network-attacks.md

Networks Attacks: a brief recap

Intelligence Gathering

Every attacks start with this phase. The attacker tries to gather information such as person names, phone numbers, email addresses, IP addresses, domains, host names, hosts, routers and so on. The attacker can use

- Public sources, such as social networking web sites, professional networking sites, resumes of current and past employs and job offers. This can help also the attacker to identify which technologies are used by the company.
- WHOIS interrogation. This is used to interrogate the whois server for the top level domain in order to learn technical contact details to maybe put in place a phishing attack or in general social engineering.
- DNS interrogation. Under the same domain can be instantiated many host names. These are machines owned by the same domain owner, that may be hidden to the public but still available through internet. It would be nice for an attacker know those host names to advance the attack. In order to know all the A records of the nameservers of the attacked company the attacker can:
  - Force a DNS zone transfer, if DNS server is misconfigured and responds to everyone (rare)
  - DNS bruteforcing, interrogating the DNS with common host names to discover them.
- Network sniffing, passive techniques but ca be used to gather network information, see unencrypted data, but it is slow and require to be inside a LAN for instance.

Network Scanning

A set of techniques aimed at discovering hosts and services on a network.

- Host Discovery: simply send ICMP requests to that host and see if it responds. If yes, this means that host is up and running
- Port Scanning is used to identify services running on a specific host. Many types of port scanning are avaialble:
  - SYN Scanning: initiate a TCP handshake on a port. If it goes well (you send SYN, you receive SYN+ACK, then you send a RST to not consume the server memory and being undetected), the port is open. Otherwise if you receive a RST, the port is closed. If server does not reply at all, it means that the port is filtered.
  - UDP Scanning: send an UDP probe with empty payload. The problem is that application will not responds to unexpected packets and no handshake is available so no ack on packets like TCP. So if you receive back an ICMP Port Unreachable, the port is closed. No response at all means the port is either OPEN or FILTERED!
  - Service Scanning: basic example, send an HTTP request on port 80. If it replies back, a web server is running!
  - TCP/IP Stack Fingerprinting: analyze fields like Time To Live in IP packets and window size in TCP segments to understand version of target Operating System.

Layer 2 Attacks

- MAC Spoofing: repeatedly sending frames with the source MAC address of a legitimate device. This will corrupt the CAM table at the switch. The effect is that the legitimate source MAC will be mapped to another port, the one attached to the attacker. So the attacker can eavesdrop all the incoming traffic directed to that host and also cause a denial of service if that host was providing a service.
- MAC Flooding: repeatedly sending frames with random MAC addresses. This will fill up the CAM table, so if the switch receive a frame from any new MAC address, even legitimate ones, will behave like a hub. The attacker will be then able to eavesdrop on the network. Moreover, since entries in the CAM table are dropped after sometime, a random MAC address can substitute a legitimate one if the latter remained silent for a sufficient amount of time. Next time the legitimate NIC will send a frame, it will be broadcasted by the switch.
- ARP Poisoning: the aim of this attacks is to change the mapping of a MAC address to an IP address, through a gARP message for instance. In this way, all the hosts in the (W)LAN will update their ARP cache. The result is that if an host wants to send a packet to an internal targeted IP, will send it to the attacker, letting him eavesdrop the traffic. An important target IP is the getaway: in this way, every outgoing traffic will be redirected to the attacker, which can eavesdrop and act like a MITM.

Layer 3 and Layer 4 attacks

- IP Spoofing: many kinds of this actually:
  - TCP Spoofing. The attacker tries to interfere with a TCP connection, he has to guess a 32-bit random sequence number.
  - UDP/ICMP spoofing, easy to mount. For instance a rogue SNMP message could be sent.
- TCP SYN Flooding, ancient way to DoS. The attacker send many SYN packets without acknowledging the received SYN+ACK. The victim keeps the connection half open, consuming an amount of memory. Let's say the server has to store at least the sequence number of its connection. The countermeasure is to make use of SYN cookies: instead of generating a random number, the server can create it by using a keyed hash of the source IP, keeping the key secret and locally.
- Smurf Attack: create an ICMP requeste packet with source IP equal to the attacked machine and destination IP equal to broadcast address. So each computer in the network will receive it and will reply back to the spoofed IP, that is the victim. So, as you can see, a single packet is amplified, leading to sending many packets to the victim. You can repeatedly send that kind of packet to perform a DoS.

DDoS

In a distributed denial of services a large network of hosts infected by a malware (called botnet) waits for a command from the attacker. The command will contain the target of the attack. For instance, if the target is a web server, the botnet will start producing infinite requests to that service, causing the web server resources to deplete. We will examine the main countermeasures taken by ISP, even though this kind of attacks is difficult to manage.

- **Blackhole filtering**: The ISP advertises a null0 BGP route to target, so that all traffic to the target is dropped. Not a real countermeasure..
- **Sinkhole routing**: route all the traffic to an intermediary server or groups of servers. Here, traffic can be analyzed. Maybe there's a way to distinguish DDoS traffic from honest one. Once you find out how to do that, you can restore normal route, putting ACL on the routers in order to discard DDoS traffic.
- **Backscatter traceback**: the aim of this technique is to precisely identify the routers where malicious traffic passes. Observation: bots typically spoof their IP address, often resulting i non allocated IPs. So we can do the following
  - advertise BGP null0 route to target, so all traffic to target is dropped.
  - route all traffic to non assigned IP to a sinkhole.

As a consequence of this, what happens is the following:

- router receive a packet with target as destination address. since the null0 route is advertised, the packet will be dropped. Every router when dropping packets create an ICMP packet to inform the sender that the packets has being dropped. This ICMP packet has as source IP the one of the router, and as destination IP a non assigned IP (if the bot generated it). So this packet will be routed using the second route and it will arrive at the sinkhole. Now the sinkhole can use each source IP to understand which routers are routing the traffic of the attack and put firewalls on them, restoring the normal routes so that normal traffic can be redirected to the ddosed servers.