24/02/2021

Step4: WHOIS & DNS Enumeration

While much of the Internet's appeal stems from its lack of centralized control, in reality several of its underlying functions must be centralized to ensure interoperability, prevent IP conflicts, and ensure universal resolvability across geographical and political boundaries.

The core functions of the Internet are managed by a No profit organization: the Internet Corporation for Assigned Names and Numbers (ICANN)

↳ coordinates the assignment of the following identifiers that must be globally unique for the Internet function:

- INTERNET DOMAIN NAMES
- IP ADDRESS NUMBERS
- PROTOCOL PARAMETERS and PORT NUMBERS.

ICANN coordinates the stable operation of the Internet's root DNS system.

ICANN → Country Code Domain Name Supporting Organization (CCNSO)
ICANN → Generics Names Supporting Organization (GNSO)
ICANN → Address Supporting Organization (ASO)

Although management is fairly centralized, the actual data is spread across the globe in numerous WHOIS servers for technical and political reasons. To further complicate matters, the WHOIS query syntax, type of permitted queries, available data, and results formatting can vary widely from server to server.

DOMAIN & IP-RELATED SEARCHES

The first order of business is to determinate which one of the many WHOIS servers contains the information we're after

Three Rs

The authoritative Registry for a given TLD (".com" in this case, contains information about which REGISTRAR the target entity registered its domain with. Then you query appropriate REGISTRAR to find the REGISTRANT details for the particular domain name you're after.

ICANN (IANA) is the authoritative registry for all of the TLDs and is a great starting point for all manual WHOIS queries. REGISTRANT details provides physical addresses, phone numbers, names, e-mail addresses, DNS server name, IPs, etc.

equivalent to

[bosh] $ whois com -h whois.iana.org
[bosh] $ whois keyhole.com -h whois.verisign-grs.com
[bosh] $ whois keyhole.com -h whois.omnis.com

- SuperScan
- NetScan Tools Pro

The WHOIS server at ICANN (IANA) doesn't currently act as an authoritative registry for all the RIRs as it does for the TLDs, but each RIR does know which IP ranges it manages. This allows us to pick any one of them to start our search. If we pick the wrong one, it will tell us which one we need to go to.

Step 5: DNS INTERROGATION

After identifying all the associated domains, you can begin to query the DNS.

↳ **WHAT IS IT?**
DNS is a distributed database used to map IP addresses to hostnames, and vice versa.

ZONE TRANSFERS allows a secondary master server to update its zone database from the primary master. → REDUNDANCY (when the primary server become unavailable).

PROBLEM: when an organization doesn't use a public/private DNS mechanism to segregate its external DNS info from its internal, private DNS information.

To perform a zone transfer we can use nslookup
[per i comandi completi, vedi pagina 34/38].

- Set record type to any so we can pull any DNS records available for a complete list.

- ls -d domain.com to list all the associated records for the domain.

We can manipulate the results with UNIX programs such as: grep, perl, sed or AWK.

If you have many DNS server, you may be able to find one that will allow zone transfers → Tools: host, dig.

- host -l } perform a zone transfer on the domain in input.

- dig used to troubleshoot DNS architectures.
- dnsrecon is the top of the tools for performing zone transfers.

- fierce 2.0 to enumerate DNS entries even though zone transfer attempts fail.

discourage the use of HINFO

Step 6: Network Reconnaissance

Traceroute/tracert → view the route that an IP packet follow from one host to the next.

It uses TTL field in IP packet to elicit an ICMP TIME-EXCEEDED msg from each router. Each router that handles the packet is required to decrement the TTL fields.

hop: counter

We can use Traceroute to determinate the exact path that our packets are taking.

There may be multiple paths; moreover, each interface may have different ACL applied.

Traceroute in UNIX use UDP packet with the option of using ICMP packet with the -I switch.

-g allows user to specify loose src routing.

-p n allows us to specify a starting UDP port number (n) that will be incremented by 1 when the probe is launched

IMPORTANT PORT: UDP port 53 (DNS queries)

COUNTERMEASURES can be employed to thwart and identify the network reconnaissance. Best N.S program to detect this activity: SNORT, BRO-IDS. Also you may be able to configure your border routers to limit ICMP and UDP traffic to specific systems

SCANNING

Scanning: is the equivalent to inspecting the walls for doors and windows as potential entry points.
We will determinate what systems are listening for inbound network traffic and are reachable using tools and techniques.

→ how to can bypass firewalls to scan systems supposedly being blocked by filtering rules.

Network pinging: is the act of sending certain types of traffic to a target and analyzing the results. → ICMP, ARP TCP & UDP traffic to identify if a host is online.

ARP Host Discovery: ARP translates MAC ADDRESS to the IP address that has been assigned to it.
The system has to send some sort of ARP request to start traversing the path to reach its dst.
An ARP scan sends an ARP request out for every host on a subnet, the host is considered "alive" if an ARP replay is received.

→ arp scan = simple ARP pinging and fingerprinting utility. You must run it as the root user.

→ Nmap = tool for anything related to host and service discovery. Nmap support ARP scanning via the -PR option. To perform a host discovery and not a port scanning, use the option: -sn.

→ Cain = provides a ton of functionality for Windows-only crowd that goes way beyond host and service discovery. To perform an

ARP host discovery scan on windows, launch Cain, go to Configure, select your network interface, enable the sniffer and then from the sniffer tab, right click and select Scan MAC addr.

ICMP Host Discovery: ICMP provides a variety of msg to help diagnose the status of a host and its network paths.

MSG TYPE:

type 0: echo replay (ping)

type 8: echo request (ping replay)

type 13: timestamp (sys time)

types 17/18: address mask request/replay (code subnet mask).

→ ping to send ICMP ECHO REQUEST packets to a single host. With Nmap is to use the -sn option.

When this command is executed as the root user, it also perform an ARP ping, sends an ICMP TIMESTAMP msg and performs some TCP pinging to TCP ports 80 & 443.

-PE send an ICMP ECHO REQUEST and skip any ARP resolution

-PM ICMP addr mask

-PP TIMESTAMP

→ Hping3: robust packet-crafting tool that allow you to define any combination of packet types.

→ nping: must be run as root (thus the sudo). The command tells nping to send two (-c 2) ICMP msg (--icmp) of type TIMESTAMP (--icmp-type time) to host 192.168.1.1.

→ SuperScan: sends out multiple ICMP ECHO REQUEST PACKETS in parallel & simply waits and listens for responses. It also allows you to resolve hostnames and view the output in an HTML file.

TCP/UDP Host discovery

Next approach an attacker can take to identify live hosts is to use TCP/UDP packets. At least one open port is available for clients to connect to.

Nmap:

-sn option enables an hybrid-type of attack where it attempts ARP, ICMP and TCP host discovery. If our target host doesn't have TCP port 80 open, or Nmap's packets are otherwise dropped on the way to the target, Nmap considers the host down. We can blindly attempt to query Nmap's default port list by telling Nmap to ignore its host discovery options and just do a port scan. Nmap option -Pn to port scan.

SuperScan:

Using TCP/UDP port scan options, you can determinate whether a host is alive or not - without using ICMP at all. Simply select the checkbox for each protocol you wish to use and the type of technique you desire, and you are off the races.

-nping: versatile, its output is more verbose by default, which may be more info that you need.

ping sweeps countermeasures:

detection: use IDS programs such as Snort, many commercial network and desktop firewall tools can detect ICMP, TCP/UDP ping sweeps.

PREVENTION:

-Evaluate the type of ICMP traffic that you allow into your networks or into specific system. Most routers don't require all types of ICMP traffic to the system directly connected to the

Internet. Although almost any firewall can filter ICMP packets, organizational needs may dictate that the firewall pass some ICMP traffic. If a true need exists, you should carefully consider which types of ICMP traffic you allow pass. If ICMP traffic can be limited with ACLs to your ISP's specific IP address, you are better off.