OSINT Report by Jack Yorgason

# Abstract

Throughout the information gathering process, Maltego was used by running transforms on different entities within the Tintictech organization. This provided a graphical interface with a layout of the organization’s infrastructure. Dig was a tool used to gather more information pertaining to the domains DNS query. Through this tool, more information on the DNS and Mail server’s addresses were uncovered. The next tool used was DNSENUM, which disclosed host names, server names, and other services. The Harvester was then used to brute force a long list of common DNS names to test the provided domain for any subdomains.

Table of Contents

[Abstract 1](#_Toc173850945)

[List of Figures 3](#_Toc173850946)

[1 Introduction 4](#_Toc173850947)

[2 Kali VM 4](#_Toc173850948)

[3 Maltego 4](#_Toc173850949)

[4 Dig 7](#_Toc173850950)

[5 DNSENUM 8](#_Toc173850951)

[6 theHarvester 10](#_Toc173850952)

[7 Methodology 12](#_Toc173850953)

[8 Conclusions and recommendations 12](#_Toc173850954)

[9 References 12](#_Toc173850955)

# List of Figures

[Figure 1, Kali VM 5](#_Toc167047513)

[Figure 2, Maltego Transform 6](#_Toc167047514)

[Figure 3, Tintictech Addresses 6](#_Toc167047515)

[Figure 4, DNS Shodan Transform 7](#_Toc167047516)

[Figure 5, DNS Table 7](#_Toc167047517)

[Figure 6, Shodan Tags 8](#_Toc167047518)

[Figure 7, Dig Output 8](#_Toc167047519)

[Figure 8, Dig Mail Server Output 9](#_Toc167047520)

[Figure 9, DNSENUM Server Output 10](#_Toc167047521)

[Figure 10, DNSENUM PHP 11](#_Toc167047522)

[Figure 11, Whois Query 11](#_Toc167047523)

[Figure 12, theHarvester 13](#_Toc167047524)

# 1 Introduction

This report was developed using different passive reconnaissance tools such as Maltego, Dig, DNSENUM, and the Harvester. The purpose of using passive reconnaissance is to gather open-source information specific to our target. The tools used are a form of Open-Source Intelligence (OSINT) which allows me to access underlying information, without being detected. Performing these tasks provided me with crucial information, that I can then use to exploit in further phases of this penetration test.

# 2 Kali VM

A screenshot of a computer

Description automatically generated

Figure 1, Kali VM

# 3 Maltego

Using Maltego, we can search multiple open-source intelligence feeds for information on a target. The information is then displayed on an interactive graphical interface. Running a Transform on Tintictech’s website, we receive a variety of different outputs, such as IP addresses, a DNS Server, and different social media accounts related to Tintictech.

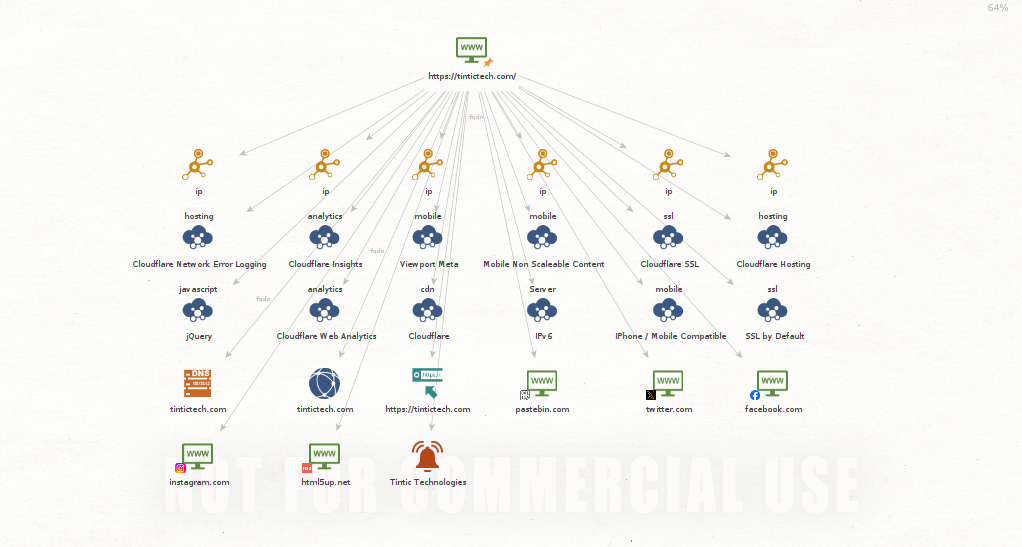


Figure 2, Maltego Transform

One rather interesting output is from Pastebin.com, which is used as an online service where users can store plain text, such as source code snippet. The link provided by Maltego takes us to a page that has a list of accounts with tintictech.com domains. If these email addresses are part of the organization, then we could use these in future tests such as phishing campaigns.

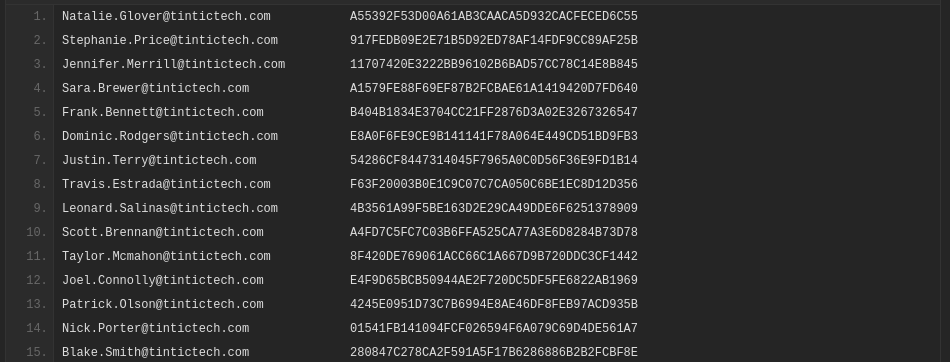


Figure 3, Tintictech Addresses

Now that we know tintictech.com is a valid DNS Server, we can dig a little deeper by running the Shodan transform on that server. We can now see a variety of subdomains/servers along with some underlying configurations (e.g., dmarc, spf, google-verified). We can also see an IP address which we can further investigate. Knowing these subdomains/servers can lead to different web-based attacks, and knowing these configurations can lead to specific evading techniques.

A diagram of a computer

Description automatically generated

Figure 4, DNS Shodan Transform

A screenshot of a computer

Description automatically generated

Figure 5, DNS Table



Figure 6, Shodan Tags

# 4 Dig

Dig is used as a command line tool, to query DNS. In this example, I ran Dig against the known tintictech.com DNS server. In the output, we can see that the output includes details like the queried server, time to live (TTL), record type, and associated IP address.

A computer screen shot of a computer

Description automatically generated

Figure 7, Dig Output

Dig can also be used to query mail servers, using the “mx” switch. In the output, we can see that Tintictech is using an Outlook mail server. This can be useful to a threat actor as they now know the targets mail server and its address.

A computer screen shot of white text

Description automatically generated

Figure 8, Dig Mail Server Output

# 5 DNSENUM

This tool will run different queries against a domain. I used the “-v” switch for verbose, “-r” for recursion on subdomains, and “-w” to perform whois. It first displays the host addresses, name servers, and mail servers.

A screenshot of a computer

Description automatically generated

Figure 9, DNSENUM Server Output

We then find something interesting when searching through the output. There is a php.myadmin.tintech.com server, indicating that php is in use. This could be a future point of entry if a php exploit is available or created.

A screen shot of a computer

Description automatically generated

Figure 10, DNSENUM PHP

The whois query responds with two IP addresses and their subnets. We can use this information to further investigate these addresses and find possible vulnerabilities.

A screenshot of a computer

Description automatically generated

Figure 11, Whois Query

# 6 theHarvester

Using theHarvester, a DNS brute force against 4989 words was ran. This will provide a list of possible DNS servers. In this output, we can see the response did not find any IP’s, email addresses, or hosts, but it did find a list of possible DNS services. I can use these findings to test for any open webpages or possible vulnerabilities.

A screenshot of a computer

Description automatically generated

Figure 12, theHarvester

# 7 Methodology

This report focuses on passive reconnaissance methodologies. Throughout these tests, the focus was on gathering as much information as possible without leaving a digital footprint. Using a variety of OSINT tools, information can be gathered and reviewed, to then use in future phases of a penetration test.

# 8 Conclusions and recommendations

When considering that this information was all found using OSINT tools, there are a variety of techniques that can be used to redact information or minimize the company’s digital footprint. It is best practice to routinely perform information gathering tests to see what information is readily available to adversaries. However, there are certain systems that cannot be hidden from the public. Implementing secure protocols on outward facing servers can be beneficial in evading adversaries and protecting crucial systems.

# 9 References

DNSENUM. (n.d.). DNSENUM [Software]. Retrieved May 20, 2024, from https://github.com/fwaeytens/dnsenum/

Edge, M. (2024). theHarvester: Open-source intelligence tool [Software]. GitHub. <https://github.com/laramies/theHarvester>

Internet Systems Consortium. (n.d.). Dig (DNS tool). Retrieved May 20, 2024, from https://www.isc.org/dig/

Paterva. (2024). Maltego [Software]. Paterva. https://www.paterva.com