ATTACKS ANALYZE IN THE COMPUTER NETWORKS

Denis MALISENCU

Universitatea Tehnică a Moldovei

Abstract: *In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. The most common attacks are flooding, sniffing and spoofing. They are very destructive and can cause a lot of loss. Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism. A cyberattack can be employed by nation-states, individuals, groups, society or organizations. A cyberattack may originate from an anonymous source.*

Keywords: *Flooding,spoofing,sniffing,DoS,MitM,DNS,ARP,IP.*

1. Flooding attacks

A flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. This effectively denies service to legitimate clients. Some systems may also malfunction or crash when other operating system functions are starved of resources in this way.

A denial-of-service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service or network. In the DoS, the attackers usually send several messages asking the server to accepts requests from invalid return addresses.

A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server. A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet.

Mirai IoT botnet-is one of the most powerful DDoS attacks of all time. Essentially,Mirai functions by scouring the internet for connected, vulnerable IoT devices and will infiltrate using common factory default credentials,after witch it infects those devices with the MIrai malware. Discovered in August of 2016 by security research firm MalwareMustDie.The Dyn attack resulted in many marquee websites, including Airbnb, GitHub, Netflix, Reddit,and Twitter, being disrupted.

2. Spoofing attacks

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Examples:

- MAC spoofing - MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device

- IP spoofing – In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of impersonating another computing system.

- Arp – In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network.

- DNS - DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address.

Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message, and are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

In 2015, unidentified hackers have used DNS spoofing techniques to redirect traffic from the official website of Malaysia Airlines. The new homepage showed an image of a plane with the text “404 – Plane Not

Found” imposed over it. Although no data was stolen or compromised during the attack, it blocked access to the website and flight status checks for a few hours.

In June 2018, hackers carried out a two-day DDoS spoofing attack against the website of the American health insurance provider, Humana. During the incident that was said to have affected at least 500 people, the hackers have managed to steal complete medical records of Humana’s clients, including the details of their health claims, services received, and related expenses.

3. Sniffing attacks

Sniffing attackor a sniffer attack, in context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets).

Sniffing attacks can be compared to tapping of phone wires and get to know about the conversation, and for this reason, it is also referred as wiretapping applied to computer networks. Using sniffing tools, attackers can sniff sensitive information from a network, including Email traffic (SMTP, POP, IMAP traffic), Web traffic (HTTP), FTP traffic (Telnet authentication, FTP Passwords, SMB, NFS) and many more. The Packet Sniffer utility usually sniffs the network data without making any modifications in the network's packets. Packet sniffers can just watch, display, and log the traffic, and this information can be accessed by the attacker. Example: 49 busted in Europe for Man-in-the-Middle bank attacks

Police seized laptops, hard disks, telephones, tablets, credit cards and cash, SIM cards, memory sticks, forged documents and bank account documents.

The parallel investigations uncovered international fraud totaling €6 million (about £4.4 million or $6.8 million) – a haul that Europol says was snagged within a “very short time.”

The gang allegedly targeted medium and large European companies via MiTM attacks.

Bibliography

1. Bastion Ballmann, *Understanding Network Hacks: Attack and Defense with Python*, 2015.
2. Matthew Monte, *Network Attacks and Exploitation: A Framework*, 2015
3. Mike O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, 2015
4. *Michael N Schmitt; Brian T O'Donnell; Naval War College, Computer network attack and international law, 2002.*