Distributed Denial of Service

Information Security – Lecture 19

Aadil Zia Khan

Practice

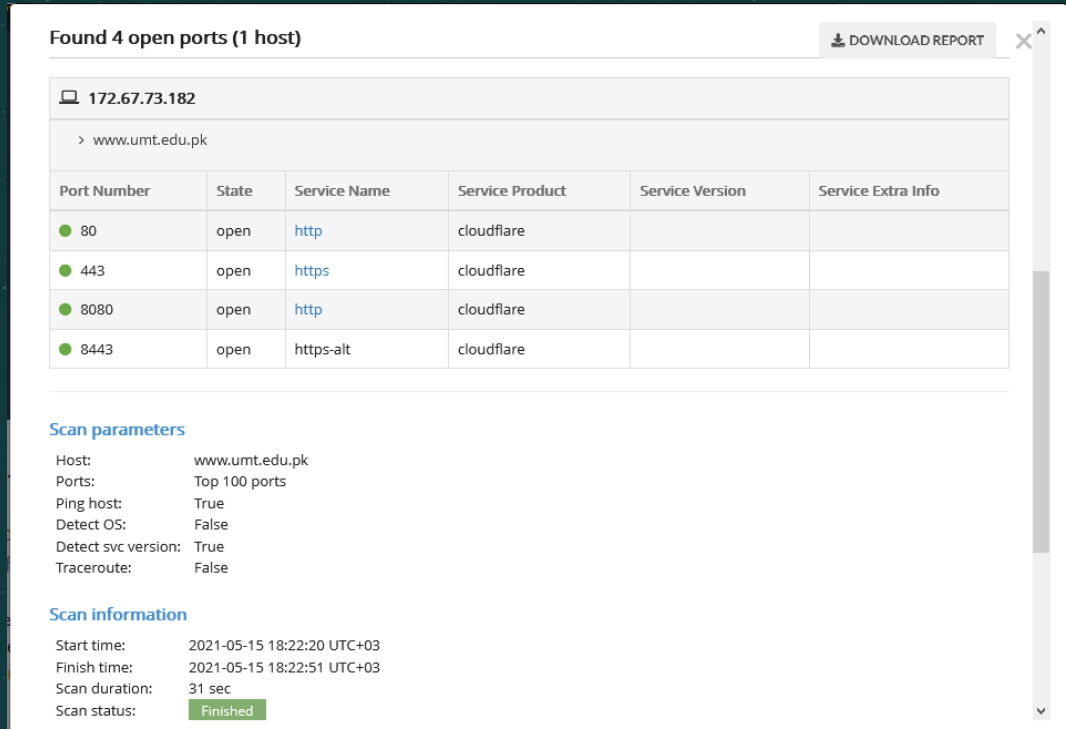
- Scenario: UMT has announced online final exams. Due to the ongoing covid situation, you were expecting that every student would get an A, and so you did not prepare. Now you plan to bring down the servers so that no one can conduct online exams. How will you carry out a Denial of Service attack?

Possible Solutions

- LMS and WWW servers are easily accessible – lets attack those
- Now we have to flood them with traffic – generate a large volume of one of the following packets
  - ICMP flood - Internet Control Message Protocol
    - Error-reporting protocol – used to report network problems
    - Ping application uses the ICMP protocol
    - ICMP caters to multiple message types (e.g., echo, destination unreachable, time exceeded)
    - Networks may block some types (e.g echo) – attacker has to find the type that is not blocked
  - TCP SYN flood / SYN spoofing
    - Send a large volume of TCP SYN packets to overwhelm the server's link and connection table
  - UDP flood
    - Write a socket program that sends a large volume of packets to any open UDP port on the server

Network Scanners

- How can we find out which UDP ports are open? How can we find out which ports are open?
  - We use scanners like Nmap
- Nmap features include:
  - Host discovery
  - Port scanning
  - OS detection
  - Topology discovery
  - …



Found 4 open ports (1 host)

DOWNLOAD REPORT

172.67.73.182

› www.umt.edu.pk

Port Number	State	Service Name	Service Product	Service Version	Service Extra Info
80	open	http	cloudflare		
443	open	https	cloudflare		
8080	open	http	cloudflare		
8443	open	https-alt	cloudflare		

Scan parameters

Host:	www.umt.edu.pk
Ports:	Top 100 ports
Ping host:	True
Detect OS:	False
Detect svc version:	True
Traceroute:	False

Scan information

Start time:	2021-05-15 18:22:20 UTC+03
Finish time:	2021-05-15 18:22:51 UTC+03
Scan duration:	31 sec
Scan status:	Finished

Network Scanners For Attack/Defense

Why scan a destination network???

- Find out about the machines visible to the public
  - These are the vulnerable machines
- Find out about the Operating Systems and applications running on those systems
  - This tells us about the running software (and hence their well known vulnerabilities)
- Find out about the open ports
  - This tells us about the ports on which the machine will connect or respond
  - Can also be used to find out about the running applications (e.g., ports 80 and 8080 imply the http server is running, and port 123 implies the Network Time Protocol server is running)
- Find out about the network topology
  - The more information about the infrastructure the attacker has, the more vulnerable it becomes

Problem (*for the attacker*) With Single Source Attack

- All of these flooding attack variants are limited in the total volume of traffic that can be generated if just a single system is used to launch the attack
- The use of a single system also means the attacker is easier to trace

Conducting More Powerful DoS Attacks

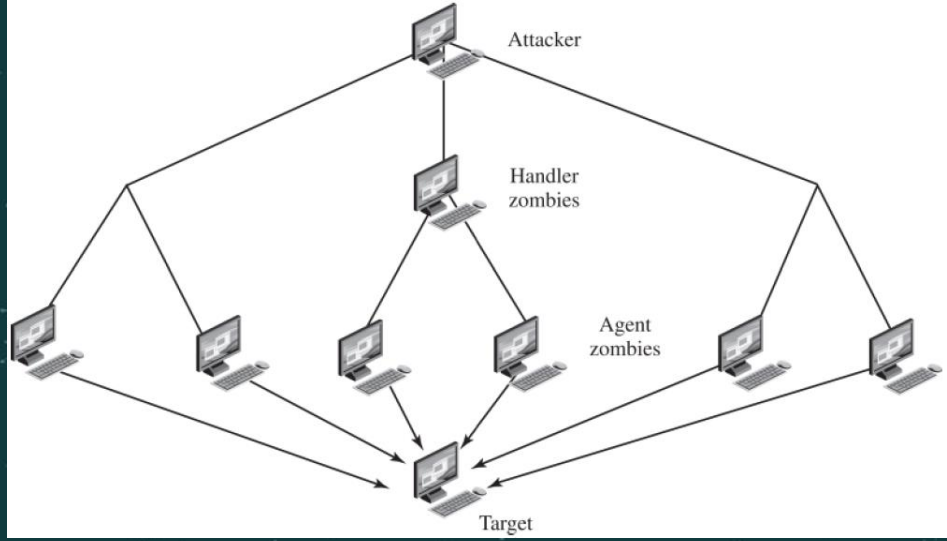
- DoS attacks more sophisticated these days and involve multiple attacking systems
- By using multiple systems, the attacker can significantly scale up the volume of traffic that can be generated
- By directing the attack through intermediaries, the attacker is further distanced from the target and significantly harder to locate and identify
- Indirect attack types that utilize multiple systems include
  - Distributed denial-of-service attacks (DDoS)
  - Reflector attacks
  - Amplifier attacks

DDoS relies on unauthorized usage of zombies/botnets

Reflector/Amplifier attacks rely on a valid usage of a protocol to carry out the attack

Both cause denial of service

Distributed DoS



- Zombies: attacker uses malware to subvert the system and to install an attack agent, which they can control
- Botnets: large collections of zombies under the control of one attacker
  - Botnets are available for hire - 40% of DDoS attacks in 2015 were from such botnets for hire
- Attacker sends a single command to handler zombies, which then automatically forward it to all the agents under their control
  - In this way a large volume of attack traffic is generated while hiding the attacker's footprint
- Famous tools for conducting DDoS attack => Tribe Flood Network, HULK, Tor's Hammer, Slowloris, LOIC, …

Reflection Attacks

Zombies/Botnets not needed

- Attacker sends packets to a known service on a valid server using victim's spoofed address
- When the intermediary responds, the response is sent to the victim
  - Basically the attack is reflected off a valid server, which is termed the reflector, towards the victim
- The reflectors are chosen to be high-capacity network servers or routers with very good network connections
- Ideally, the attacker would like to use a service that creates a larger response packet than the original request
  - This allows the attacker to convert a lower volume stream of packets from the originating system into a higher volume response stream directed at the victim
  - The DNS, SNMP, ISAKMP services have all been exploited in this manner, in part because they can be made to generate larger response packets directed at the victim
  - TCP SYN packets with spoofed address can also be used in reflection attacks

Amplification Attacks

Zombies/Botnets not needed

- Amplification attacks are a variant of reflector attacks
  - They involve sending a packet with a spoofed source address for the victim system to the reflector
  - They differ in that they generate multiple response packets for each original packet sent
    - E.g., by directing the original request to the broadcast address for some network so that all hosts on that network can potentially respond to the request, generating a flood of responses

Example: DNS Reflection-Amplification Attacks

- A selection of suitable DNS servers with good network connections are chosen
- Attacker creates a series of DNS requests containing the spoofed source address of the victim - directed at a number of the selected name servers
- Servers respond to these requests, sending the replies to the spoofed source, which appears to them to be the legitimate requesting system
- Victim is then flooded with their responses
- Because of the amplification achieved, the attacker need only generate a moderate flow of packets to cause a larger, amplified flow to flood and overflow the link to the target system

Example: Smurf Reflection-Amplification Attack

- Large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address
  - Note: when using a unicast IP address, a packets goes from one node to another - when using a broadcast IP address, every node that receives the packet makes copies and forwards to all other nodes
- The attacker only needs to send a single packet – the network makes copies and causes a broadcast storm
- Devices on a network will, respond to this by sending a reply to the source IP address
- If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic
- Google smurf.c in case interested in exploring the source code for this attack