|  |
| --- |
|  |
| Capstone Experience  IST 894 |
| Lab 10 – Reconnaissance and Network Scanning  Scott Finlon |

Table of Contents

[1. General Context 3](#_Toc87732060)

[2. Technical Context 4](#_Toc87732061)

[3. Solution 6](#_Toc87732062)

[References 12](#_Toc87732063)

# General Context

There are often as many more times that you might think that you’ll need to do research and reconnaissance on an IP address or domain when you are defending your network. It may not seem like taking forward action to find out more information about an entity is helpful in defending, but identifying who owns or operates an IP address or domain can be helpful to identify patterns. You can also use tools like Nmap to identify hosts or endpoints on your network, it can tell you what ports the various hosts have open and what services or service types are running as well. These two components, investigating IP addresses and domains and enumerating what’s on your local network are both important for successful defense, but they both are incredibly different.

External research is generally done with WHOIS for domains, and nslookup or dig for IP addresses. All of these are services that provide ownership information, and sometimes location information for both IPs and domains. For example, when you’re being attacked with a Distributed Denial of Service (DDoS) attack, knowing where the attack traffic is coming from can drastically change your strategy to mitigate it. If you can identify that the majority of traffic is from a certain country, or network it can be much easier to put in a mitigation for that specific group of address than a situation where you’re being attacked by a botnet that consists of thousands of residential Internet Service Provider (ISP) IP addresses. If you’re a company that relies on customers who live behind those residential IPs it’s a much more difficult decision to block the traffic outright and a more sophisticated approach like traffic scrubbing (How Traffic Scrubbing Can Guard against DDoS Attacks, n.d.) might be necessary.

When you are looking at your internal network, how can you expect to defend it if you don’t know what there is to defend. Doing internal network scans to find IP addresses that responds and show that they are alive, and knowing what ports are open on those hosts can allow you to create a risk profile to determine where your efforts should be targeted.

# Technical Context

Obviously, there are some difficulties when it comes to trying to identify external entities compared to internal ones. Nslookup and dig are both tools that allow you to query Domain Name System (DNS) servers to translate domain names to one or more IP addresses. WHOIS is a tool that tells you more information about who owns that specific domain, IP address, or network block. Nmap doesn’t provide any thing like ownership information, but it gives you multiple different ways to scan IP addresses and ports to identify potential vulnerabilities on your network, you can scan with TCP SYN, TCP connect, or UDP scans. This is helpful because different network security devices might block one attempt or protocol but not another, so scanning with different types might show different results that allow you to stitch together a whole picture.

A WHOIS record is a listing that identifies who owns a domain, IP address, or IP network as well as how to get in contact with them. It contains information associated with the person, group, or company that registers the domain name or address space (What Is Whois Information and Why Is It Valuable?, n.d.). However, the European Union adopted the General Data Protection Regulation in April of 2016 and it took effect in May 2018. It’s goal is to protect the privacy of all European Union citizens from disclosures and breaches. It applies to all companies that are based in the EU, but also any company that holds data on any EU citizen regardless of where the company resides (Data Protection and Privacy Issues - ICANN, n.d.). Due to the nature of the sensitive private information that is in a WHOIS record by design, it directly conflicts with GDPR and as a result ICANN and many registrars that do business in the EU or with EU citizens made the decision to redact or remove most of the WHOIS information. While it’s still available for law enforcement agencies, it’s arguably not as useful of a tool anymore. There are many products and services that provide historical WHOIS information to let you know who may have owned a domain or address range at a specific point in history (Historical Whois Data (WhoWas), n.d.).

Nmap on the other hand can be quite powerful, but you there are several things to remember when using it as well. First, there are multiple scan methods, but most are only available to privileged users because nmap sends and receives raw packets, it needs higher access to be able to access them. Second, just because nmap doesn’t say that a specific port on a specific IP isn’t listening, it isn’t always accurate. This is because nmap replicates ‘normal’ traffic and as such all of it’s insights are limited to what traffic is returned to it. This means that firewalls, access control lists, and intrusion detection and prevention devices can see and alter the scan traffic, but some applications are programmed to specifically give false information back to nmap when a scan packet is detected (Port Scanning Techniques | Nmap Network Scanning, n.d.). This is why performing multiple scans can provide a clearer overall picture say if a TCP SYN scan is detected and blocked for some hosts, but UDP is successful and the reverse for other hosts.

# Solution

We start off this lab by taking a look at the Internet Corporation for Assigned Names and Numbers (ICANN) website. They have a WHOIS lookup tool right on their website at https://lookup.icann.org/, they are the authoritative source because it is their responsibility to handle all IP address allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions (ICANN | Archives | ICANN - English, n.d.).

We can use their service to do a WHOIS lookup for the domain ‘zero.com’ and see that it was created in June of 1992, and is owned by Google, however, a lot of the contact information has been redacted to conform with GDPR.

Graphical user interface, text, application, email

Description automatically generated

Figure 1 - WHOIS lookup of zero.com

Graphical user interface, text, application

Description automatically generated

Figure 2 - Contact information for zero.com

Some services allow you to perform a reverse WHOIS lookup, basically the service keeps their own copy of scraped WHOIS data that they make fully searchable. Viewdns.info is a site that does this and allows you to search by Registrant. For example, if we search for all domains owned by Kevin O’Leary, we see there is a large list. Due to the sensitive nature of what is included in the WHOIS registrant and contact sections, GDPR has redacted much of the personally identifiable information, but domain privacy companies like WhoisGuard have existed for many years. Their goal was to provide protection for individuals who didn’t want all of their contact information available to the general public, however it’s been abused by many malicious people and services to hide their information so that sites and services can’t be tracked to them.

Graphical user interface, table

Description automatically generated

Figure 3 - Reverse WHOIS information for Kevin O'Leary

Next in the lab, we use a few different applications to translate domains into IP addresses, and do reverse lookups on IP addresses to see what domain they resolve to. First, we take a look at ‘nslookup’ which has been deprecated but, for the time being, is still included in most \*nix distributions. Nslookup allows you to search various DNS record types, by default it will return an A record followed by an AAAA record. We then perform a ‘nslookup’ query on the psu.edu domain and see that it resolves to three IP addresses. This is because it’s not just one sever that hosts the psu.edu website, there are several servers for redundancy and load sharing purposes. We can then do the same query with ‘dig’ which is a newer DNS querying tool that was meant to replace nslookup. Dig returns the same three IP addresses, but gives much more information with the basic default query. Dig also has a ‘-x’ flag that allows you to do a reverse IP address lookup, where you query an IP address and it will attempt to tell you what hostname resolve to it. When we run `dig -x 8.8.8.8` we see that the domain dns.google resolves to it.

Text

Description automatically generated

Figure 4 - nslookup default query type

Text

Description automatically generated

Figure 5 - nslookup of psu.edu

Text

Description automatically generated

Figure 6 - dig query of psu.edu

Text

Description automatically generated

Figure 7 - dig -x manual entry

Text

Description automatically generated

Figure 8 - dig reverse lookup of 8.8.8.8

The next task of this lab turns towards reconnaissance of internal network entities instead of external. We use the ‘nmap’ application to scan our internal network to find IP addresses where hosts are alive on the network and then identify what ports are open and what services are running. The first thing we need to do is figure out what our local IP address is, this will tell us what subnet we are on and how many available addresses there are. Running `ifconfig eth0` tells us that we are 10.1.94.98 and our subnet mask is 255.255.240.0 which converts to a /20 CIDR notation. This means that our subnet has 4096 addresses, but 4094 that are available to hosts since two are reserved for the network ID and broadcast address. Now that we know our IP and subnet/CIDR, we can run `nmap -sn 10.1.94.98/20` which does a basic scan by sending a ping to every address in the subnet and waiting for a response. From that we see that there are four hosts that are alive, including ours. You can then run a default nmap scan on each individual address, for example `nmap 10.1.85.134` does a basic scan on the first 1000 ports of that IP address and shows that port 80 is open. We can do a full port scan on the whole subnet by just removing the ‘-sn’ from the initial command, it takes a few seconds longer but returns all of the open ports on all four hosts. From that result we see two IP addresses listening on port 80. Finally, if we run `nmap -sV <ip address>` we see that 10.1.85.134 is running Apache version 2.4.25 and 10.1.82.151 is running Apache 2.4.18. This can help to enumerate what services are running on internal hosts, which makes monitoring and mitigation steps easier when bug reports come out releasing vulnerability information.

Text

Description automatically generated

Figure 9 - ifconfig to identify local IP address

Text

Description automatically generated

Figure 10 - simple nmap scan of our local subnet

Text

Description automatically generated

Figure 11 - nmap port scan of a specific IP address

Text

Description automatically generated

Figure 12 - nmap port scan of our entire local subnet

Text

Description automatically generated

Figure 13 - nmap probe of open ports to determine service/version info

# ****References****

*Data Protection and Privacy Issues—ICANN*. (n.d.). Retrieved November 12, 2021, from <https://www.icann.org/dataprotectionprivacy>

*Historical Whois Data (WhoWas)*. (n.d.). Retrieved November 12, 2021, from <https://www.arin.net/reference/research/whowas/>

*How traffic scrubbing can guard against DDoS attacks*. (n.d.). Retrieved November 12, 2021, from <https://www.computerweekly.com/news/252456702/How-traffic-scrubbing-can-guard-against-DDoS-attacks>

*ICANN | Archives | ICANN - English*. (n.d.). Retrieved November 13, 2021, from <http://archive.icann.org/tr/english.html>

*Port Scanning Techniques | Nmap Network Scanning*. (n.d.). Retrieved November 12, 2021, from <https://nmap.org/book/man-port-scanning-techniques.html>

*What is Whois Information and Why is it Valuable? | DomainTools Support*. (n.d.). DomainTools. Retrieved November 12, 2021, from <https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable>