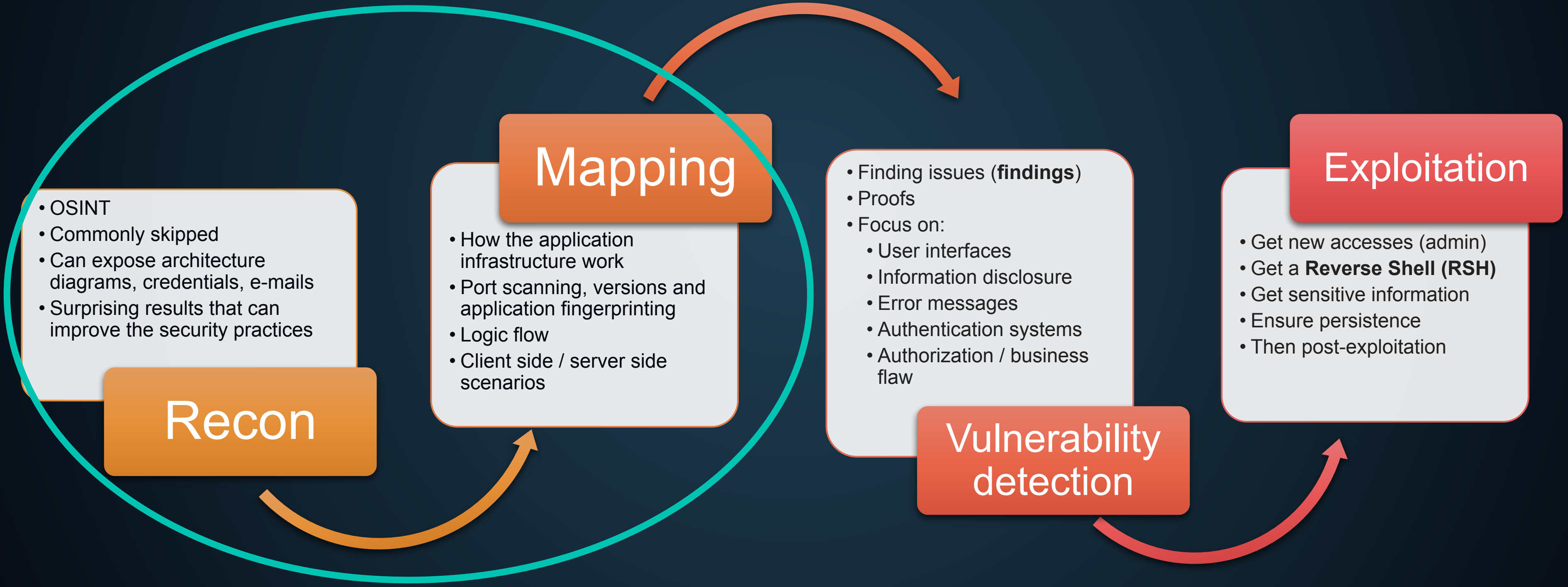
RT0706 – Web Security Reconnaissance and Mapping

Penetration Test Methodology



Recon

- OSINT
- Commonly skipped
- Can expose architecture diagrams, credentials, e-mails
- Surprising results that can improve the security practices

Mapping

- How the application infrastructure work
- Port scanning, versions and application fingerprinting
- Logic flow
- Client side / server side scenarios

Vulnerability detection

- Finding issues (**findings**)
- Proofs
- Focus on:
  - User interfaces
  - Information disclosure
  - Error messages
  - Authentication systems
  - Authorization / business flaw

Exploitation

- Get new accesses (admin)
- Get a **Reverse Shell (RSH)**
- Get sensitive information
- Ensure persistence
- Then post-exploitation

Table of Contents

1

Reconnaissance

How to make reconnaissance ?

2

Mapping

How to map web assets ?

3

Proxy

How to use a web proxy?

1

Reconnaissance

How to make reconnaissance?

Reconnaissance

First step in our methodology

- Can be time saving or time wasting
- Often skipped and done if the consultant feels that it is necessary during the vulnerability detection phase

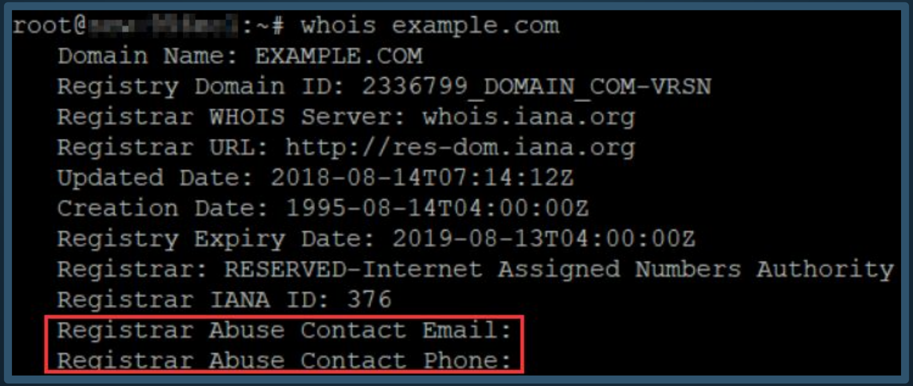
It gives knowledge on the target

- Data for valid inputs
  - E-mail addresses
  - Phone numbers
  - Names of employees
- Network / application / software / framework / infrastructure / processes knowledge

WHOIS service

WHOIS

- It is a directory service
- You can collect the registrar / emails / phone numbers / domains related to the target
- It is a good way to know the different providers of the target

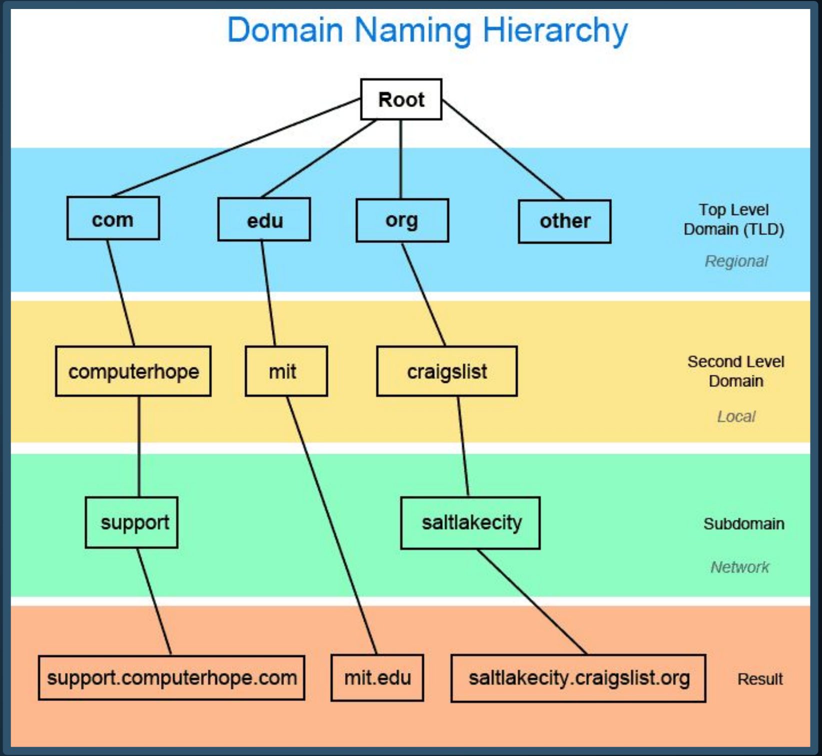


```
root@[redacted]:~# whois example.com
   Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2018-08-14T07:14:12Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2019-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
```

Domain Name Service

DNS

- Internet's phonebook
- Each domain name has one or more IPs
- The DNS server maps domain to IP



Domain Naming Hierarchy

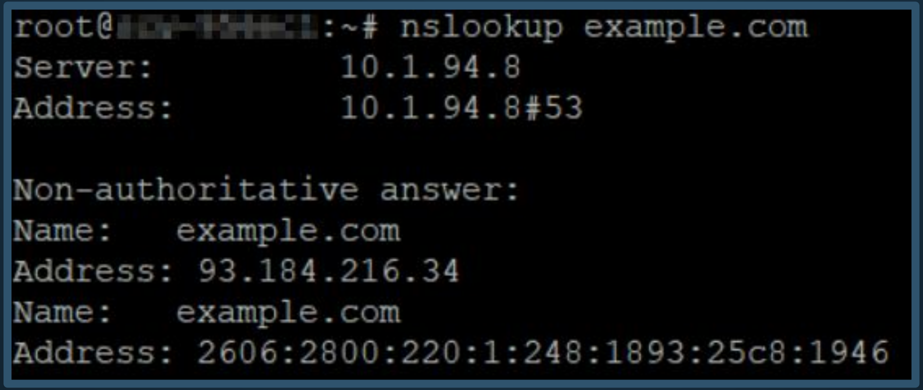
Types of DNS record

Type	Description	Function
A	Address record	Link the domain or subdomain to an IPv4 address
NS	Name Server record	Delegates a DNS zone to use the given authoritative name servers
MX	Mail Exchange record	Directs email to servers for a domain with the order priority
CNAME	Text record	Used for SPF, domain key...
SOA	Start of authoritative record	Specifies authoritative information about a DNS zone

DNS query

Nslookup

- It gives the mapping between domain name and IP address or other DNS records
- Preferred on Windows
- Deprecated on Linux (use dig instead)



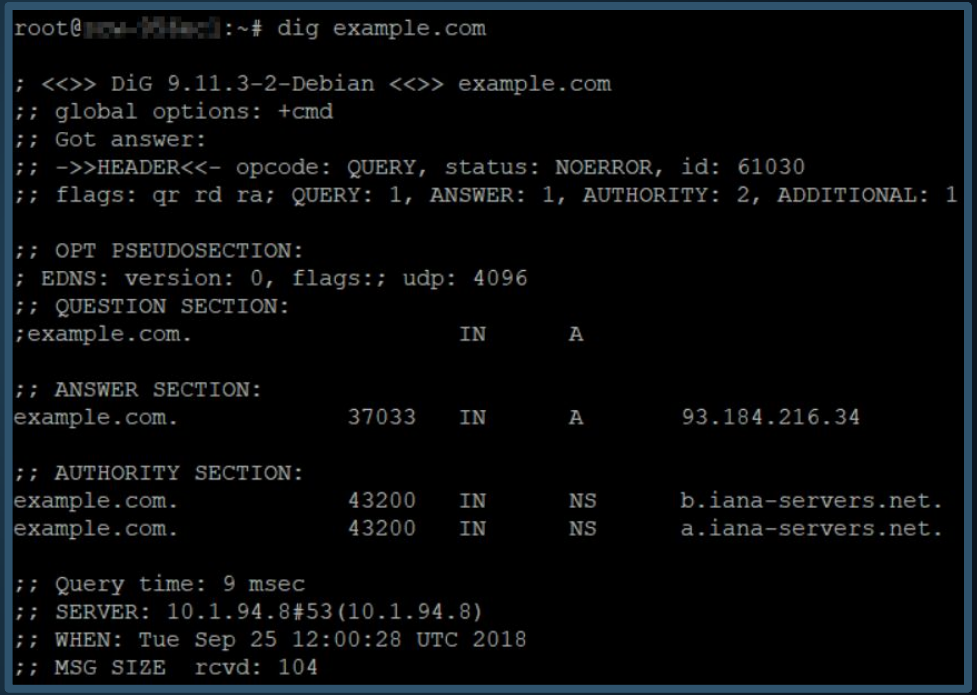
```
root@[redacted]:~# nslookup example.com
Server:         10.1.94.8
Address:        10.1.94.8#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
Name:   example.com
Address: 2606:2800:220:1:248:1893:25c8:1946
```

DNS query

Dig

- Can search specifics records
    - MX for mail servers
    - AXFR for zone transfer
    - ANY for any records



```
root@[redacted]:~# dig example.com

; <<>> DiG 9.11.3-2-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61030
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            37033   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.com.            43200   IN      NS      b.iana-servers.net.
example.com.            43200   IN      NS      a.iana-servers.net.

;; Query time: 9 msec
;; SERVER: 10.1.94.8#53(10.1.94.8)
;; WHEN: Tue Sep 25 12:00:28 UTC 2018
;; MSG SIZE  rcvd: 104
```

DNS zone

A DNS zone is a subset of the DNS tree

- It is delegated for administration purposes

Zone transfer

- DNS zone transfer is the process where a DNS server passes a copy of it's database (which is called a "zone") to another DNS server
- You just pretend to be a slave and ask the master for a copy of the zone records

```
dig axfr <IP> @<DNS_SERVER_IP>
```

Domain Names Reconnaissance

DNSrecon

- It performs DNS enumeration on a domain
    - Python script that collects standard records and attempts zone transfer
    - Default dictionary: /usr/share/wordlists/dnsmap.txt

```
dnsrecon -d <DOMAIN> -t std -D <WORDLIST>
```

Subdomain brute-forcer

- https://github.com/aboul3la/Sublist3r

```
python sublist3r.py -d <DOMAIN> -b
```

DNS Reconnaissance

Open Source Intelligence

OSINT

- Public data and information that can be collected legally
- It can be performed without interacting with the targeted infrastructure
- It is essential for an external penetration test
- Not always used for a web pentest depending on the scope
- The information gathered can be sensitive
    - Many pointless data or information can lead to sensitive data, information or intelligence

Google Search Engine

Google dorks

- It supports various search directives and operators
- It limits drastically search results and can provide quick-wins

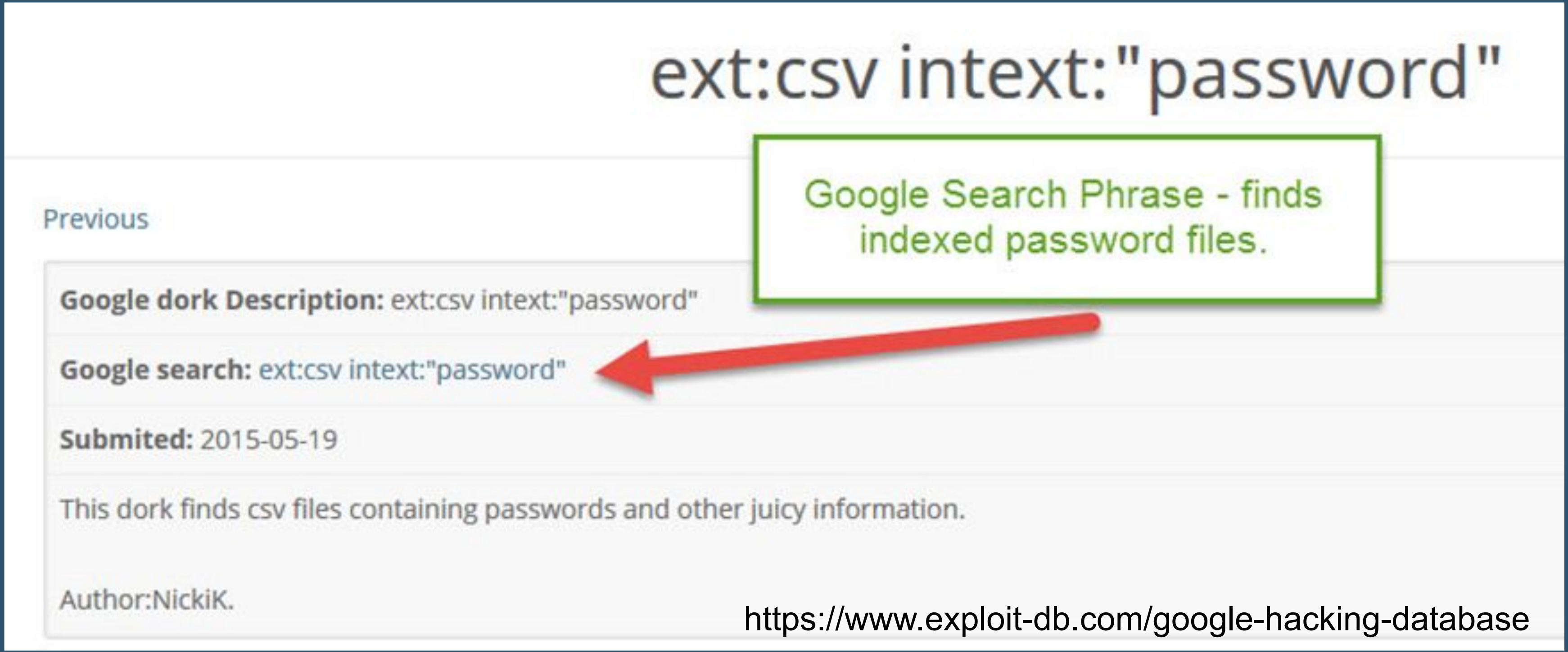
Directives

- site:example.fr
- Inurl:phpinfo / intitle:”Admin page”
- Ext:xslx / filetype:pdf

Operators

- OR AND “” * - +

Google Dorking



ext:csv intext:"password"

Google Search Phrase - finds indexed password files.

Previous

Google dork Description: ext:csv intext:"password"

Google search: ext:csv intext:"password"

Submited: 2015-05-19

This dork finds csv files containing passwords and other juicy information.

Author:NickiK.

https://www.exploit-db.com/google-hacking-database

Social Networks

A lot of information are disclosed on social networks

Many social networks allow the search based on company name

- Dictionary creation for password guessing
- Answers for password reset
- Photos at work
- Valid email addresses and pattern

Shodan

Web crawler scanning the Internet and index results in a knowledge base

- Port scanner / banner gathering / default pages and password testing

Very limited use without an account

Free account specifications:

- Search based on domain / IP / technology and version
- Basic operation on country / hostname / Net / Os / Port

Attacker point of view

- Domains and subdomains linked to the targets
- Open ports / services hosted / technologies used...

Information Gathering on a Domain

theHarverster

- Python script that gathers information on a targeted domain
    - Email addresses
    - IP addresses
    - Domain names

It is based on search engines, PGP keys, Shodan...

```
theHarvester -d <DOMAIN> -l 300 -b all -f output
```

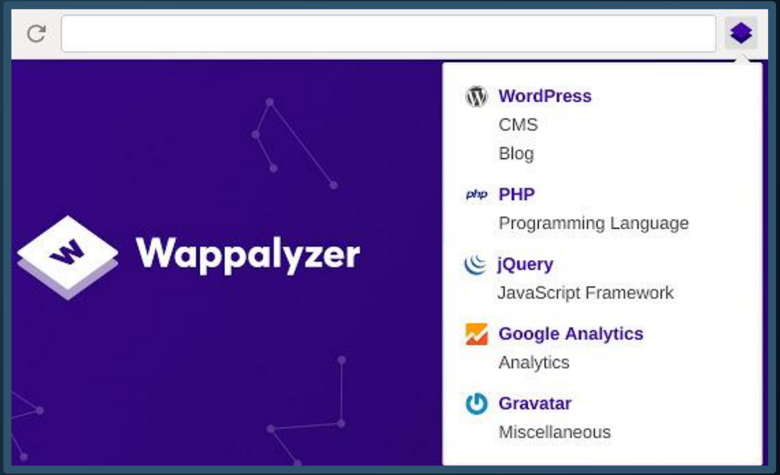
Technology Gathering

Wappalyzer is a plugin for Firefox and Chrome

- Python

It allows retrieving the technologies with versions

- Ecommerce platforms
- Web frameworks
- Server software
- Analytics tools

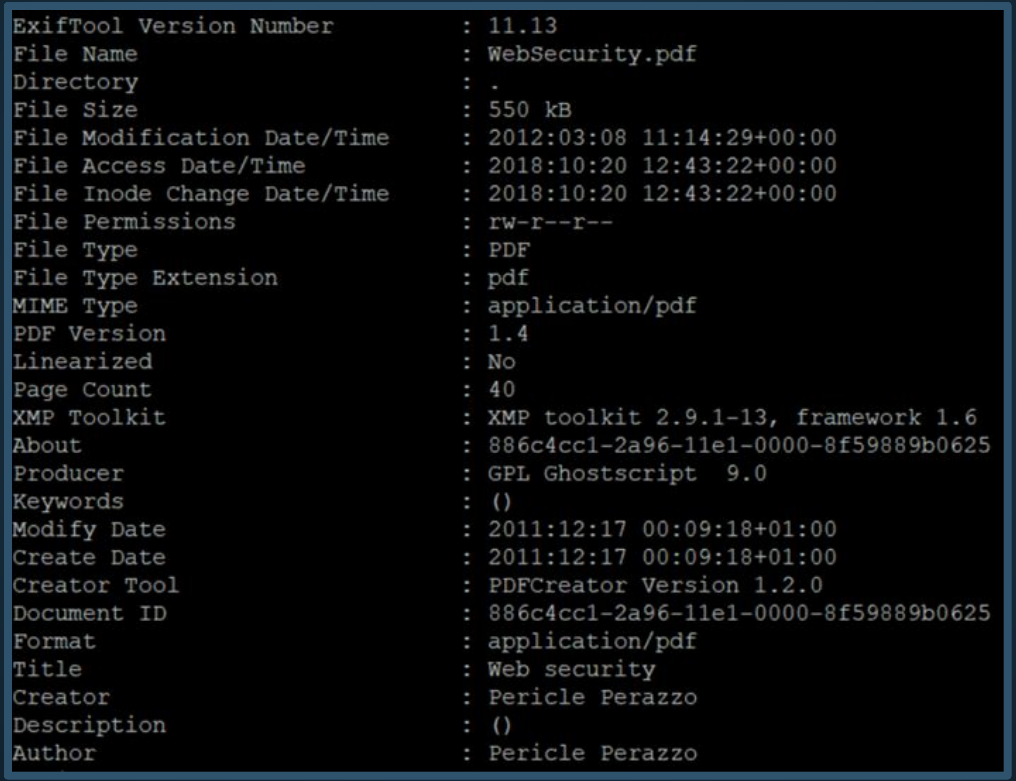


Files Metadata

Exiftool is a command line tool in Perl to manipulate meta information in files

- Platform-independent that is very powerful and fast
- Read / Write / Editing meta information
- Useful to retrieve information from public files
  - Internal OS and software version
  - Names and emails
  - ...

Exiftool



```
ExifTool Version Number         : 11.13
File Name                       : WebSecurity.pdf
Directory                       : .
File Size                       : 550 kB
File Modification Date/Time     : 2012:03:08 11:14:29+00:00
File Access Date/Time           : 2018:10:20 12:43:22+00:00
File Inode Change Date/Time     : 2018:10:20 12:43:22+00:00
File Permissions                : rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 40
XMP Toolkit                     : XMP toolkit 2.9.1-13, framework 1.6
About                           : 886c4cc1-2a96-11e1-0000-8f59889b0625
Producer                        : GPL Ghostscript  9.0
Keywords                        : ()
Modify Date                     : 2011:12:17 00:09:18+01:00
Create Date                     : 2011:12:17 00:09:18+01:00
Creator Tool                    : PDFCreator Version 1.2.0
Document ID                     : 886c4cc1-2a96-11e1-0000-8f59889b0625
Format                          : application/pdf
Title                           : Web security
Creator                         : Pericle Perazzo
Description                     : ()
Author                          : Pericle Perazzo
```

OSINT

2

Mapping

How to map web assets?

Mapping

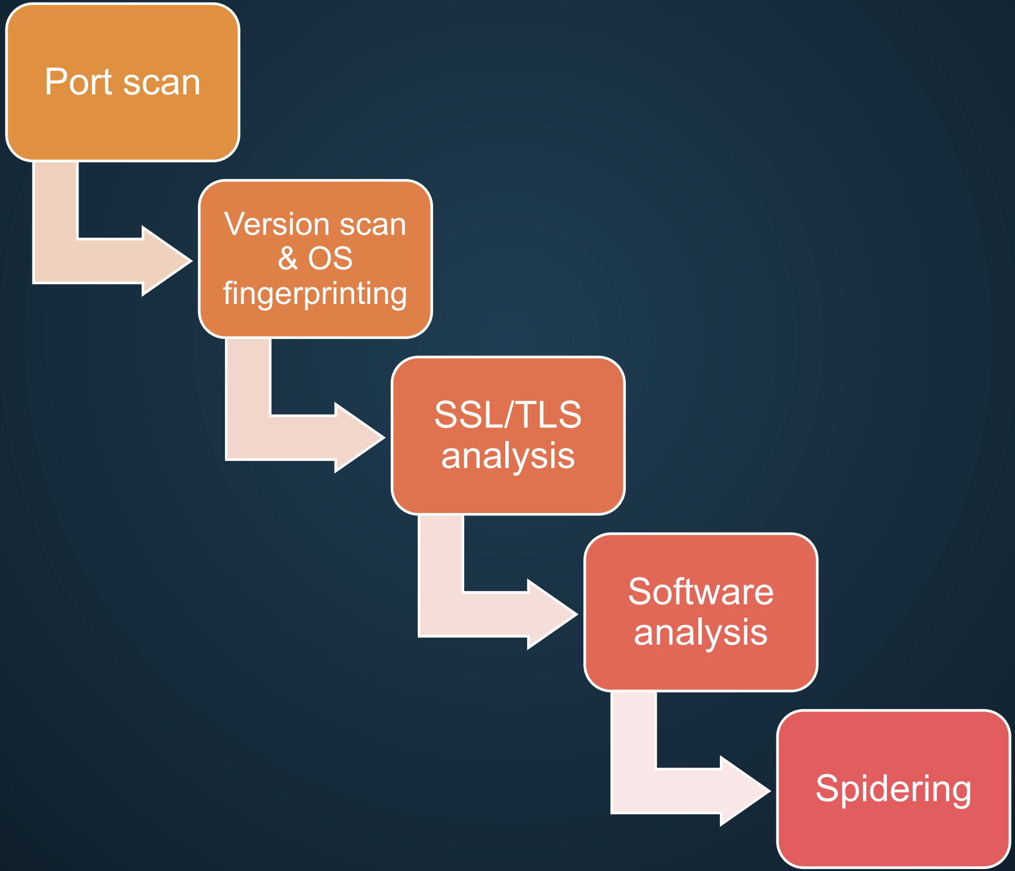
Mapping is an essential phase

- First findings and quick-wins
- It gives the foundations to start the next phase

This is a semi-automatic phase

- Check manually the application while the scans are running
- Cross-check the information from the scans manually
- The goal is to understand how the application works

Mapping Phases



Port scan

Version scan & OS fingerprinting

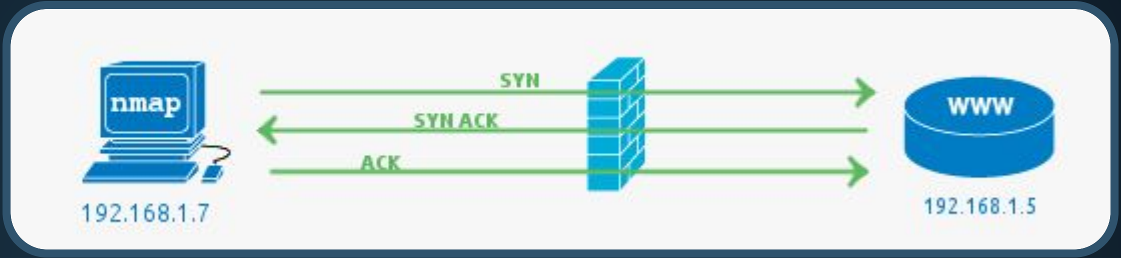
SSL/TLS analysis

Software analysis

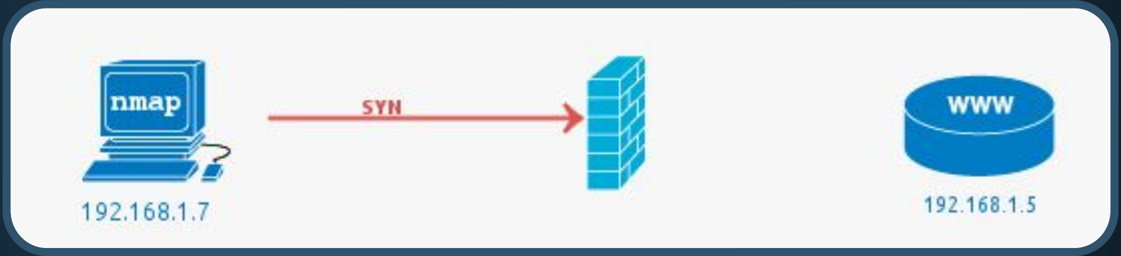
Spidering

Port Scanning

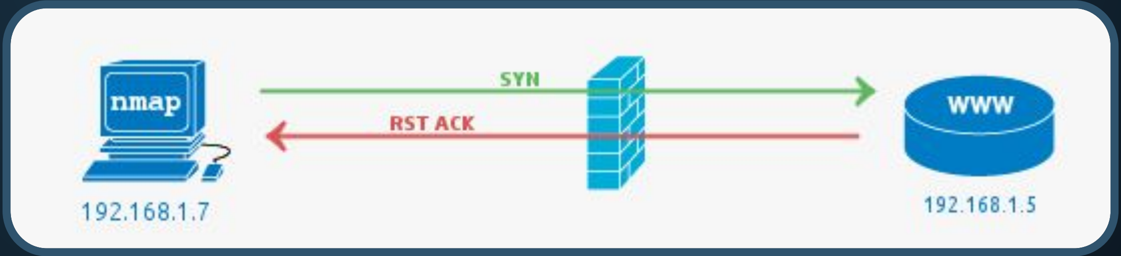
OPEN



FILTERED



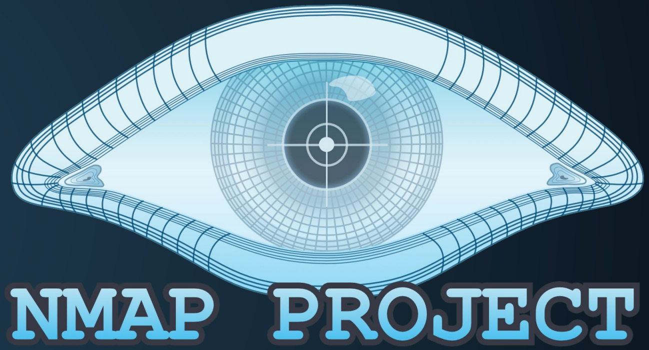
CLOSED



Network Mapper

Nmap

- Free and open source
- Network / host / service / port discovery
- OS and software version detection
- Basic vulnerability scanner via scripts (NSE)



Nmap

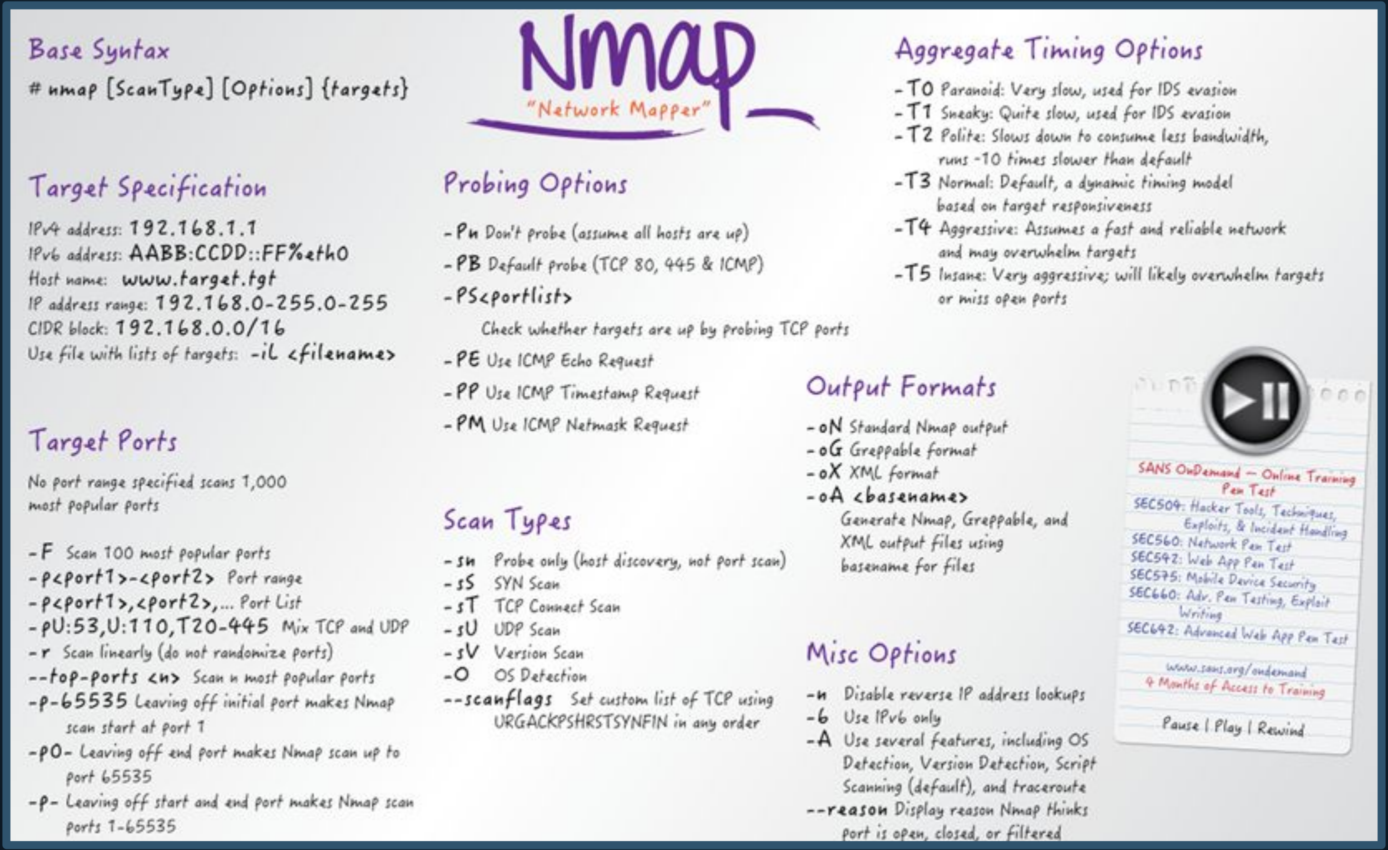
The OS and services versions can be vulnerable

- Quick-wins by checking known CVE
- Discover of non-web ports
- Architecture and technology knowledge

Is port scanning legal?

- It depends on the local jurisdiction and enterprise policy
- It is controversial but Shodan does not care about it

Nmap



Nmap
"Network Mapper"

Base Syntax

```
# nmap [ScanType] [Options] {targets}
```

Target Specification

IPv4 address: 192.168.1.1
IPv6 address: AABB:CCDD::FF%eth0
Host name: www.target.tgt
IP address range: 192.168.0-255.0-255
CIDR block: 192.168.0.0/16
Use file with lists of targets: -iL <filename>

Target Ports

No port range specified scans 1,000 most popular ports

- -F Scan 100 most popular ports
- -p<port1>-<port2> Port range
- -p<port1>,<port2>,... Port List
- -pU:53,U:110,T20-445 Mix TCP and UDP
- -r Scan linearly (do not randomize ports)
- --top-ports <n> Scan n most popular ports
- -p-65535 Leaving off initial port makes Nmap scan start at port 1
- -p0- Leaving off end port makes Nmap scan up to port 65535
- -p- Leaving off start and end port makes Nmap scan ports 1-65535

Probing Options

- -Pn Don't probe (assume all hosts are up)
- -PB Default probe (TCP 80, 445 & ICMP)
- -PS<portlist>
  Check whether targets are up by probing TCP ports
- -PE Use ICMP Echo Request
- -PP Use ICMP Timestamp Request
- -PM Use ICMP Netmask Request

Scan Types

- -sn Probe only (host discovery, not port scan)
- -sS SYN Scan
- -sT TCP Connect Scan
- -sU UDP Scan
- -sV Version Scan
- -O OS Detection
- --scanflags Set custom list of TCP using URGACKPSHRSTSYNFIN in any order

Aggregate Timing Options

- -T0 Paranoid: Very slow, used for IDS evasion
- -T1 Sneaky: Quite slow, used for IDS evasion
- -T2 Polite: Slows down to consume less bandwidth, runs ~10 times slower than default
- -T3 Normal: Default, a dynamic timing model based on target responsiveness
- -T4 Aggressive: Assumes a fast and reliable network and may overwhelm targets
- -T5 Insane: Very aggressive; will likely overwhelm targets or miss open ports

Output Formats

- -oN Standard Nmap output
- -oG Greppable format
- -oX XML format
- -oA <basename>
  Generate Nmap, Greppable, and XML output files using basename for files

Misc Options

- -n Disable reverse IP address lookups
- -6 Use IPv6 only
- -A Use several features, including OS Detection, Version Detection, Script Scanning (default), and traceroute
- --reason Display reason Nmap thinks port is open, closed, or filtered

SSL / TLS Analysis

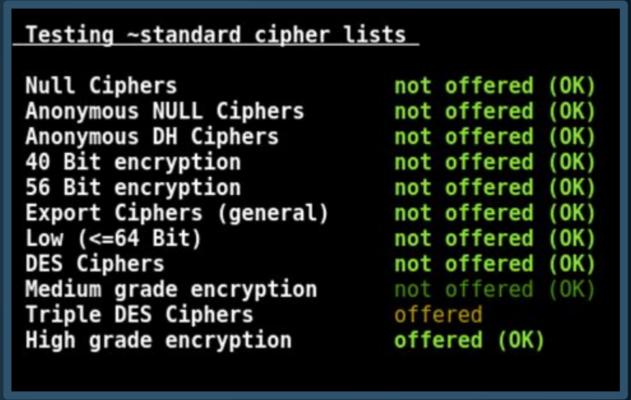
Why testing SSL / TLS is important?

- SSL and TLS knew important vulnerabilities in the past
- SSL / TLS is rarely an attack vector
- Nowadays HTTPS configurations can benefit from best practice hardenings
  - If the server accepts weak cipher suites the traffic can be considered as unencrypted
    - From a guest (OPEN) Wi-Fi all the traffic may be decrypted easily
- Keep in mind that the traffic can be captured and if a vulnerability is disclosed later, all the traffic can be decrypted

SSL / TLS Analysis

Tools

- Check the validity of the certificate
- Check the encryption robustness
- Check common and known vulnerabilities
- https://testssl.sh
- https://www.ssllabs.com/ssltest



```
 Testing ~standard cipher lists

 Null Ciphers                  not offered (OK)
 Anonymous NULL Ciphers        not offered (OK)
 Anonymous DH Ciphers          not offered (OK)
 40 Bit encryption             not offered (OK)
 56 Bit encryption             not offered (OK)
 Export Ciphers (general)      not offered (OK)
 Low (<=64 Bit)                not offered (OK)
 DES Ciphers                   not offered (OK)
 Medium grade encryption       not offered (OK)
 Triple DES Ciphers            offered
 High grade encryption         offered (OK)
```

Software Configuration Analysis

Focus on the application level

Here we are looking for

- Default pages and passwords
- Sensitive pages and information
- Software technologies and versions linked to known vulnerabilities
- Supported methods (GET / POST / TRACE / OPTIONS...)
- And much more...

Software Configuration Analysis

It should be done manually while using web scanners

The tools can be generic and adapted to known frameworks

- Nikto

They can be integrated to a proxy

- Burp pro and ZAP

They can be specific to a content management system (CMS)

- Wpscan for Wordpress
- Joomscan for Joomla
- Droopscan for Drupal

Software Configuration Analysis

Nikto

- It is an open source (GPL) Perl script useful for known frameworks, CMS and vulnerabilities
  - 3500 potential dangerous files tested
  - Known information disclosure, misconfigurations and version-specific issues
  - Injections (SQLi / XSS)
  - Remote command execution / remote shell...
- Nearly useless for custom development, you will need to test it manually
- May have false positives, you will need to cross check manually

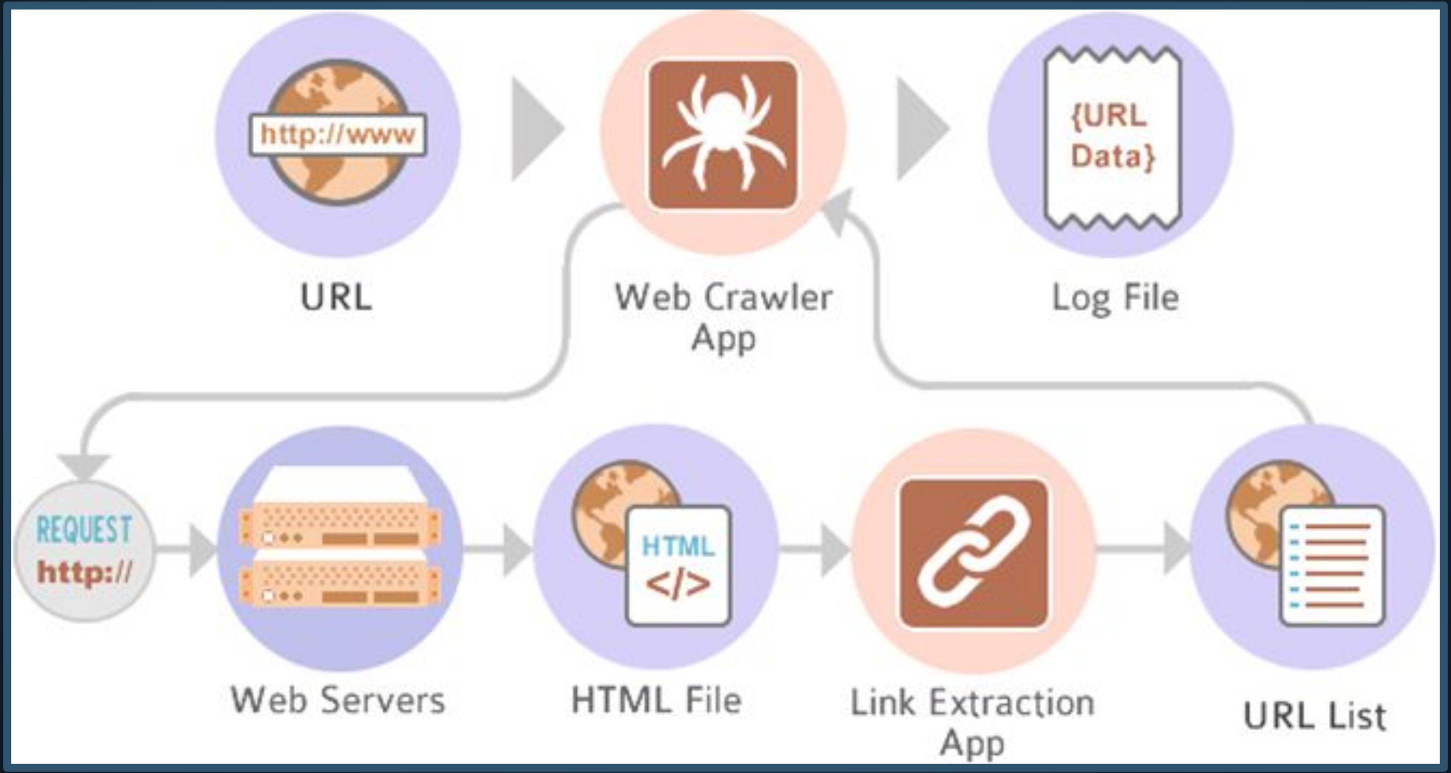
```
nikto -h https://example.com
```

Spidering

Also called crawling, it is the action of following web links to list them all

- It takes an URL and follow all the links found in the source code recursively
- The goal is to have a copy of the website arborescence
- It is typically automated to save time and avoid oversights
- It is also used to pull data that are read from the source code
  - Email addresses
  - Names / phone numbers
  - Internal IP addresses...

Spidering


http://www
URL
Web Crawler App
{URL Data}
Log File
REQUEST
http://
Web Servers
HTML
</>
HTML File
Link Extraction App
URL List

Spidering

A lot of requests are sent to the server in a shot timing frame while spidering

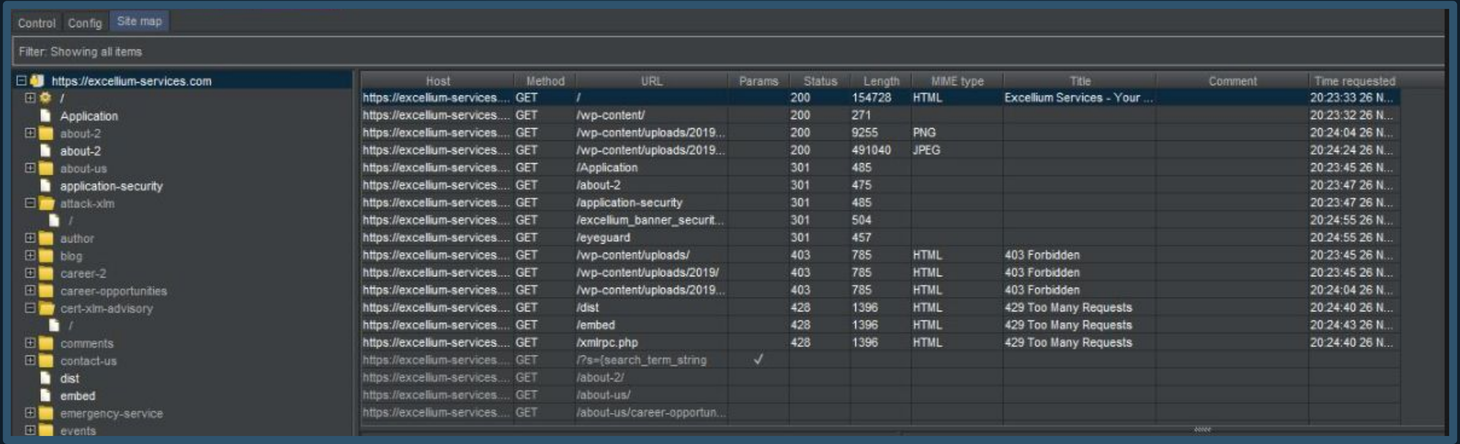
- The WAF can throttle the requests or ban you (public IP or session cookie)
- Some tools allow you to throttle your requests to avoid ban

Spidering can be done using a proxy

- ZAP & Burp
- They list all the links in a folder giving an overview and the complexity of the website
  - Features of the application and how it works
  - You can defined your own color coding marked the links as tested / vulnerable...

For Single Page Application (SPA) you will have to make it manually

Spidering



- https://excellium-services.com
  - /
  - Application
  - about-2
  - about-2
  - about-us
  - application-security
  - attack-xlm
    - /
  - author
  - blog
  - career-2
  - career-opportunities
  - cert-xlm-advisory
    - /
  - comments
  - contact-us
  - dist
  - embed
  - emergency-service
  - events

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
https://excellium-services....	GET	/		200	154728	HTML	Excellium Services - Your ...		20:23:33 26 N...
https://excellium-services....	GET	/wp-content/		200	271				20:23:32 26 N...
https://excellium-services....	GET	/wp-content/uploads/2019...		200	9255	PNG			20:24:04 26 N...
https://excellium-services....	GET	/wp-content/uploads/2019...		200	491040	JPEG			20:24:24 26 N...
https://excellium-services....	GET	/Application		301	485				20:23:45 26 N...
https://excellium-services....	GET	/about-2		301	475				20:23:47 26 N...
https://excellium-services....	GET	/application-security		301	485				20:23:47 26 N...
https://excellium-services....	GET	/excellium_banner_securit...		301	504				20:24:55 26 N...
https://excellium-services....	GET	/eyeguard		301	457				20:24:55 26 N...
https://excellium-services....	GET	/wp-content/uploads/		403	785	HTML	403 Forbidden		20:23:45 26 N...
https://excellium-services....	GET	/wp-content/uploads/2019/		403	785	HTML	403 Forbidden		20:23:45 26 N...
https://excellium-services....	GET	/wp-content/uploads/2019...		403	785	HTML	403 Forbidden		20:24:04 26 N...
https://excellium-services....	GET	/dist		428	1396	HTML	429 Too Many Requests		20:24:40 26 N...
https://excellium-services....	GET	/embed		428	1396	HTML	429 Too Many Requests		20:24:43 26 N...
https://excellium-services....	GET	/xmlrpc.php		428	1396	HTML	429 Too Many Requests		20:24:40 26 N...
https://excellium-services....	GET	/?s={search_term_string	✓						
https://excellium-services....	GET	/about-2/							
https://excellium-services....	GET	/about-us/							
https://excellium-services....	GET	/about-us/career-opportun...							

Spidering

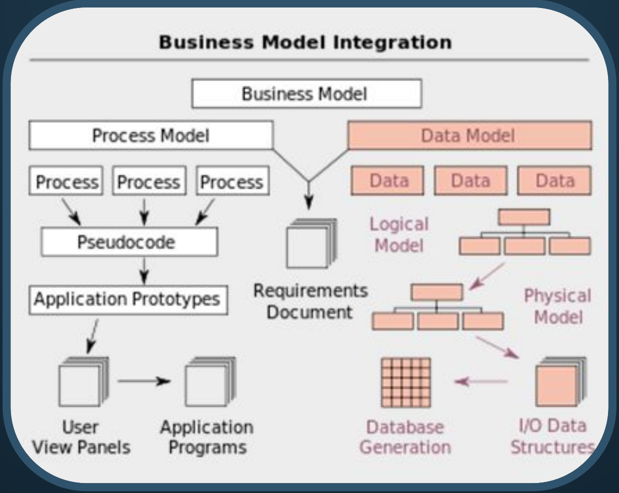
Look for potential quick win features from the spidering result

- Upload feature
- Admin and sensitive pages
  - Commented code or old development pages
- Sensitives documents hosted on the website
- Disabled functionalities
  - Old admin features that are left without restrictions

Spidering

Relationship analysis

- Check the interactions between the different parts of the application
- It can be very useful to understand the business model and logic
    - It can be used to test authorization bypass



Directory Listing

Spidering only follow links found on the source code

Some resources may not be referenced in source code

- Dirb is a web content scanner that recursively looks for existing web directories and pages
  - It works by launching a dictionary based attack against a web server and by analysing the HTTP response
  - It should be done to complete the spidering phase for pages that are not linked
    - Browse manually to the pages found by dirb through a proxy and it will be automatically added to the website arborescence in the proxy
  - It uses /usr/share/dirb/wordlists/common.txt as default dictionary

Directory Listing

Other tools may have their advantage against dirb

- https://cs.piosky.fr/web/directory_listing/

The dictionary choice is very important

- https://cs.piosky.fr/web/directory_listing/#dictionaries

The discovery of a hidden page is based on the HTTP code

- It can lead to false positives
  - HTTP code 200 instead for 404 (very useful mitigation)

Mapping

3

Mapping

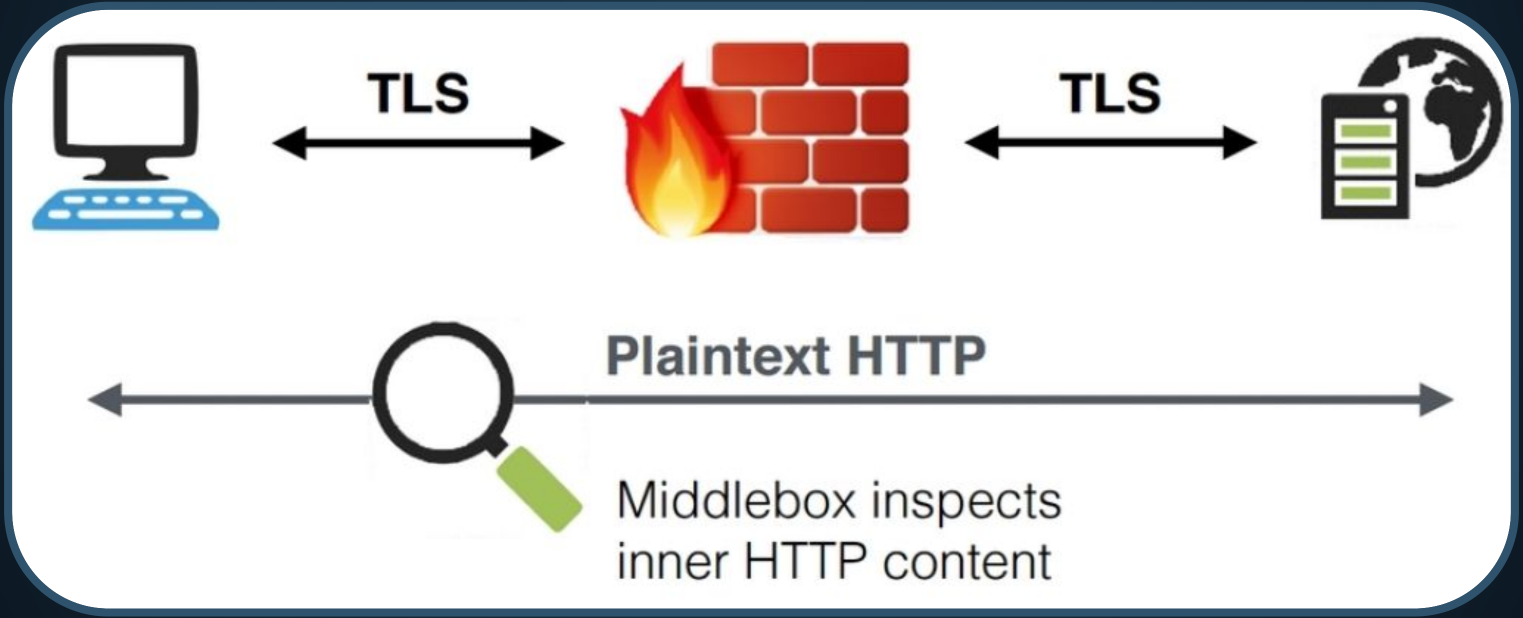
How to use a web proxy?

Proxy

The web proxy is the main tool for testing web application

- It is placed in a MiTM position and intercepts SSL / TLS
  - Add the proxy certificate in your browser
  - The proxy will negotiate an encryption with your browser and another one with the website
- It intercepts requests and responses
  - You can replay and modify requests on the fly
- It records and logs HTTP(S) traffic

Proxy


TLS
TLS
Plaintext HTTP
Middlebox inspects
inner HTTP content

Proxy

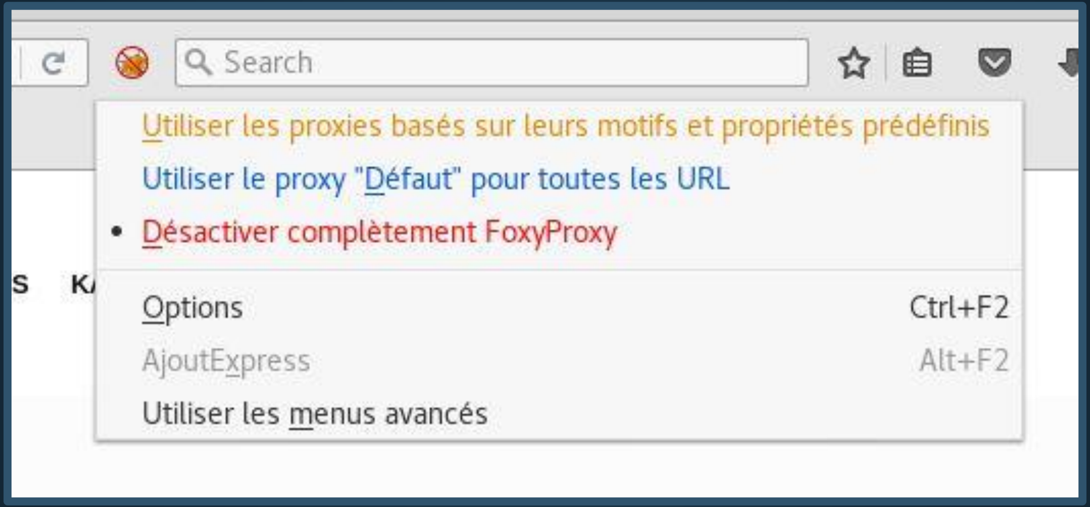
Tools

- Burp Suite
- OWASP Zed Attack Proxy (ZAP)
- Tamper data for Firefox
- Mitmproxy

Manage your web proxy with a plugin in your browser to save time

- FoxyProxy

FoxyProxy



Search

Utiliser les proxies basés sur leurs motifs et propriétés prédéfinis

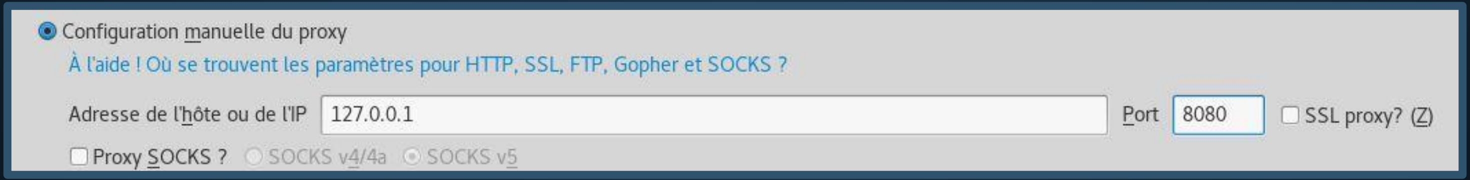
Utiliser le proxy "Défaut" pour toutes les URL

- Désactiver complètement FoxyProxy

Options Ctrl+F2

AjoutExpress Alt+F2

Utiliser les menus avancés



● Configuration manuelle du proxy

À l'aide ! Où se trouvent les paramètres pour HTTP, SSL, FTP, Gopher et SOCKS ?

Adresse de l'hôte ou de l'IP 127.0.0.1 Port 8080 □ SSL proxy? (Z)

□ Proxy SOCKS ? ○ SOCKS v4/4a ● SOCKS v5

Burp

Powered by portswigger

- Java-based and available on Windows and Linux
- Free version
  - Traffic interception essentially
- Paid version
  - Web crawler and efficient vulnerability scanner
  - Great performance against all the OWASP top 10 vulnerabilities

Zed Attack Proxy

ZAP

- Java-based and available on Windows and Linux
- Free and open source
- It includes web crawler and vulnerability scanner

Burp free vs ZAP

- Make you own choice

Burp pro vs ZAP

- Burp pro 349.00€ per year

Mapping

Questions

THANKS!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**