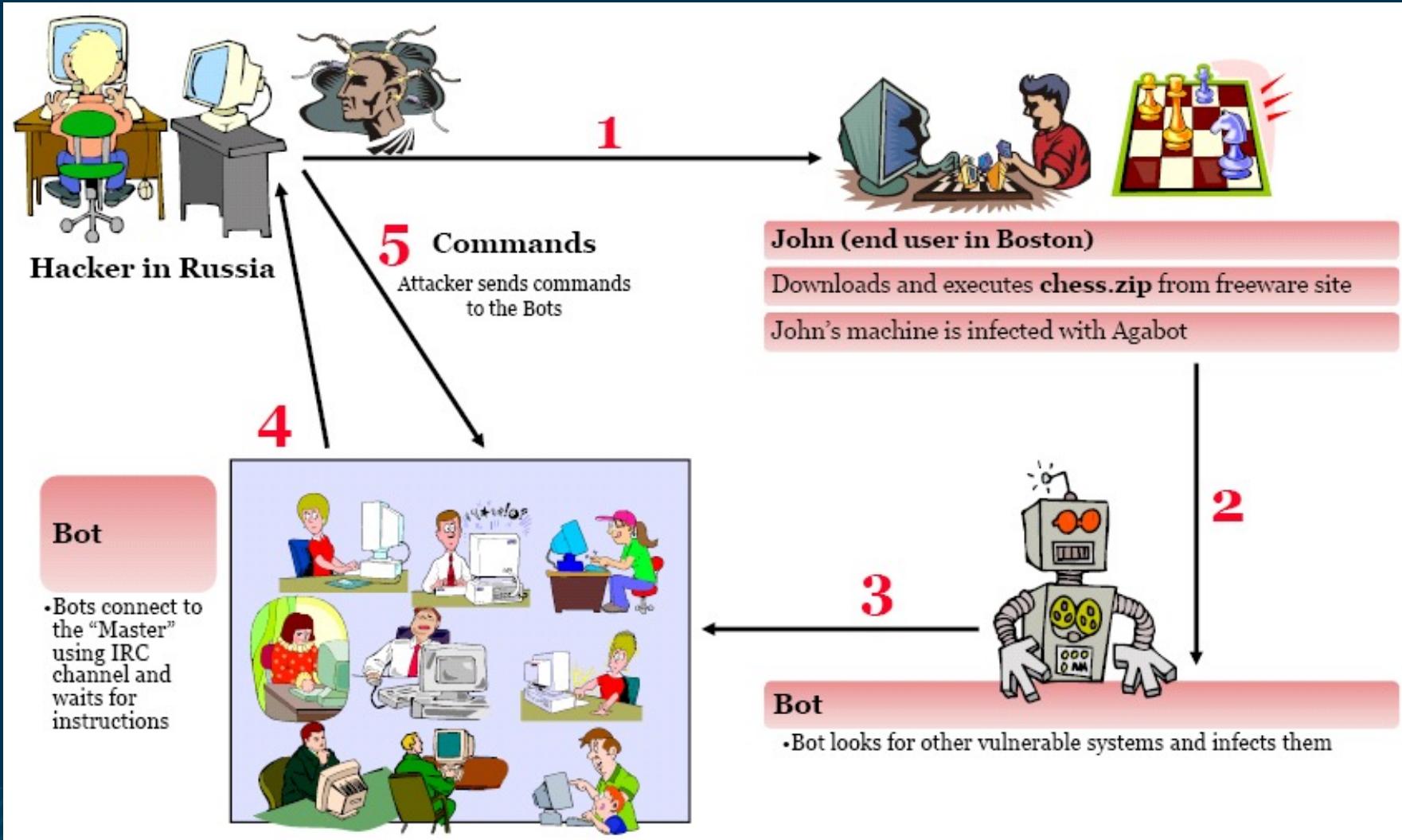


2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

8. *Denial of Service Attacks*

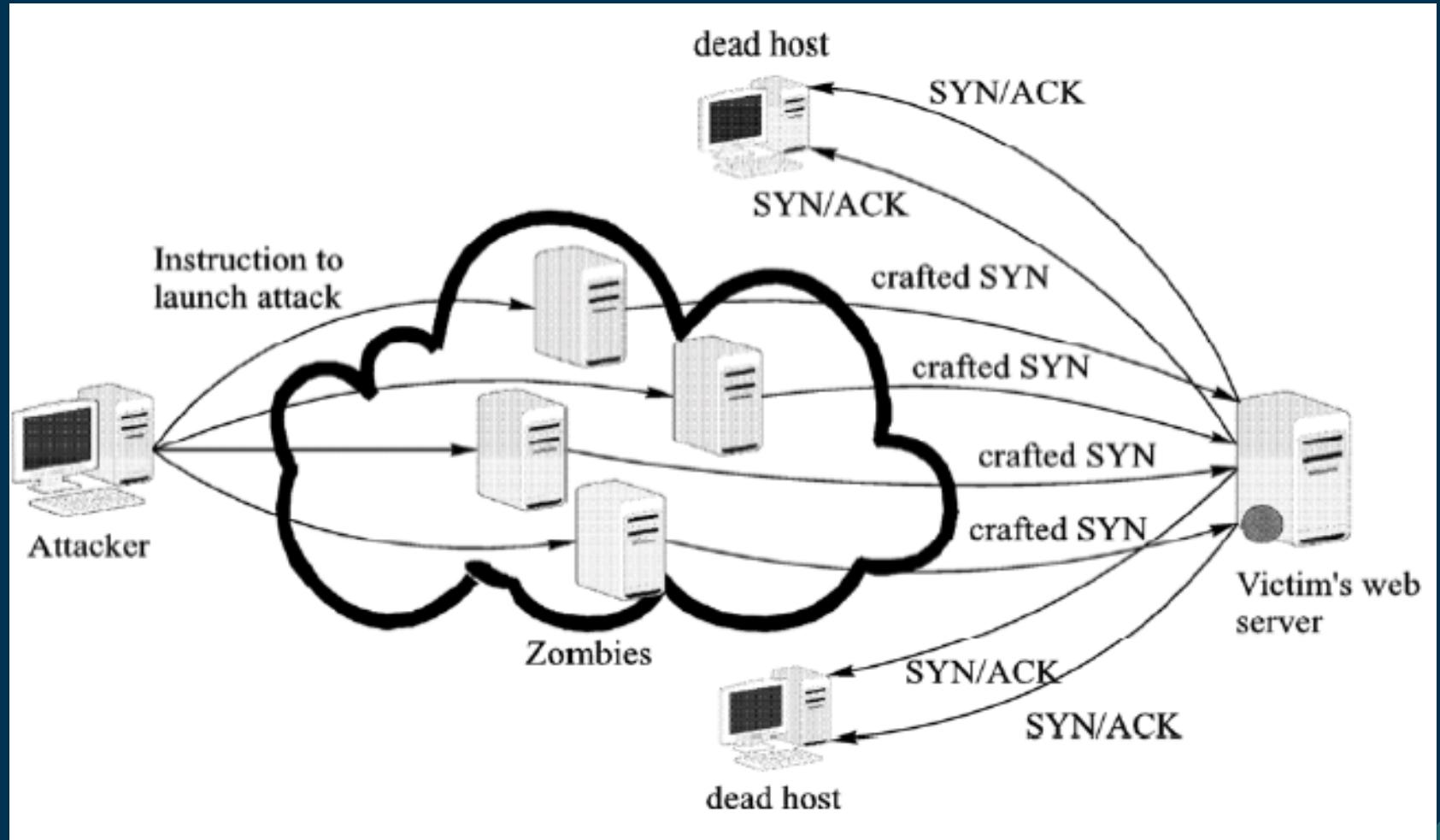
- DDoS (Distributed DoS) có cơ chế hoạt động:
 - Attackers thường sử dụng Trojan để kiểm soát cùng lúc nhiều máy tính nối mạng.
 - Attacker cài đặt một phần mềm đặc biệt (phần mềm zombie) lên các máy tính này (máy tính zombie) để tạo ra một đội quân zombie (botnet) nhằm tấn công DoS sau này trên máy nạn nhân.
 - Phát hành một lệnh tấn công vào các máy tính zombie để khởi động một cuộc tấn công DoS trên cùng một mục tiêu (máy nạn nhân) cùng một lúc.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

Một cuộc tấn công DDoS sử dụng SYN flooding



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

- 1 Trojan-Spy.Win32.Zbot
- 2 Trojan.Win32.Nymaim
- 3 Trojan.Win32.Neurevt
- 4 SpyEye
- 5 Trojan-Banker.Win32.Gozi
- 6 Emotet
- 7 Caphaw
- 8 Trickster
- 9 Cridex/Dridex
- 10 Backdoor.Win32.Shiz

financial malware

9. *Malicious Software*

Các phần mềm độc hại bao gồm:

- Virus,
- Worms,
- Trojan horses,
- Logic bombs,
- Backdoors
- Spyware,
- Ransomware
- Rootkit
- ...

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. Malicious Software

- **Virus**

- Là một phần mềm có thể sao chép chính nó. Nó không đứng một mình mà phải gắn vào một tập tin hoặc một chương trình khác.
- Khi một chương trình bị nhiễm virus máy tính được thực hiện hoặc một tập tin bị nhiễm được mở ra, loại virus chứa trong nó sẽ được thực thi.
- Khi thực hiện, virus có thể làm hại máy tính và sao chép chính nó để lây nhiễm sang máy khác trong hệ thống.

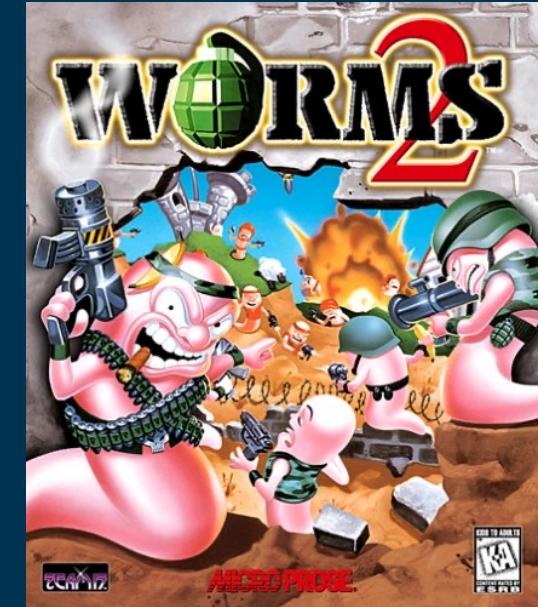


2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Worms***

- Cũng là một chương trình có thể tự sao chép chính nó. Nhưng không giống như virus, Worm là một chương trình đứng một mình (stand alone program). Nói cách khác là nó không cần vật chủ để ký sinh.
- Một Worm có thể tự thực thi tại bất kỳ thời điểm nào nó muốn.
- Khi thực thi, Worm có thể gây nguy hiểm cho hệ thống nơi nó thường trú hoặc tái sinh chính nó trên các hệ thống qua mạng.



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Trojan horses:***

- Thường ngụy trang mình kèm theo những chương trình ứng dụng thông thường và vô hại như trò chơi hoặc những công cụ miễn phí để người dùng tải về máy.
- Trojan không tự sinh sản như virus hay worm và chỉ thực hiện khi người dùng chạy chương trình có đính kèm Trojan.
- Chức năng chính của Trojan là điều khiển máy tính từ xa, ăn cắp thông tin của nạn nhân hoặc làm nhiệm vụ backdoor.

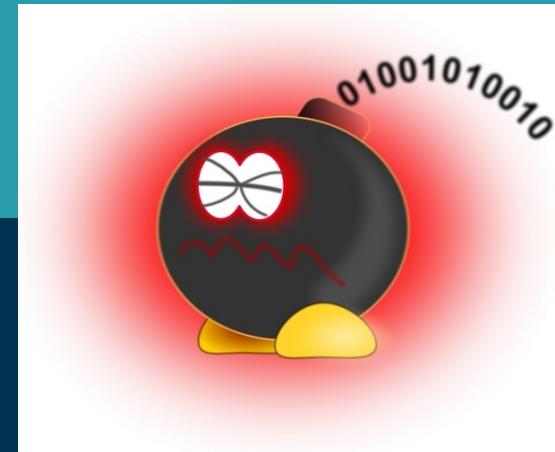


2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Logic bombs***

- Bom logic là chương trình con hoặc lệnh được nhúng trong một chương trình. Sự thi hành của nó được kích hoạt bởi câu lệnh điều kiện.
- Ví dụ, một nhân viên công ty làm việc trên một dự án phát triển có thể cài đặt một quả bom logic bên trong một chương trình. Quả bom được kích hoạt chỉ nếu nhân viên này đã không chạy chương trình trong một thời gian nhất định. Khi điều kiện được đáp ứng, có nghĩa là nhân viên này đã bị sa thải một thời gian trước đó. Quả bom logic trong trường hợp này được sử dụng để trả thù chống lại chủ nhân.



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. Malicious Software

- **Backdoors**

- Backdoors là những đoạn chương trình bí mật thường được đính kèm vào những chương trình khác nhằm giúp kẻ tấn công sau khi đã xâm nhập được vào hệ thống mở sẵn những lối vào (cổng hậu)..
- Khi được chạy trên máy nạn nhân, Backdoors sẽ thường trực trong bộ nhớ, mở một port (mặc định hoặc do kẻ tấn công quy định) giúp kẻ tấn công dễ dàng đột nhập vào máy nạn nhân thông qua port này.



2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

- ***Spywares***
 - Spyware là một loại phần mềm tự cài đặt chính nó trên máy tính của người dùng. Spyware thường được sử dụng để theo dõi xem người dùng làm gì và quấy rối họ với những thông điệp thương mại xuất hiện trong những cửa sổ popup.
 - Thường gồm các loại Browser hijacking và Zombieware.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software* • *Spywares*

- Browser Hijacking: là một kỹ thuật có thể thay đổi các thiết lập của trình duyệt của người dùng. Nó có thể thay thế Website mặc định của người dùng với một trang web khác được lựa chọn bởi kẻ tấn công. Hoặc nó có thể ngăn chặn người dùng truy cập vào các Websites họ muốn đến thăm.
- Zombieware: là phần mềm có trên máy tính của người dùng và biến nó thành một zombie để khởi động các cuộc tấn công DDoS hoặc thực hiện các hoạt động có hại như gửi thư rác hoặc phát tán virus.

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

9. *Malicious Software*

• **Ransomware**

- Được thiết kế để ngăn chặn truy cập vào máy tính hoặc dữ liệu cho tới khi người dùng trả tiền chuộc.
- Ransomware thường lây lan qua email lừa đảo hoặc vô tình truy cập trang web bị nhiễm.

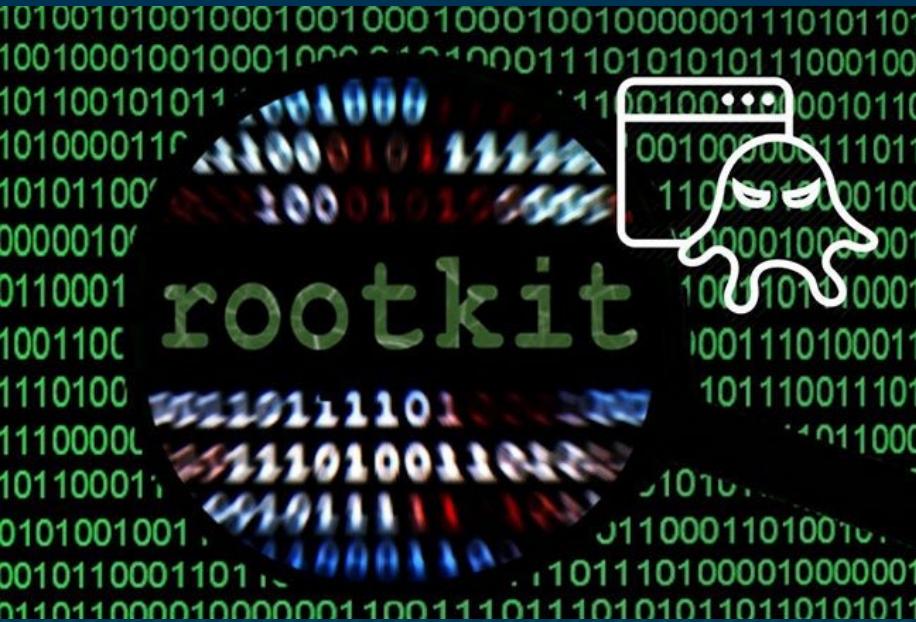
TOP 10 most widespread encryptor families

Name	Verdict	%*
1 WannaCry	Trojan-Ransom.Win32.Wanna	23.56
2 (generic verdict)	Trojan-Ransom.Win32.Phny	16.81
3 GandCrab	Trojan-Ransom.Win32.GandCrypt	12.17
4 (generic verdict)	Trojan-Ransom.Win32.Gen	6.26
5 (generic verdict)	Trojan-Ransom.Win32.Crypmod	5.08
6 (generic verdict)	Trojan-Ransom.Win32.Encoder	4.65
7 Shade	Trojan-Ransom.Win32.Shade	2.66
8 PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2.43
9 (generic verdict)	Trojan-Ransom.Win32.Crypren	2.28
10 Stop	Trojan-Ransom.Win32.Stop	1.94

2. Các kỹ thuật tấn công phổ biến và cơ chế phòng thủ

10. Rootkit

- Giúp che giấu sự tồn tại của phần mềm khác trên hệ thống máy tính
- Không thể phát hiện được bằng các công cụ: “Registry Editor”, “Find Files”, “Task Manager”
- Các loại:
 - Kernel mode rootkit
 - User mode rootkit
 - Bootkit
 - Firmware rootkit



3. Lý lịch của những kẻ tấn công

- Các attacker có thể là:
 - Black-hat hackers
 - Script kiddies
 - Cyber spies
 - Vicious employees
 - Cyber terrorists



3. Lý lịch của những kẻ tấn công

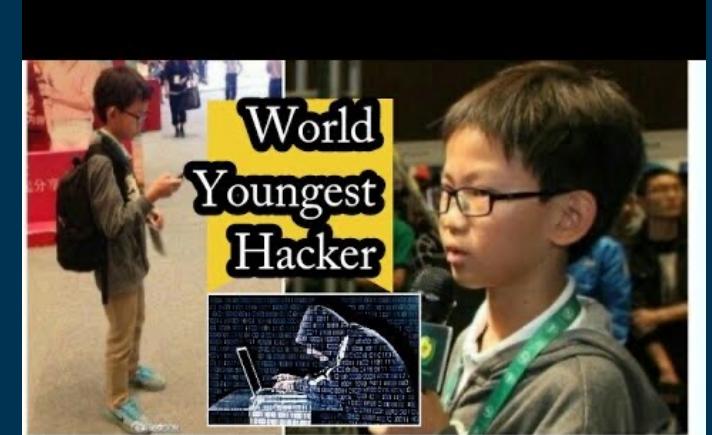
- Black-hat hackers
 - Hackers là những người có tri thức đặc biệt về hệ thống máy tính. Họ quan tâm đến những chi tiết tinh tế của phần mềm, giải thuật, mạng máy tính và cấu hình hệ thống. Họ là một nhóm người ưu tú, năng động, được đào tạo tốt.
 - Tùy theo mục đích, hackers được chia thành hackers mũ đen (cybercrime), hackers mũ trắng (ethical) và hackers mũ xám (.?.).



3. Lý lịch của những kẻ tấn công

- Script kiddies

- Là những người sử dụng các script hoặc các chương trình được phát triển bởi các hacker mũ đen (những công cụ hack) để tấn công các máy tính và gây thiệt hại cho người khác.
- Script kiddies chỉ biết sử dụng công cụ hack để tấn công các mục tiêu chứ không hiểu cách thức hoạt động và cũng không có khả năng viết ra những công cụ tương tự.
- Đa số Script kiddies chỉ là những thanh thiếu niên, không đủ nhận thức và chín chắn để hiểu hết những hậu quả do mình gây ra.



3. Lý lịch của những kẻ tấn công

- Cyber spies

- Có thể hoạt động trên lãnh vực quân sự, kinh tế...
- Đánh chặn truyền thông trên mạng và phá mã các thông điệp đã được mã hoá.
- Nhiều tổ chức tình báo lớn trên thế giới đã thuê các nhà toán học, các nhà khoa học máy tính, các giáo sư đại học làm việc cho họ để phát triển các công cụ nhằm chống lại loại tội phạm này.



3. Lý lịch của những kẻ tấn công

- Vicious employees

- Là những người cố tình vi phạm an ninh để làm hại những người sử dụng họ.
- Tấn công máy tính công ty để kiểm sự quan tâm từ những người lãnh đạo.
- Hoạt động như gián điệp mạng để thu thập và bán bí mật của công ty.



3. Lý lịch của những kẻ tấn công

- Cyber terrorists:
 - Là những kẻ khủng bố cực đoan sử dụng máy tính và công nghệ mạng làm công cụ.
 - Phá hoại tài sản công cộng và cuộc sống của những người vô tội nên cực kỳ nguy hiểm.
 - Vẫn chưa có những báo cáo đầy đủ về loại tội phạm này.

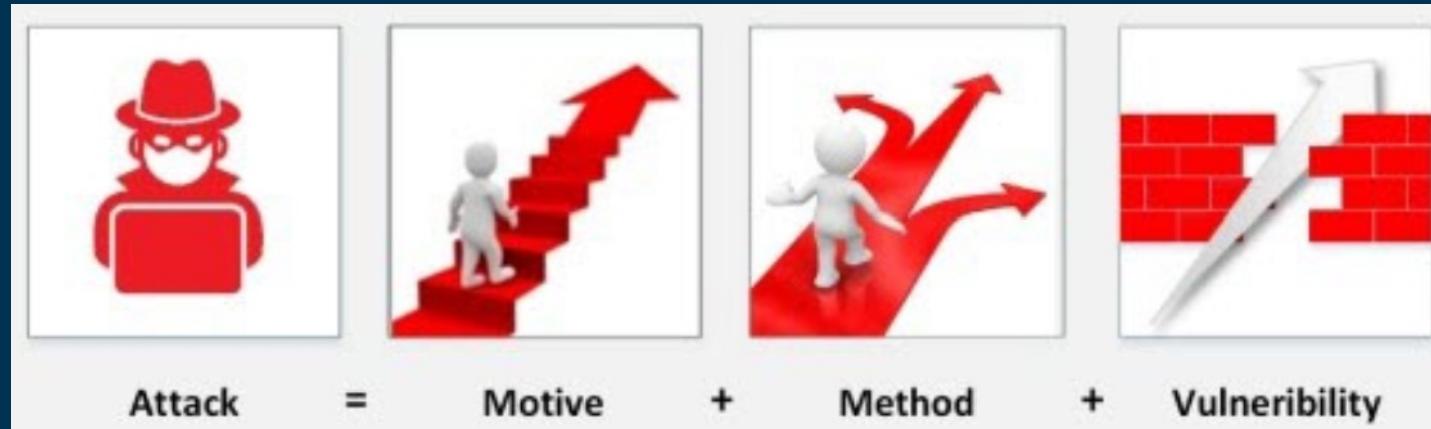


3. Lý lịch của những kẻ tấn công **Động lực, mục tiêu và đối tượng**

- Động lực của các cuộc tấn công?
 - Phá vỡ sự liên tục của việc kinh doanh
 - Đánh cắp thông tin
 - Thao túng dữ liệu
 - Tạo ra sự hỗn loạn về hạ tầng
 - Truyền bá về chính trị, tôn giáo
 - Chiếm các trạng thái trong lĩnh vực quân sự
 - Hạ uy tín của mục tiêu
 - Trả thù
 - ...

3. Lý lịch của những kẻ tấn công Động lực, mục tiêu và đối tượng

- Một cuộc tấn công được cấu thành từ những yếu tố nào?



3. Lý lịch của những kẻ tấn công

Những kỹ năng của một Ethical Hacker

1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has “**high technical**” knowledge to launch the sophisticated attacks

2 Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- Ability to learn** and adapt new technologies quickly
- Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**





4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công

Phase 1 - Reconnaissance



Reconnaissance refers to the preparatory phase where an **attacker** seeks to **gather information** about a target prior to launching an attack



Could be the future point of return, noted for ease of entry for an attack when more about the **target** is known on a broad scale



Reconnaissance target range may include the **target organization's clients, employees, operations, network, and systems**

1

2

3

4. Các giai đoạn của cuộc tấn công

Phase 1 - Reconnaissance

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department



4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công

- 1** Footprinting through Search Engines
- 2** Footprinting Using Advanced Google Hacking Techniques
- 3** Footprinting through Social Networking Sites
- 4** Website Footprinting
- 5** Email Footprinting
- 6** Competitive Intelligence
- 7** WHOIS Footprinting
- 8** DNS Footprinting
- 9** Network Footprinting
- 10** Footprinting through Social Engineering

4. Các giai đoạn của cuộc tấn công

- **allinurl:** This operator restricts results to only those pages containing all the query terms specified in the URL.
For example, the [allinurl: google career] query returns only pages containing the words "google" and "career" in the URL.
- **inurl:** This operator restricts the results to only those pages containing the word specified in the URL.
For example, the [inurl: copy site:www.google.com] query returns only pages in Google site in which the URL has the word "copy."
- **allintitle:** This operator restricts results to only those pages containing all the query terms specified in the title.
For example, the [allintitle: detect malware] query returns only pages containing the words "detect" and "malware" in the title.
- **intitle:** This operator restricts results to only those pages containing the specified term in the title.
For example, the [malware detection intitle:help] query returns only pages that have the term "help" in the title, and "malware" and "detection" terms anywhere within the page.
- **inanchor:** This operator restricts results to only those pages containing the query terms specified in the anchor text on links to the page.
For example, the [Anti-virus inanchor:Norton] query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus."
- **allinanchor:** This operator restricts results to only those pages containing all query terms specified in the anchor text on links to the page.
For example, the [allinanchor: best cloud service provider] query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider."
- **cache:** This operator displays Google's cached version of a web page, instead of the current version of the web page.
For example, [cache:www.eff.org] will show Google's cached version of the Electronic Frontier Foundation home page.

- **Ví dụ Google Search:**

- Tìm chính xác từ: thêm dấu “ ”
- Tìm kiếm ký tự đại diện hoặc từ chưa biết: dùng dấu *
- Tìm kiếm kết hợp: đặt OR hoặc | giữa các truy vấn
- Tìm kiếm 1 site cụ thể: “site:” trước 1 địa chỉ website
- Tìm kiếm loại file: filetype:“loại file”.
- Tìm kiếm truyền thông xã hội: @ trước 1 từ
- Tìm kiếm hashtag: # trước 1 từ
- Tìm kiếm giá: \$ trước 1 số
- Toán tử: +, -
- Tìm trong 1 phạm vi: đặt .. Giữa 2 số
- ...

4. Các giai đoạn của cuộc tấn công

Phase 2 - Scanning

Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance



Port Scanner

Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.

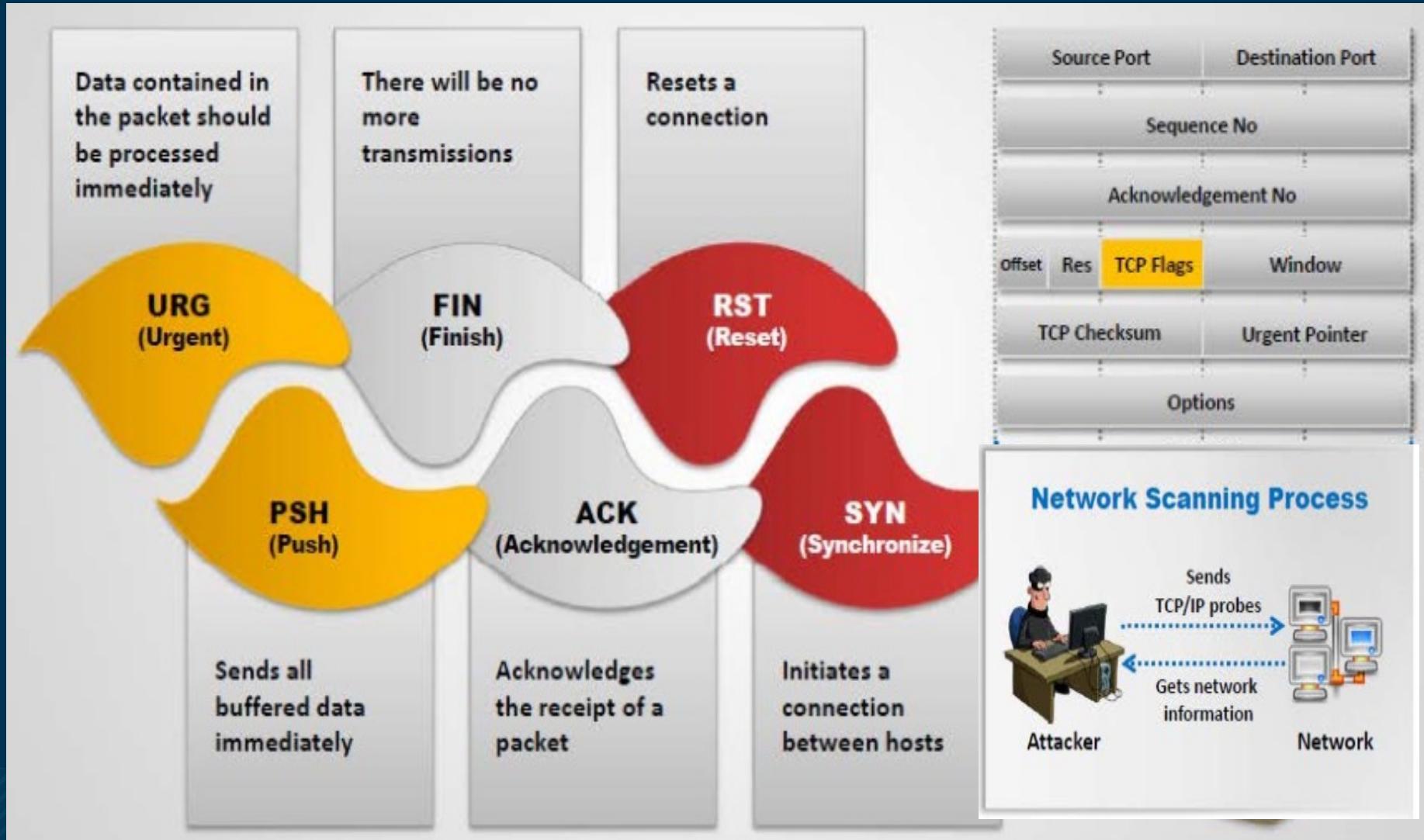


Extract Information

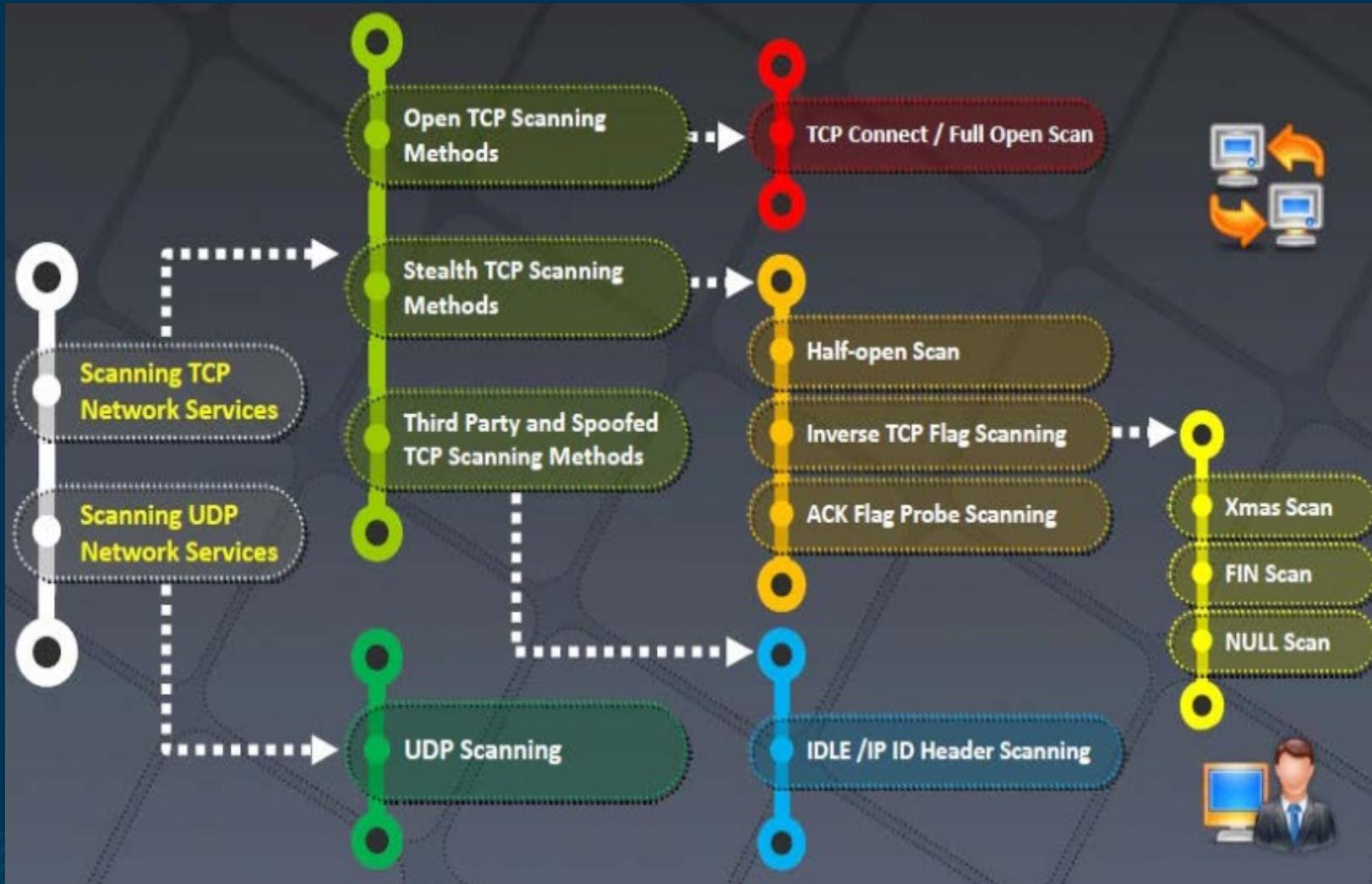
Attackers extract information such as computer names, IP address, and user accounts to launch attack



4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công

NMAP Scan Options

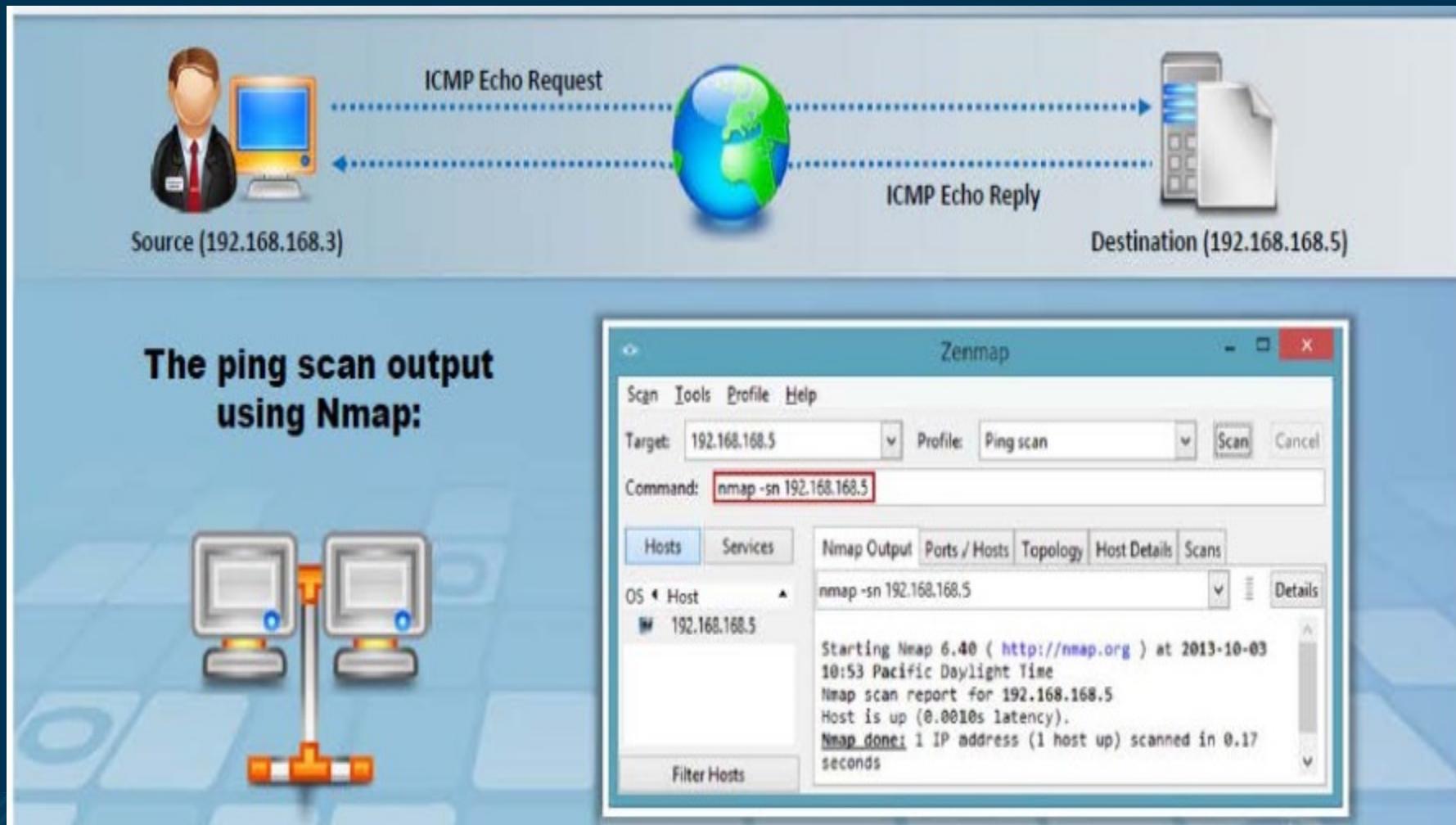


The slide displays a list of Nmap scan options categorized into two columns. A central icon of a circular shield with a green triangle at the top right serves as a visual separator between the two columns.

Scan Options	Description
-sT (TcpConnect)	
-sS (SYN scan)	
-sF (Fin Scan)	
-sX (Xmas Scan)	
-sN (Null Scan)	
-sP (Ping Scan)	
-sU (UDP scans)	
-sO (Protocol Scan)	
-sI (Idle Scan)	
-sA (Ack Scan)	
-sW (Window Scan)	
-sR (RPC scan)	
-sL (List/Dns Scan)	
-P0 (don't ping)	
-PT (TCP ping)	
-PS (SYN ping)	
-PI (ICMP ping)	
-PB (= PT + PI)	
-PP (ICMP timestamp)	
-PM (ICMP netmask)	

EC-Council Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited

4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công

The ping sweep output using Nmap

Zenmap

Scan Tools Profile Help

Target: -sn -PE -PA21,23,30,3389 192.168.168.1-3

Command: nmap -sn -PE -PA21,23,30,3389 192.168.168.1-3

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.168.1

192.168.168.2

192.168.168.3

nmap scan report for 192.168.168.2
Host is up (0.021s latency).
Not shown: 982 filtered ports
PORT STATE SERVICE
25/tcp open satp
80/tcp open http
81/tcp open hstcfd-nu
82/tcp open xfer
119/tcp open mntp
139/tcp open netbios-ssn
465/tcp open smtps
563/icmp open anws
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
3128/tcp open squid-https
5357/tcp open usdapl
8008/tcp open http
8080/tcp open http-proxy
8081/tcp open blackice-iccap
8888/tcp open sun-answerbook
49156/tcp open unknown
nmap scan report for 192.168.168.3
Host is up (0.014s latency).

Source 192.168.168.3

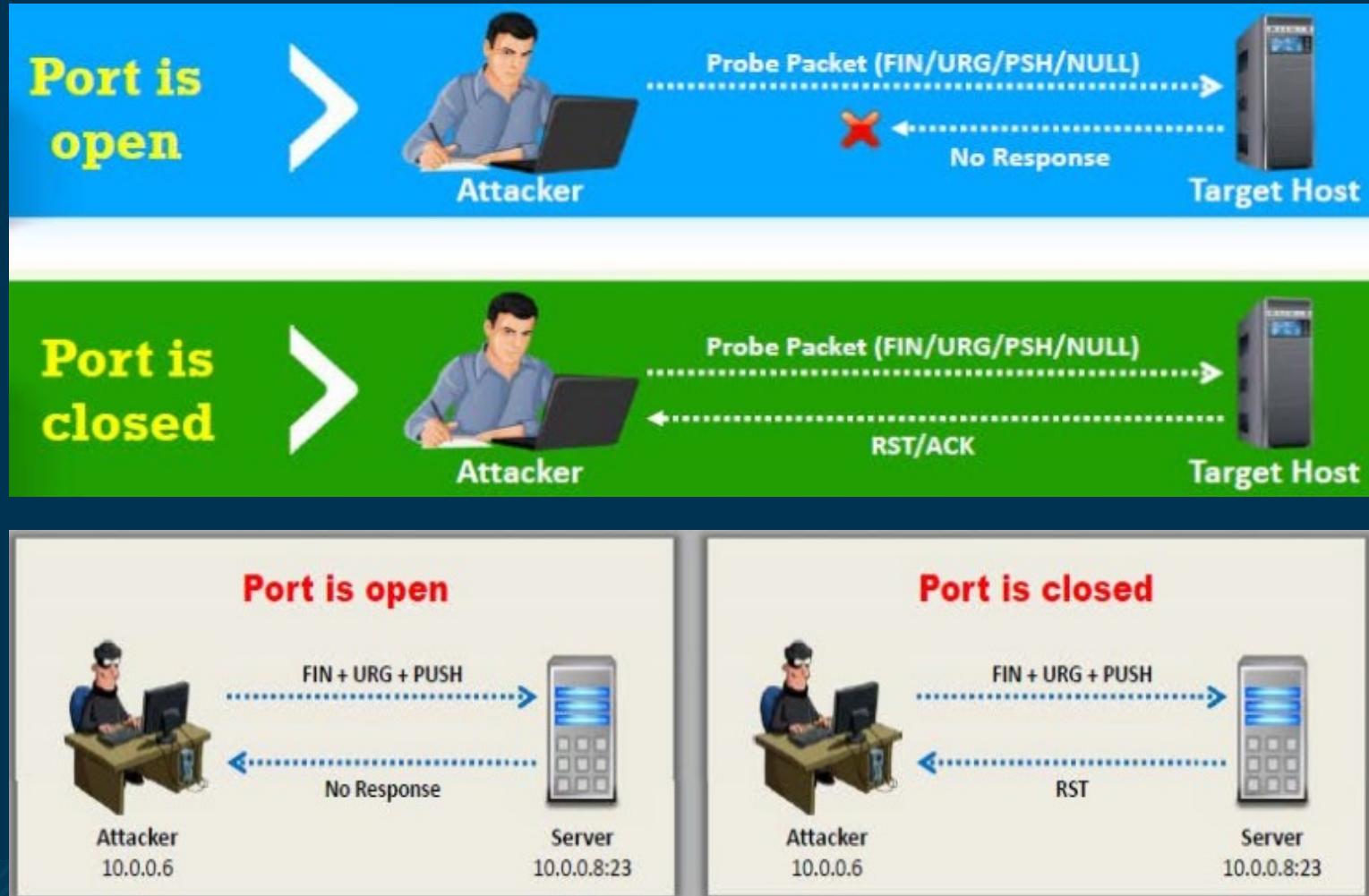
ICMP Echo Request 192.168.168.5

ICMP Echo Reply 192.168.168.6

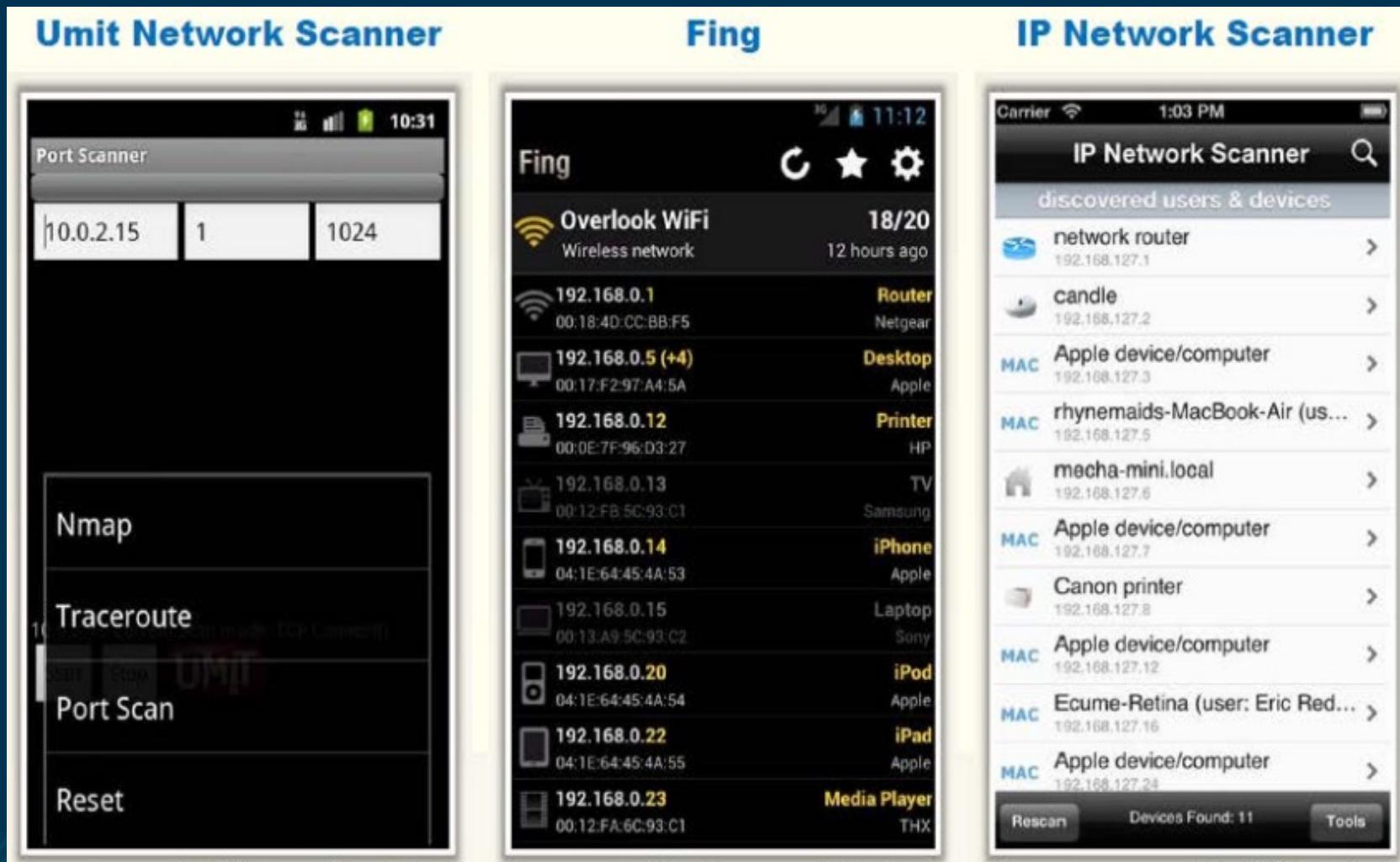
ICMP Echo Request 192.168.168.7

ICMP Echo Reply 192.168.168.8

4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công



4. Các giai đoạn của cuộc tấn công

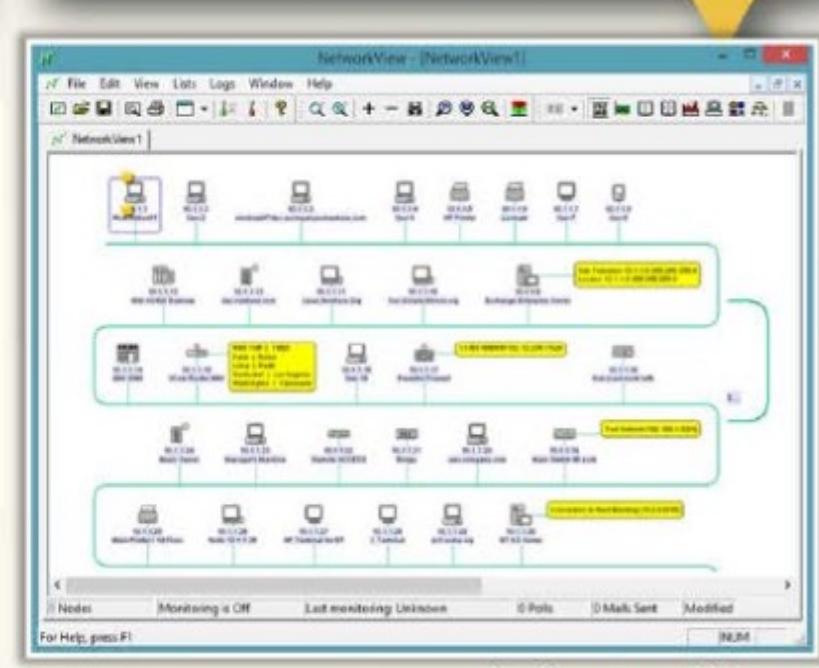
OpManager

OpManager is a network monitoring software that offers advanced **fault and performance management** functionality across critical **IT resources** such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, etc.



NetworkView

- NetworkView is a **network discovery and management** tool for Windows
- Discover TCP/IP nodes and routes** using DNS, SNMP, ports, NetBIOS, and WMI



4. Các giai đoạn của cuộc tấn công

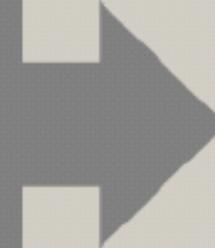
Phase 3 – Gaining Access

Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network

The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

The attacker can gain access at the operating system level, application level, or network level

Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.



4. Các giai đoạn của cuộc tấn công

Phase 4 – Maintaining Access



Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system



Attackers use the compromised system to launch further attacks



Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans



Attackers can upload, download, or manipulate data, applications, and configurations on the owned system



4. Các giai đoạn của cuộc tấn công

Phase 5 – Covering Tracks

Covering tracks refers to the activities carried out by an attacker to hide malicious acts

The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution

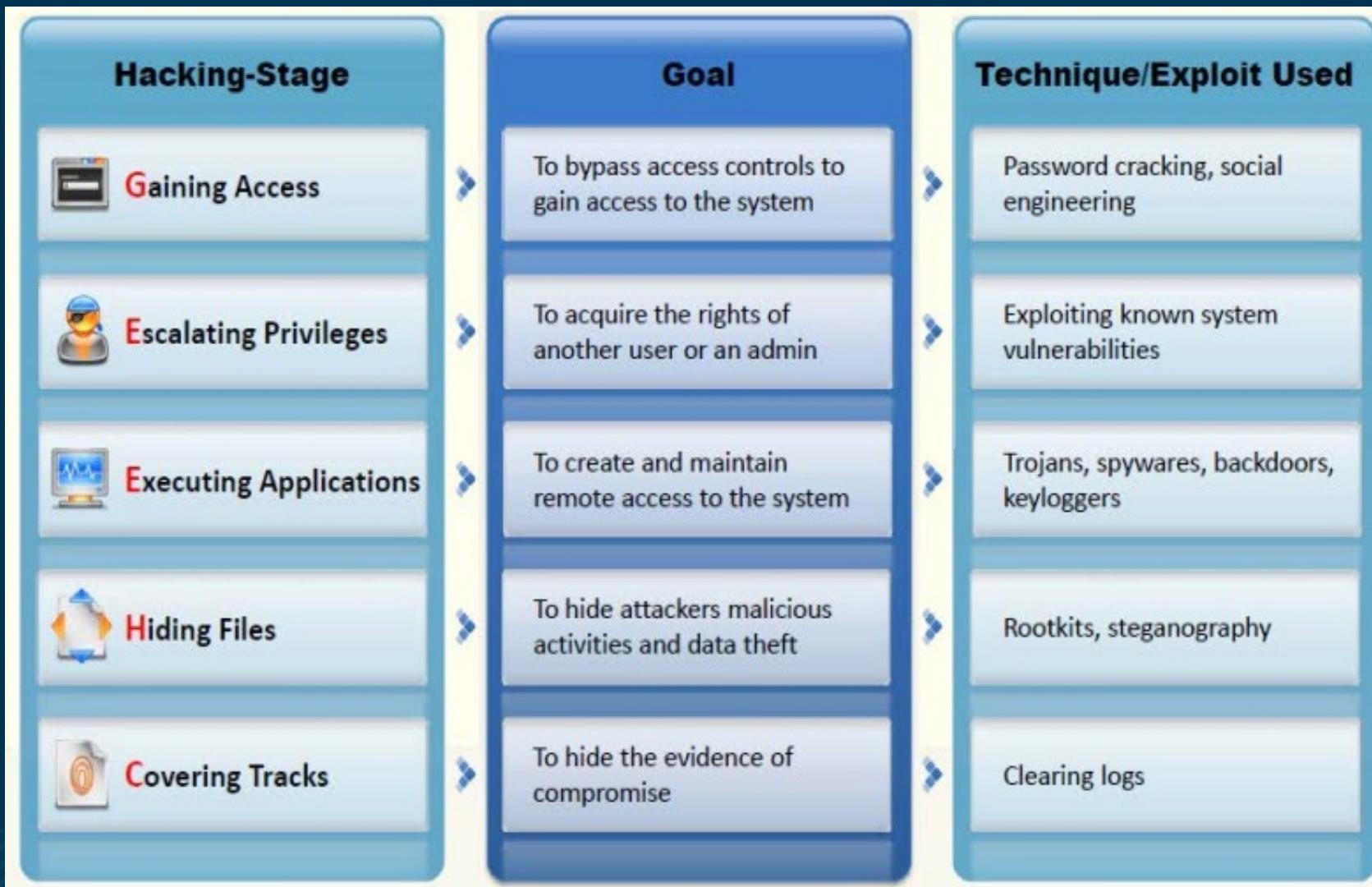


The attacker overwrites the server, system, and application logs to avoid suspicion



Attackers always cover tracks to hide their identity

4. Các giai đoạn của cuộc tấn công



Bài tập

1. Tìm hiểu và trình bày các cuộc tấn công mạng đã xảy ra:

- Thực hiện theo nhóm đồ án
- Mỗi nhóm thực hiện:
 - 2 cuộc tấn công mạng
 - 2 loại mã độc
- Gợi ý: Tên, loại, thời gian, cơ chế/phương pháp hoạt động/tấn công, mức độ nguy hiểm, hậu quả, biện pháp khắc phục, ...

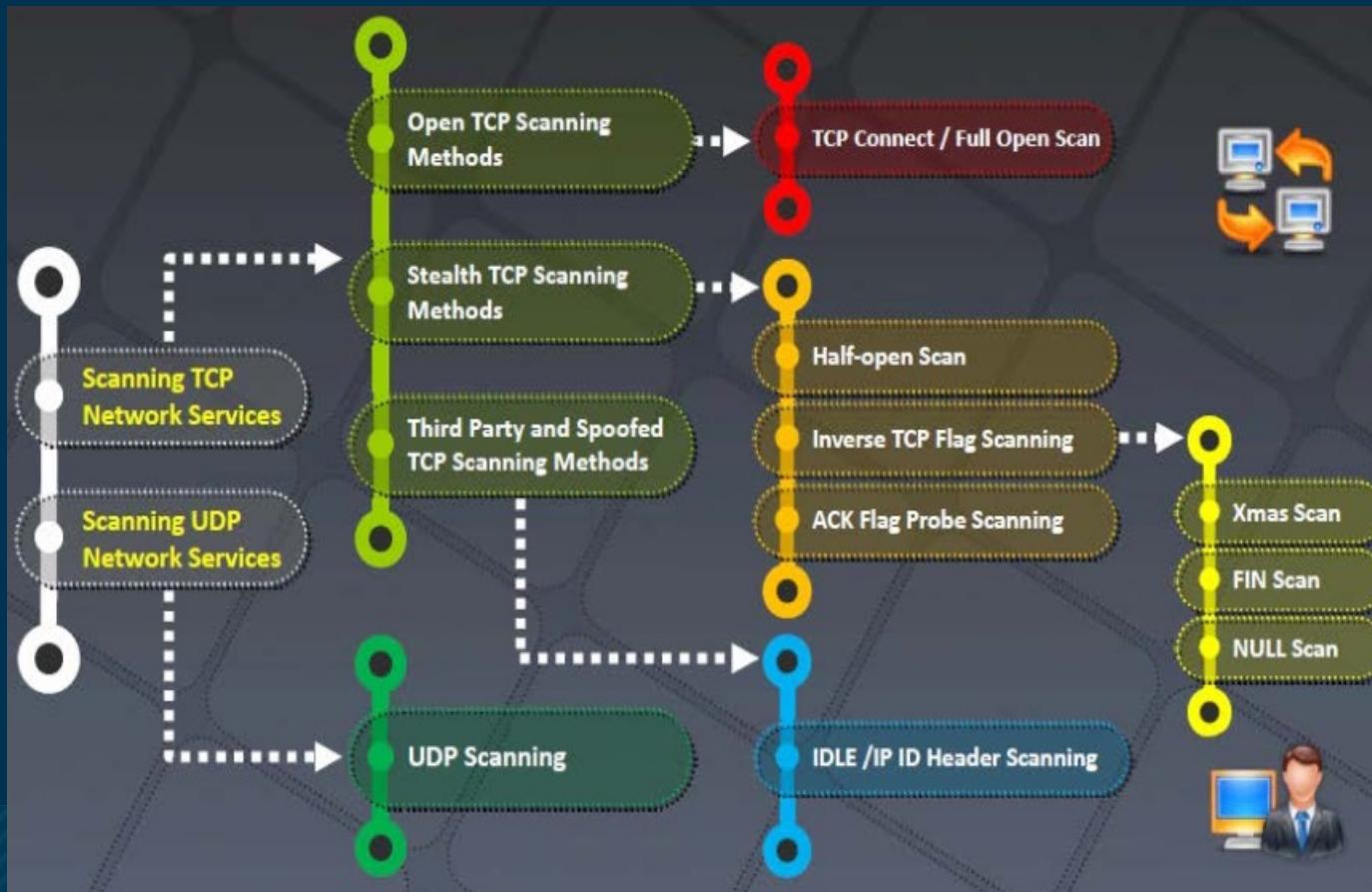
Bài tập

2. Sử dụng các kỹ thuật Reconnaissance, Scanning trong các bước thực hiện của một cuộc tấn công để tìm hiểu về:

- Bản thân
 - Thông tin về Trường ĐH CNTT
- Trên không gian mạng Internet?

Bài tập

3. Trình bày chi tiết cơ chế hoạt động của các kỹ thuật scanning sau:



Refs

- CEH Slides
- An toàn mạng máy tính, ThS. Tô Nguyễn Nhật Quang, UIT
- Kaspersky Security Bulletin 2017
- ...



Thank You

AN TOÀN MẠNG MÁY TÍNH

#02: CÁC KỸ THUẬT, GIAI ĐOẠN TÂN CÔNG CƠ BẢN

ThS. Lê Đức Thịnh, UIT