

An ninh mạng 1

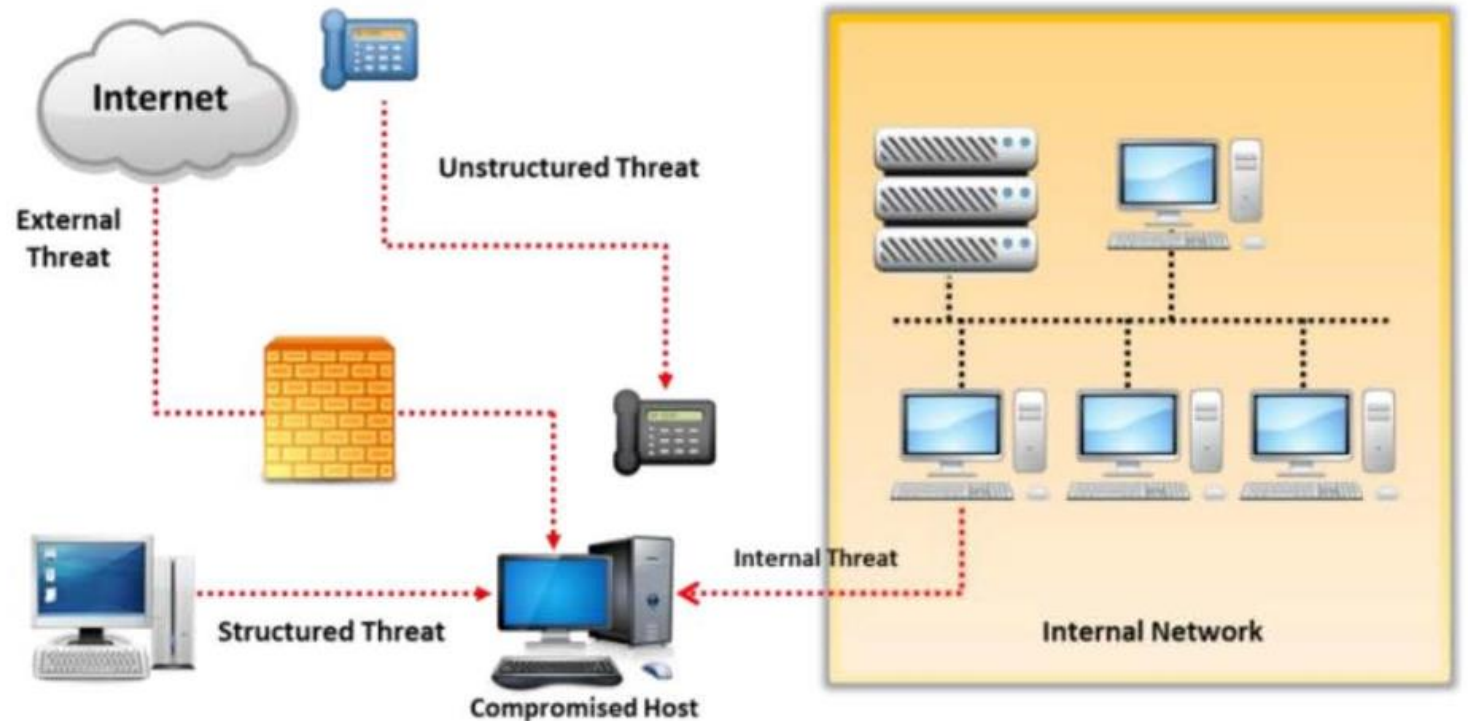
Một số thuật ngữ về an toàn thông tin

- Thread
 - Hacker, virus, hỏng phần cứng/mềm...
- Vulnerability
 - Thiếu bản vá lỗi bảo mật, password yếu
- Exploit
 - Quá trình khai thác điểm yếu bảo mật
 - Local exploit/remote exploit
- Attack



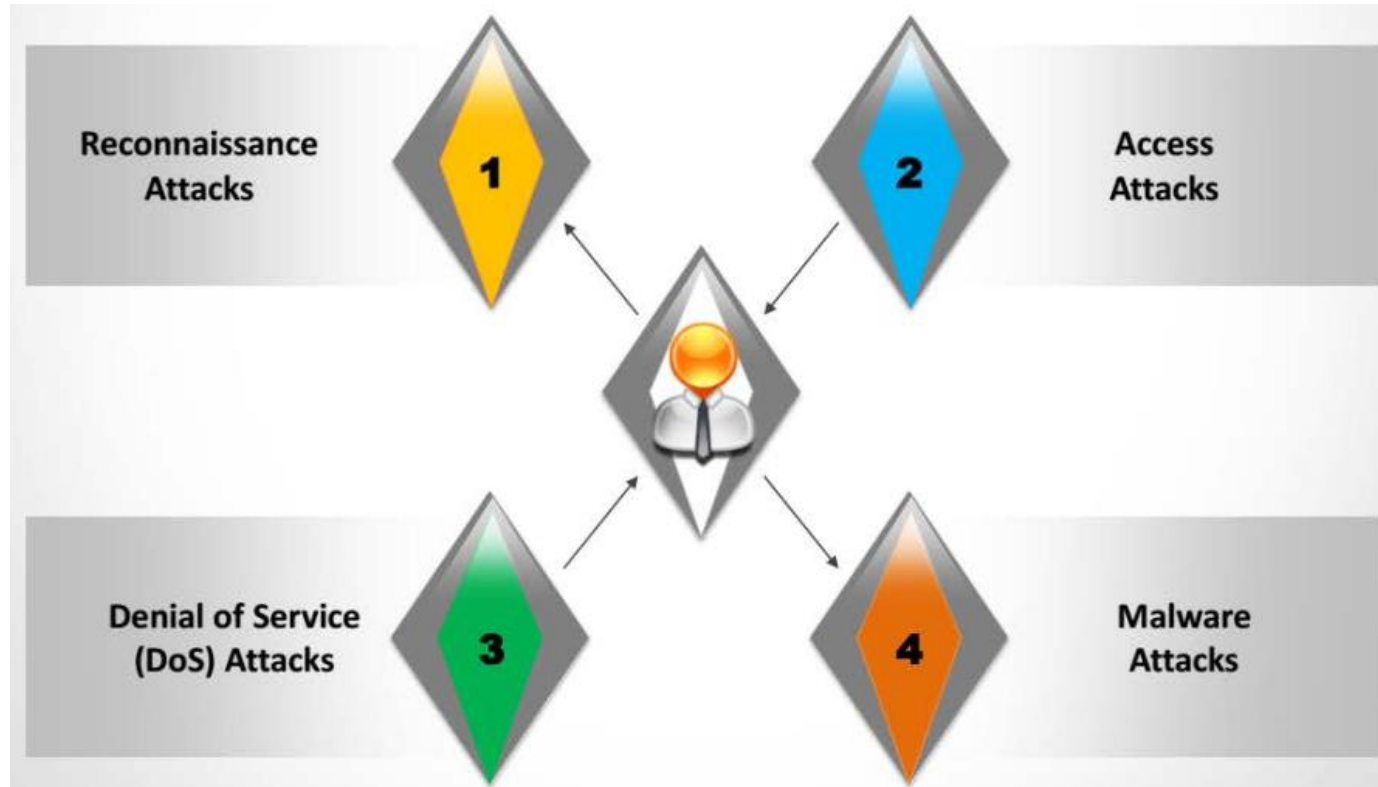
Các kiểu thread

- Internal thread
- External thread
- Unstructured thread
- Structured thread



Một số kiểu tấn công

- Lấy thông tin



Khai thác điểm yếu
Unauthorized access, brute force, privilege escalations, man-in-the-middle

Trojans, virus, worms

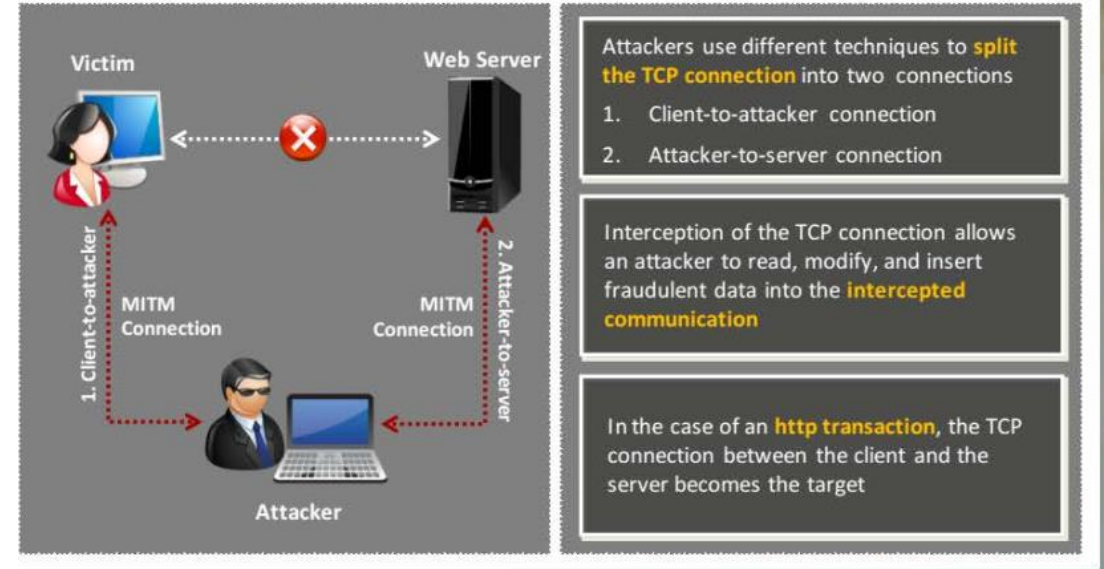
Thu thập thông tin

- Các kỹ thuật thu thập thông tin
 - Social engineering
 - Port scanning
 - DNS Footprinting
 - Ping Sweeping
- ICMP scanning
- Nmap scan

- 
- Domain Name
 - Internal Domain Names
 - Network Blocks
 - IP Addresses of the Reachable Systems
 - Rogue Websites/Private Websites
 - TCP and UDP Services Running
 - Access Control Mechanisms and ACL's
 - Networking Protocols
 - VPN Points
 - IDSes Running
 - Analog/Digital Telephone Numbers
 - Authentication Mechanisms
 - System Enumeration

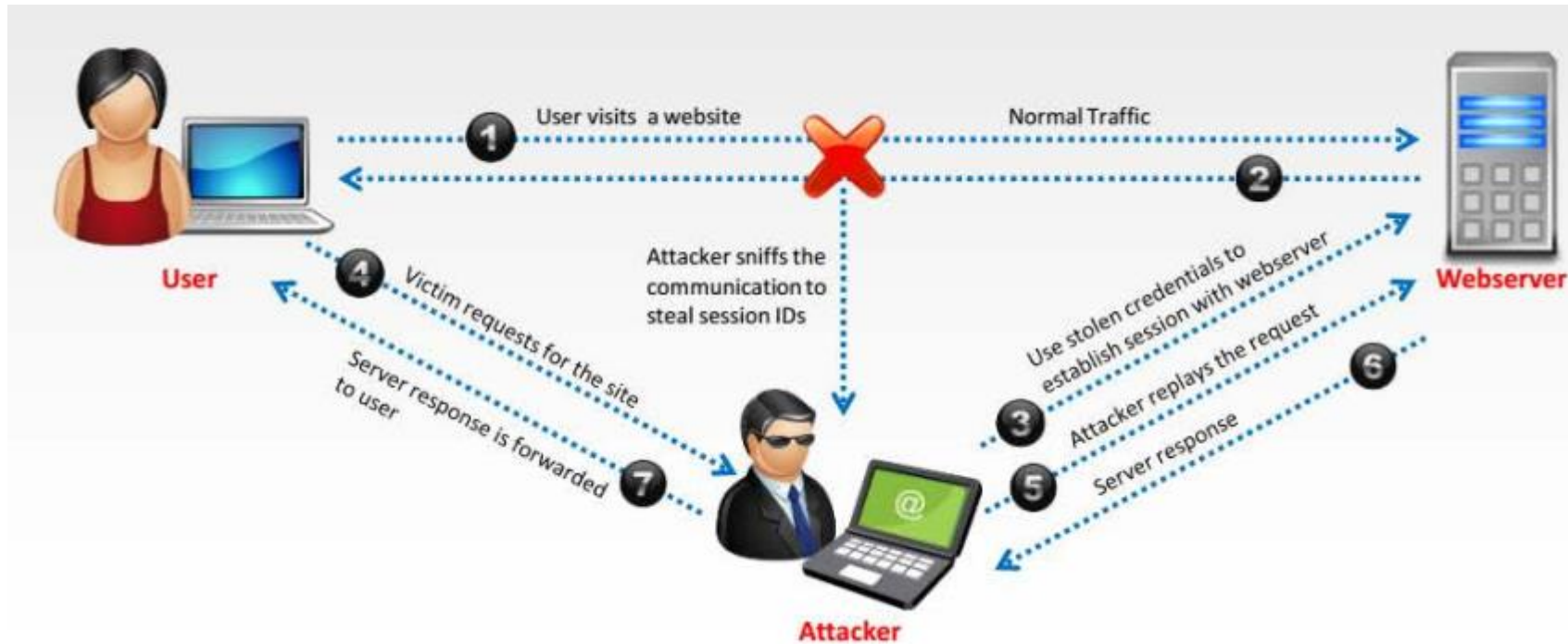
Access attack

- Password attack
 - Tấn công server và router
 - Kỹ thuật brute-force, social engineering, spoofing, phishing, malware, sniffing
- Network sniffing
 - Bắt gói tin
- Man-in-the-middle attack



Access attack

- Replay attack

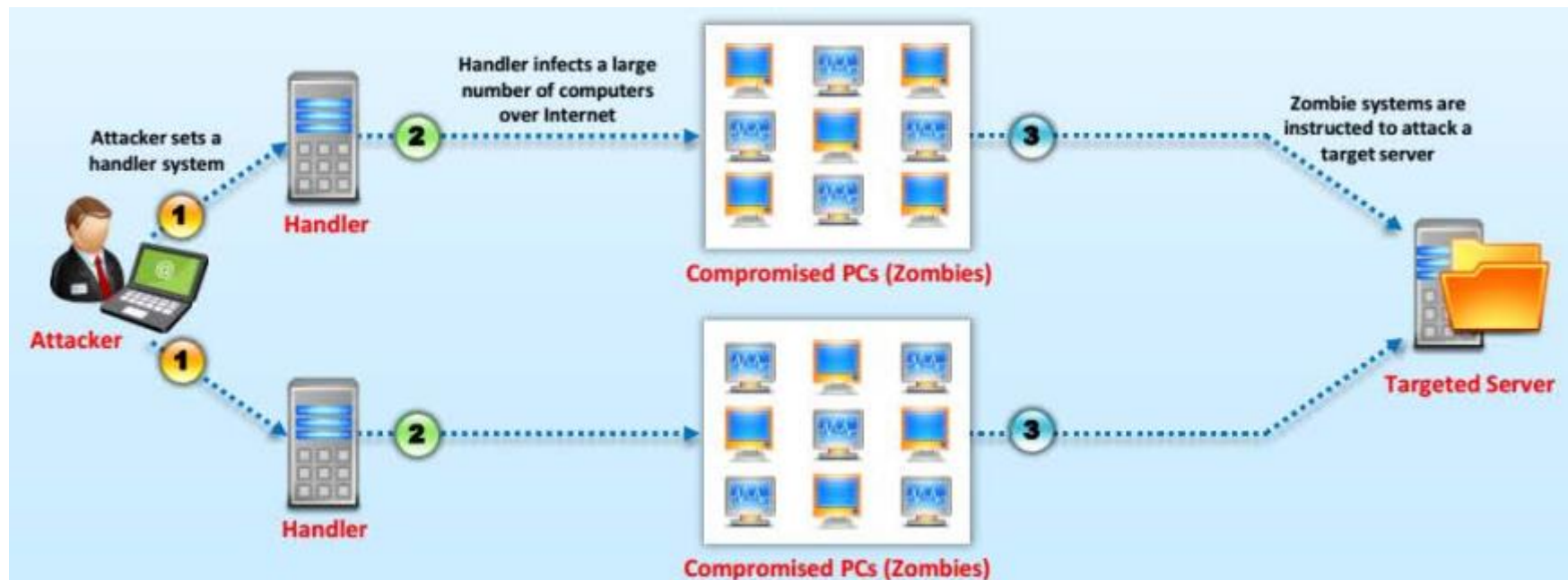


Access attack

- Privilege escalation
 - Sử dụng tài khoản mức thấp để lấy quyền admin
- DNS poisoning
- DNS cache poisoning
- ARP poisoning
- DHCP starvation attack
- DHCP spoofing attack
- Switch port stealing
- MAC spoofing/duplicating

Deny of service – DoS/DDoS

- DoS ngăn chặn người dùng truy cập mạng bằng cách tấn công network bandwidth
- DDoS



Malware attack

- Virus
- Trojan
- Adware
- Spyware
- Rootkit
- Backdoor