**Part I –Social Engineering Attacks**

Phishing 没有特定目标

oSpear有特定的群体, Whaling高层, Vishing

Tailgating后挡门

Dumpster Diving废纸里找

Shoulder Surfing偷看

Impersonation假装

**Part II –Network Protocol Review**

**DNS (Domain Name System)**： Recursive Query 向其他服务器查询 / Non-recursive query 直接回答

**TCP (Transmission Control Protocol)**： Connection oriented (Used for high reliability)

HTTP, HTTPS, FTP, SMTP, etc. （SYN，ACK，FIN）

Spoofing Source Addresses

**UDP (User Datagram Protocol)**： •Connection-less (Used for speed)

VOIP, Streaming Audio and Video Protocols, DNS, etc.

**ICMP (Internet Control Message Protocol)**： •Used for diagnostic or control purposes

**Part III –Network Scanning （ports）**

**Nmap**–Security Scanner: World’s most popular network security scanner

•GUI version also available called Zenmap

**9 Phases of an Nmap Scan**

1.Target enumeration计算:

2.Host discovery (Ping scanning):

Can use ARP, ICMP, TCP requests for discovery

3.Reverse-DNS Resolution:

4.Port Scanning:

5.Version Detection:

6.OS Detection:

7.Traceroute:

8.Script Scanning:

NmapScripting Engine (NSE) uses Luaprogramming language to gain even more information about targets

9.Output:

Scanners typically skip port 0

•Attackers will often use different scan techniques for stealth or to try to sneak past firewalls

•-sSSYN Stealth Scan

•-sAACK scan to determine is firewall rules are

stateful

•-sF, -sX, -sNFIN, Xmas, Null are used to try to

determine if services are up past firewalls

**Part IV –Denial拒绝 of Service Attacks (DoS& DDoS)**

定义: An action that prevents or impairs损伤 the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.

•Denial of Service (DoS) = Single Attacker

•Distributed Denial of Service (DDoS) = Multiple Attackers or Botnet

Denial of Service Attacks are Generally Against:

**•Network bandwidth**

通常有：•Flooding attack types:

**SYN**

•Attacker can:

1.Exhaust System Resources

Send SYNs until victim computer’s connection queue is full

2.Exhaust Network Bandwidth

Send massive amounts of SYNs to overwhelm the network data link if victim computer has a large connection queue

骇客自己不DoS的防止办法：Spoof the source address!

SYN Flood Defenses

•Reject source IP(s) with a filter or IPS

•Increase TCP connection queue size

•Traffic Shaping

Load balancing

Cache SYNs

SYN Flood DDoSDefenses

•Contact ISP for:

Upstream Filtering (usually ineffective if DDoSdirected at a website)

Cloud-Based Mitigation (malicious requests scrubbed)

•Prolexicis a DDoSmitigation service

1.8 Tbpsof dedicated mitigation bandwidth

Provides SOC personnel to monitor customer on-premiseequipment

**ICMP**

•Could block Pings but attackers use other ICMP packet types:

Destination unreachable

Time exceeded

•May use spoofed source addresses

**UDP**

Scapy

•A powerful interactive packet manipulation program

•Can be imported into Python for protocol testing or to create DoSscripts

**Smurf Attack 拆分洗钱**

•In an ICMP flood, the attacker directly attacks the victim with ICMP requests

•In contrast, a Smurf attack uses a network of hosts to indirectly attack the victim with ICMP replies Smurf Attack

•Attacker sends ICMP echo request (ping) to the network broadcast address.

Smurf Attack Defenses

•Shut off response to directed broadcasts on your firewall or router.

•Cisco:

“no ipdirected-broadcast” for each interface

“no ipsource route”

•Linux:

echo 1 >/proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts

Smurf Attack Defenses

**Slowloris （Web Server DoS-SlowlorisAttack）**

•No spoofing and complete TCP handshake

•Issues partial HTTP requests with no terminating new line sequence

•Over several minutes, slowly sends additional partial HTTP headers to keep sockets from closing

Repeat that 100s of times to saturate web server’s connection queue to not allow new connections

SlowlorisDefenses

•Load balancer

•Firewall filters

•Patching web server

•Reset web server service

**DNS Reflector Attack**

•Send queries to DNS server with spoofed source address as victim

•Replies get sent to the victim

•Exhausts network bandwidth

**DNS Amplification扩大**

•Similar to DNS Reflector but uses public recursive lookups to amplify attack.

•Exhausts network bandwidth

DNS Amplification Attack Steps：

1.Attacker locates public DNS servers that will perform public recursive lookups

2.Attacker has own DNS server with a huge TXT record ready

TXT record provides text information to sources outside of your domain

3.Attacker sends request to public DNS server that will have to lookup the record located on the attacker’s DNS server

4.Public DNS server caches the huge TXT record waiting for the next time it receives a query for it

5.Attacker sends another DNS request to the public server but spoofs the source address (which will receive the DNS response to the query) with the victim’s IP

6.Public DNS server hits the victim with the huge TXT record as a response to the query

7.Attacker repeats step 5 over and over to flood victim



DNS Amplification Attacks Defenses

•If you have public DNS servers, perform recursion only for your internal network

•ISP upstream filtering

•DDoSservice

**IP Fragmentation Attack**

•Max IPv4 packet size is 65,535 bytes

•Large packets are fragmented in order to travel across a network:

Ethernet Maximum Transmission Unit (MTU) = 1500 bytes

•Packet > 65,535 bytes would therefore be above the protocol limit and would also be sent as fragmented

IP Fragmentation Attack –Ping of Death

•Attacker sends original unfragmented65,536 byte datagram:

•Packet is fragmented into several smaller 1500 byte datagrams to travel across Ethernet LAN

•Victim’s system receives the fragmented datagrams and beings reassembling them into the 65,536 byte original datagram

•Since the datagram is one byte over the protocol specification, a buffer overflow could occur which could cause a system crash

IP Fragmentation Attack Defenses

•System patches implement a check:

if sum of datagram fragments > 65,535

reject packet

else

accept packet

Part V –MiTMAttacks

**Man-in-The-Middle Attacks (MiTM)**

•Attacker inserts themselves as relay/proxy between communications of two hosts

•Attacker could then either:

Accept and sniff traffic from each host and forward it to other host

Hijack and alter traffic during transit

Hijack and drop traffic during transit

**Types of MiTMAttacks**

•ARP Cache Poisoning

•Web Spoofing

•DNS Spoofing

•ICMP redirects

•DNS Poisoning

•Session Hijacking

•What is ARP?

Address Resolution Protocol

We use ARP to map IP addresses to MAC addresses

•What is a MAC address?

Media Access Control

The address of a network interface

•Every computer has an ARP cache that holds these IP to MAC address mappings

arp-a

•However, ARP allows any host to send a response even if no request was initiated

This is called Gratuitous免费的 ARP

•Therefore, an attacker could poison the ARP cache to direct traffic however they want!

•Attacker must be on the same network as the victim to poison the ARP cache

**ARP Cache Poisoning**

Attacker Poisoning –Three Necessary Steps

•Attacker sends two Gratuitous ARP responses:

First one to update Victim’s ARP cache

oHey, the Gateway’s IP is at attacker’s MAC address!

Second one to update Gateway’s ARP cache

oHey, the Victim’s IP is at attacker’s MAC address!

•Attacker enables IP forwarding on their host to intercept and forward all incoming and outgoing traffic

After Attacker Poisoning

•Attacker can now intercept all incoming and outgoing transmissions between the Victim and any other host on the Internet!

Part VII –A Few Final Attacks

Session Hijacking

•An attacker could also hijack the session between two computers

Same as spoofing except in hijacking the attacker is also taking the victim offline so that she can hijack and takeover the session between victim and other host

•Attacker uses ARP poisoning to sniff the traffic to see the TCP sequence numbers between the victim and a web server

•Attacker responds with correct TCP sequence numbers pretending to be the victim to try and take over the session

•An ACK Storm will occur:



**DoS through ARP Poisoning**

•Attacker could DoSthe victim by sending two Gratuitous ARP responses:

•Response to update the Victim’s ARP cache

Hey, the Gateway’s IP is at AA:BB:CC:DD:EE:FF!

•Response to update the Gateway’s ARP cache

Hey, the Victim’s IP is at FF:BB:CC:AA:EE:DD!

\*AA:BB:CC:DD:EE:FF and FF:BB:CC:AA:EE:DD are non-existent MAC address made up by the attacker.

Defenses for ARP Cache Poisoning

•Software to inspect all ARP requests and responses

Example: Cisco’s Dynamic ARP Inspection feature

•Hard assign the ARP tables

Pain to add new machines to the network

•Use encryption! SSH, TLS 1.1+, etc.

**Replay Attacks**

•Keep in mind that there are also tools available such as tcpreplaythat can take a pcapand play it back.

•What is the danger of that?

Could replay the pcapto pass a victim’s authentication credentials or session cookies in order to authenticate as the victim.

Defenses for Replay Attacks

•Time Stamped Tickets such as Kerberos

•Session Cookies with Quick Expiration

**Buffer Overflows**

•Occurs when a program accepts more data than the developer allocated for it

•Example:

char buffer[10]; #Holds 10 characters

•User could enter 20 characters and overflow the buffer depending on the function used

•Common functions in buffer overflows that don’t perform bounds-checking

Basically, these functions don’t check the size of the destination buffers:

gets

getws

memcpy

memmove

printf

Buffer Overflows

scanf

sprintf

strcat

strcpy

strcmp