Real World Reconnaissance

Executive Summary

The Real-World Reconnaissance paper includes the findings of passive reconnaissance on our target organization using eight different tools and techniques. The purpose of this paper is to replicate attacker's mindset and illustrate the findings which can help in carrying out an effective cyber-attack. The tools and techniques used in this reconnaissance are as follows:

- Google-fu
- Maltego community edition v4.2.9
- Spiderfoot
- Metagoofil v2.2
- Dmitry
- Netcraft
- Censys
- theHarvester v3.1.0

Let us briefly go through some of the findings. Google-fu yielded some results describing some hardware and software used in the organization like fax software, printers, load balancers and signature capture hardware. Using Maltego, different hosting providers in an organization along with their netblocks and their location could be identified. Spiderfoot's scan comprised of some interesting results which included over 75 compromised passwords and over 350 compromised hashes. Metadata like applications, usernames and email addresses were found using Metagoofil. Dmitry and Netcraft provided us with some footprint of nameservers and analysis of web servers. With the help of Censys, we could find some of vulnerable nginx servers running in the organization. Finally, theHarvester provided us with names and job descriptions of employees using social media analysis.

All the findings are not documented in this report as it would become inordinately long.

Introduction

I chose this organization as it is a medium size healthcare company. Healthcare industry is a prime target for many cybercriminals. Many hospitals in California, Maryland, Kentucky and Indiana have faced brutal Ransomware attacks. Healthcare industry is a perfect target due to the lucrative data they possess. Also, they have a high affinity towards using out-of-date legacy systems. As with any cyberattack, launching ransomware attacks requires the attacker to perform a detailed reconnaissance of the target. This assignment can help replicate that **attacker mindset** and perform a passive reconnaissance of our target.

Passive Reconnaissance

Conducting a reconnaissance before an attack is one of the best practices to ensure the effectiveness of an attack. This involves probing the target using publicly available information. There can be two types of reconnaissance: active and passive. Active reconnaissance is more direct way for engaging with the target to get the required information. In contrast, passive reconnaissance is a more benign attempt to gather information without raising suspicions or triggering alarms. In this assignment, we will be performing a passive reconnaissance of our target and gather as much useful data as possible using eight different tools and techniques.

Tools & Techniques Used

The tools and techniques used in this assignment are as follows:

1. Google-fu

With the help of Google and Yandex search engines, I could find some of the data on my target. Information about their business partners could be found. This information could really be useful in a social engineering attack. Apart from partners, the following information about their hardware could also be found on the company's website.

FAX software - [redacted]

Load balancers – [redacted]

Printers - [redacted]

Signature Capture Hardware - [redacted]

From this information, attacker can get a basic sense of hardware and software running in an organization. If there are any vulnerabilities in the software, the attacker can leverage this data to compromise them.

Suggested Controls: This information about partners, hardware or software could be valuable to attackers. Hence policies should be implemented, restricting any such revealing data on the company's web servers.

2. Maltego

I have used Maltego community edition version 4.2.9 in the assignment. Maltego is one of the best open source intelligent tool (OSINT) out in the market. Maltego not only gathers useful information but also interprets it in a visually pleasing way so that user can understand the different relationships. Maltego works by using different modules known as transforms. A transform is a small snippet of code which can be installed and run immediately. There are over 30 public sources to gather data from. Although, some of them needs to be purchased separately, most of them are freeware. Some of the transforms require API key to function properly. Some

of the popular hub items include Shodan, Have I been Pawned? And Farsight DNSDB. Maltego helps to determine relationships between different entities like People, Organizations, and Infrastructures (DNS, domains, netblocks.) etc.

Running a scan is easy - Open Maltego and start with a new graph by pressing ‘Ctrl + t’. Once a new graph opens, one choose one or more entities from the Entity Palette. After choosing an entity and renaming it to the desired target, right click on your entity to run all transformations or choose individual transformations. There are different types of views which can be selected for a clear visual representation.

Using Maltego I have made the following interpretations on my target:

Hosting Provider	IPv4 Address	Netblock	Location
Amazon AWS	[redacted]	[redacted]	[redacted]
Cloudflare Inc	[redacted]	[redacted]	[redacted]
Rackspace (Mail Server)	[redacted]	[redacted]	[redacted]
Oracle Co.(parent)- Dynamic network services (Name Server)	[redacted]	[redacted]	[redacted]
Visitor Management System - ProxyClick	[redacted]	[redacted]	[redacted]
Proxy server	[redacted]	[redacted]	[redacted]
Hosting.com	[redacted]	[redacted]	[redacted]

From the above information attackers can infer that the different hosting providers in an organization along with their **netblocks** and their location. Attackers can use this intel to target specific service, compromise them and work their way into our target organization.

3. Spiderfoot

Spiderfoot is another popular tool for passive reconnaissance. It comprehensively gathers data from over 100 public data sources. These sources can include DNS information, WHois databases, metadata, threat intelligence etc. The data which may be included in the scan ranges from Domain names, Blacklisted IP Addresses, Compromised hashes, Compromised Passwords, DNS SPF, SRV and TXT Records, Hacked Email Addresses, Malicious IP Addresses and much more. Spiderfoot is highly favored to other tools due to the complete automation it provides. It also gives us the independence of going through the scan module by module. Spiderfoot can also be configured to run automatic scans on a weekly or monthly basis. It provides with over 200 useful modules with an easy to use web UI.

To begin scanning in Web UI mode, we need to first assign an IP and port. This can be done by issuing “python3 sf.py -l IP:port”. Once it starts listening we can go to any browser of our choice and start performing the scan. We can also run the scan from CLI mode. The target can be

specified using the -s option. The modules can be enabled by using the -m option. The modules can be listed by -M option. For proper functioning of the Spiderfoot modules, they need an API key. We can get this key by visiting the respective site, signing up and entering it in the Spiderfoot UI. Spiderfoot has also given us the liberty of creating our own modules. A scan by be run in one of the 3 forms: By Use Case, By Required Data or By Module.

To be as stealthy and passive as possible my scan against our target, we are running the scan by use case and in passive mode. The following data could be found by running a scan against our target domain. What makes it interesting is we have found some Email Addresses, Compromised Hashes and Passwords !

Breach Data from Scylla API

There are over **75 usernames and passwords** found from the Spiderfoot scan. Some of them are listed below:

username:password	**username:password**
Ja[illegible]s1	de[illegible]l
ab[illegible]are	de[illegible]P34
an[illegible]oeboo	dh[illegible]na
an[illegible]85	di[illegible]
an[illegible]u$12	di[illegible]
ap[illegible]a	dic[illegible]09
as[illegible]al	eri[illegible]ley
as[illegible]12	ga[illegible]
ba[illegible]l81	ha[illegible]23
br[illegible]iya1	he[illegible]
br[illegible]rd69	jan[illegible]29
de[illegible]ins	jas[illegible]e
br[illegible]rd	jer[illegible]000
ca[illegible]e2	jul[illegible]ns1
ca[illegible]ss	la[illegible]in]
ch[illegible]an3	lis[illegible]
ch[illegible]ans	ma[illegible]771
ch[illegible]e01	ma[illegible]
as[illegible]12	mi[illegible]lea
ch[illegible]b78	na[illegible]23
sa[illegible]n85	so[illegible]5
sa[illegible]iji	ste[illegible]pton
su[illegible]500	su[illegible]11
su[illegible]ine	su[illegible]67
sa[illegible]hmd	su[illegible]happy

There are **over 300 unique compromised password hashes** found. Some of them are listed below:

Ja	30bb62b
aa aF	1PuGV4V7tLVRS.la8J2gF3
ab	e945cf0
ab	63e2bd9
ad	919
ad	59c150e
ak	0a4caa4b8
al	85a

The leaked password dump includes hundreds of passwords and hashes. If an attacker manages to access even one of those accounts, the results would be catastrophic. This is because different users can have different kind of privileges. If the attacker is lucky to find an account with elevated privileges, he/she can do some serious damage to the organization. Passwords can also be obtained from the hashes found. The passwords found can be used for **Credential Stuffing**, **Password Spraying,** and other attacks. The hashes found can be taken offline and **cracked** or used in other attacks like **pass the hash**.

Suggested Controls: Strong password policies should be implemented in an organization. Implementing 2FA becomes essential in these scenarios where it is the only thing guarding the organization from the attackers.

4. Metagoofil

Metagoofil is one of powerful OSINT tools for intelligence gathering. This tool helps in gathering and extracting the metadata of publicly available documents. A wide variety of documents are supported like pdf, ppt, doc, xls etc. It is also really easy to use the tool .Although this tool is not shipped directly with kali Linux, it is easy to install it by issuing the apt -get install command. The tool works by searching the required documents regarding a particular domain using google and downloads them. Then it can use its specialized libraries like pdf miner to generate a report with all the metadata.

The following data could be found on our target:

Applications along with their version:

Mi	r Version 9.3.0.1233
Mi	10.01
Ac	S6 (Macintosh)
PS	y 9.9
Mi	C 14.0 (Macintosh)
Mi	S5.5 (7.5.3)
Ad	C 2014 (Macintosh)
Ad	y 11.0
Ac	)
Ad	C 2017 (Macintosh)
Ad	0.1.5 (Windows)

Company related **usernames** and **email addresses** are also found:

Je	
Ja	
Ja	
Lo	.com
Ja	om
Gr	com
M	
Ka	
Be	
Ha	com.
Be	.com.

The findings include different applications (along with their version numbers) along with some company related email addresses and usernames. This intel could equip attackers with some really good arsenal for conducting **social engineering** attacks.

Suggested controls: These kinds of data leaks are inevitable. We need to raise awareness and educate employees to not to reveal sensitive information to someone over the phone. Security awareness programs should be conducted regularly to train employees about the different kinds of social engineering attacks.

5. Dmitry

Deepmagic Information Gathering Tool is an OSINT tool that gives analysis about a host. This tool can perform a whois lookup on both IP address and domain name of the host. This tool also has an option of performing a tcp port scan on the host. Since, we are performing only a passive reconnaissance we will not be using this option . This tool comes installed with Kali Linux. The usage of this tool is also very clear and concise. A simple scan can be run by issuing “dmitry [-options] [hostname]” command. The information found from this tool is as follows:

Hostname:

Host IP:

Nameservers	
a1	t
a1	t
a1	t
a2	t
a2	t
a5	
ns	net
ns	net
ns	net
ns	net

Hostname	Hostname IP
w	4
m	30
bl	80
he	
m	36
sp	45

DNSSEC: unsigned

The information found via using this tool is regarding the **nameservers** from our target domain. Few subdomains along with hostnames could also be found. An important finding is **DNSSEC** is not assigned. This could be valuable to attackers as they now learn **DNS spoofing/poisoning** could be possible on their targets.

Suggested controls: DNSSEC should be implemented by the target organization to provide authentication and integrity protection.

6. Netcraft

Netcraft is another OSINT tool used for a websites deep information gathering. This tool works similar to that of Dmitry. This tool should also be used along with Dmitry for gathering complete information against a target website. Netcraft basically provides analysis on web server and web hosting provider. The usage of this tool is easiest amongst all the tools. It simply involves visiting netcraft site and entering the target domain. The following information could be gathered from this tool:

Domain	[illegible]
Domain IP Address	[illegible]
Nameserver	[illegible]
Hosting OS	[illegible]
Web server – year 2020	[illegible]
Web server – year 2017	[illegible]
Server-side Technology	[illegible]
Client-side Technology	[illegible]
Client-Side Scripting Frameworks	[illegible]
Server-side Scripting	[illegible]
Blog software	[illegible]
Content Management System	[illegible]
Web feed formats	[illegible]
Web analytics	[illegible]
Character Encoding	[illegible]

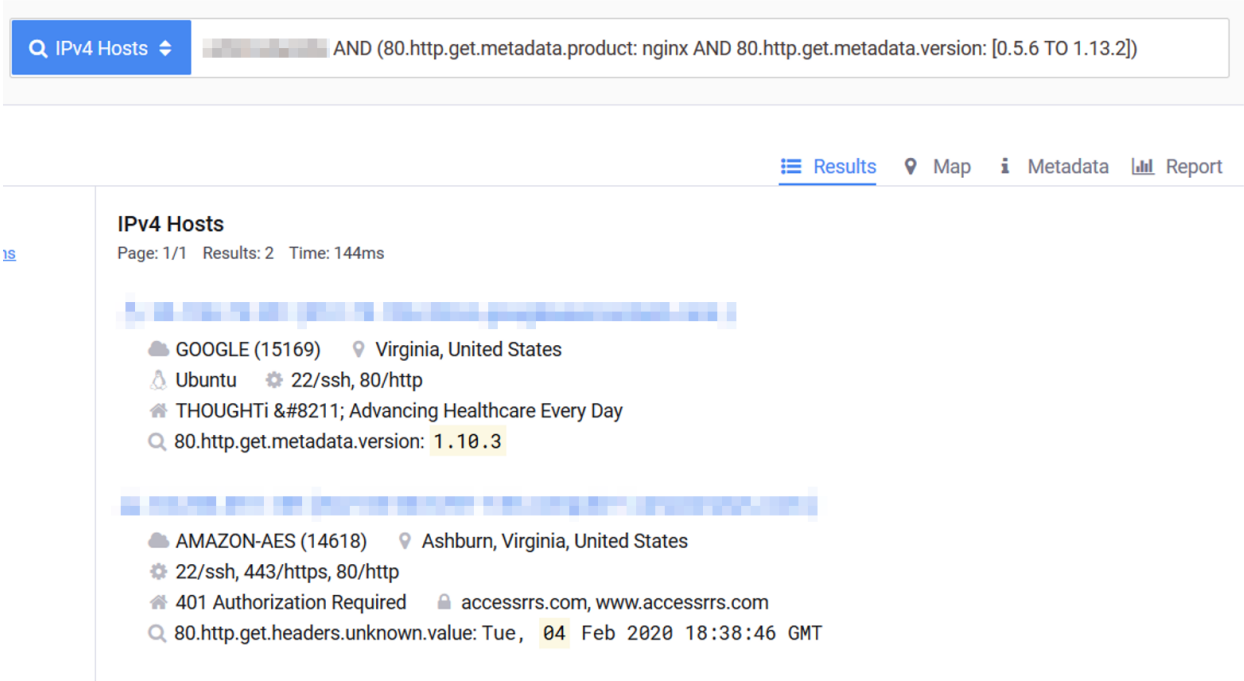
DNS Admin:
Admin Name: [illegible]
Admin Phone: [illegible]
Admin Email: [illegible]

The above information will provide attackers a lot of valuable information about the site. An interesting finding is that the webserver's software in the year 2017 was visible. But, since 2019 the webserver software has been hidden.. It can be noted that DNS Admin's details are visible to public which could be helpful in a social engineering attack.

Suggested controls: Similar to webserver software details, other information should be limited by the company. The DNS admins details should also be hidden.

7. Censys

Censys is a search engine but for internet facing devices. Using Censys, vulnerable devices and networks can be found easily on the internet. Censys maintains a database full of exposed vulnerable devices and by using the right search directives we can gather useful information during the reconnaissance phase. The following information could be found:



Nginx servers running with **vulnerable** versions **(CVE-2017-7529**) are found on our target. These servers are vulnerable to integer overflow and lead to potential leak of sensitive information.

Suggested Controls: Servers need to be upgraded to version which are free of this vulnerability.

8. theHarvester

The final tool we are working with is called theHarvester. This tool helps in gathering of **subdomains, email addresses , employee names etc.** from a variety of search engines and sources like google, yahoo, twitter, LinkedIn etc. The following information could be found on my target:

Name	Job Role	Organization
[illegible]	Network Engineer	[illegible]
[illegible]	Site Director	[illegible]
[illegible]	Sr. Sales Executive	[illegible]
[illegible]	Product Specialist	[illegible]
[illegible]	Software Trainer	[illegible]
[illegible]	Project Manager	[illegible]
[illegible]	Business Intelligence	[illegible]
[illegible]	Social Media Specialist	[illegible]
[illegible]	Revenue Analyst	[illegible]
[illegible]	Team Lead	[illegible]
[illegible]	Sr. Enterprise Architect	[illegible]
[illegible]	Sales And Service Consultant SMB	[illegible]
[illegible]	Clinical Risk Analyst	[illegible]
[illegible]		[illegible]
[illegible]	Human Resources	[illegible]
[illegible]	Product Manager	[illegible]
[illegible]	Product Management	[illegible]
[illegible]	Account Manager	[illegible]
[illegible]	Product Manager	[illegible]
[illegible]	Product Analyst	[illegible]
[illegible]	Product Analyst	[illegible]
[illegible]	Software Training Specialist	[illegible]
[illegible]	Software Engineer	[illegible]
[illegible]	Post Sales Coordinator	[illegible]
[illegible]	Human Resources	[illegible]
[illegible]	Product Manager	[illegible]
[illegible]	Sales Coordinator	[illegible]
[illegible]	Independent Distributor	[illegible]
[illegible]	Human Resources	[illegible]
[illegible]	Training Admin	[illegible]
[illegible]	Product Manager	[illegible]
[illegible]	Sales	[illegible]
[illegible]	CSC	[illegible]
[illegible]	CFO	[illegible]
[illegible]	Sales Coordinator	[illegible]
[illegible]	Executive Assistant	[illegible]
[illegible]	Sales Coordinator	[illegible]
[illegible]	Director	[illegible]
[illegible]	Payroll Manager	[illegible]
[illegible]	Team Lead	[illegible]
[illegible]	CEO	[illegible]
[illegible]	Payroll Specialist	[illegible]
[illegible]	Project Manager	[illegible]

The above information could really be useful to an attacker for conducting a social engineering attack.

Suggested Controls: Security awareness programs should be conducted regularly to train employees about the different kinds of social engineering attacks.

Works Cited:

Skoudis, Ed, and Tom Liston. *Counter Hack Reloaded: a Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall, 2011.

Blogs, Hacking, et al. "What Is Netcraft and Dmitry Tool? Information Gathering." *Hacking Blogs | Become an Ethical Hacker*, 12 Oct. 2019, hackingblogs.com/netcraft-dmitry-tool-information-gathering/.

"Best Practices." *Support :* docs.maltego.com/support/solutions/articles/15000019250-best-practices.

"OSINT Automation." *SpiderFoot*, www.spiderfoot.net/documentation/.

"TheHarvester." *Penetration Testing Tools*, tools.kali.org/information-gathering/theharvester.

"What's That Site Running?" *Netcraft*, sitereport.netcraft.com/.