Footprinting for security auditors

Jose Manuel Ortega
@jmortegac
Agenda

- Information gathering
- Footprinting tools
- Port scanning with nmap
- Nmap scripts
Security auditing phases

**Analysis**
Who is
DNS Lookup
Search Engines
Enumeration

Analyze publicly available information. Set scope of attack and identify key targets.

**Scanning**
Machines
Ports
Applications

Check for vulnerabilities on each target resource.

**Exploitation**
Buffer Overflows
Spoofing
Password
Rootkit

Attack targets using library of tools and techniques.

**Damage**
“Owning” IP Theft,
Blackmail, Defacing,
Espionage,
Destruction, DoS

Footprinting for security auditors
Information Gathering
Information gathering

**Footprinting** (gather target information)
→ names, addresses, system types, ...

**Fingerprinting** (identify topologies & systems)
→ network layout, operating systems, services

**Sniffing** (collect network traffic)
→ addresses, names, information (passwords, ...)

**Enumeration** (collect access information)
→ list of user accounts, share names, ...

**Scanning** (detect systems and services)
→ response from network stack, applications, ...

---

Footprinting for security auditors
Footprinting

- Identify locations, domain names, IP address ranges, e-mail addresses, dial-in phone numbers, systems used, administrator names, network topology.

- Using public information.

- Without network /physical connection to the target.
Tools
Footprinting for security auditors
Whois Online Tools

- Get information about domains, IP address, DNS
- Identify the domain names and associated networks related to a particular organization
  - https://www.whois.net/
  - https://tools.whois.net/
  - http://www.whois.com/whois
  - http://who.is
  - http://toolbar.netcraft.com/site_report
  - http://whois.domaintools.com/
Footprinting for security auditors

- [http://toolbar.netcraft.com/site_report/?url=fosdem.org](http://toolbar.netcraft.com/site_report/?url=fosdem.org)

<table>
<thead>
<tr>
<th>Site</th>
<th><a href="http://fosdem.org">http://fosdem.org</a></th>
<th>Netblock Owner</th>
<th>FOSDEM infrastructure at bru-hdc.be</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>fosdem.org</td>
<td>Nameserver</td>
<td>ns1.fosdem.org</td>
</tr>
<tr>
<td>IP address</td>
<td>31.22.22.135</td>
<td>DNS admin</td>
<td><a href="mailto:hostmaster@fosdem.org">hostmaster@fosdem.org</a></td>
</tr>
<tr>
<td>IPv6 address</td>
<td>2001:67c:1808:0:0:0:0:5</td>
<td>Reverse DNS</td>
<td>unknown</td>
</tr>
<tr>
<td>Domain registrar</td>
<td>pir.org</td>
<td>Nameserver organisation</td>
<td>whois.pir.org</td>
</tr>
<tr>
<td>Organisation</td>
<td>FOSDEM VZW, Guldenendale 9, Nossegem, 1930, BE</td>
<td>Hosting company</td>
<td>tigrone.be</td>
</tr>
<tr>
<td>Top Level Domain</td>
<td>Organization entities (.org)</td>
<td>DNS Security Extensions</td>
<td>Enabled</td>
</tr>
<tr>
<td>Hosting country</td>
<td>BE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Whois

<table>
<thead>
<tr>
<th><strong>WHOIS &amp; Quick Stats</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Registrant Org</strong></td>
</tr>
<tr>
<td><strong>Dates</strong></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
</tr>
<tr>
<td><strong>IP Location</strong></td>
</tr>
<tr>
<td><strong>ASN</strong></td>
</tr>
<tr>
<td><strong>Domain Status</strong></td>
</tr>
<tr>
<td><strong>Whois History</strong></td>
</tr>
<tr>
<td><strong>IP History</strong></td>
</tr>
<tr>
<td><strong>Hosting History</strong></td>
</tr>
<tr>
<td><strong>Whois Server</strong></td>
</tr>
</tbody>
</table>

Footprinting for security auditors
Whois command

Domain Name: FOSDEM.ORG
Domain ID: D73040373-LROR
WHOIS Server:
Referral URL: http://www.key-systems.net
Updated Date: 2016-09-13T10:39:39Z
Creation Date: 2001-06-22T15:15:11Z
Registry Expiry Date: 2018-06-22T15:15:11Z
Sponsoring Registrar: Key-Systems GmbH
Sponsoring Registrar IANA ID: 269
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant ID: GED908411161
Registrant Name: Gerry Demaret
Registrant Organization: FOSDEM VZW
Registrant Street: Guldenlille 9
Registrant City: Nossegem
Registrant State/Province: 
Registrant Postal Code: 1930
Registrant Country: BE
Registrant Phone: +32.27887474
Registrant Phone Ext: 
Registrant Fax: 
Registrant Fax Ext: 
Registrant Email: info@fosdem.org
Host command

- Ge IPv4,v6,mail server
Network tools


Footprinting for security auditors
**NETWORK Tools**

- **https://www.dnssniffer.com/networktools**

The image shows a screenshot of the DNNSniffer tool, which offers various network tools for security auditors. The page includes options for Port Test, Heartbleed Test, and SIP Test, each with fields for inputting hostnames and ports. The tool also provides explanations for each function, such as the ability to look up domain or IP WHOIS information and ping a hostname or IP.
# Footprinting for security auditors

This section of the document includes a screenshot of a tool for security auditors. The tool, called `SuperTool Beta`, allows for MX lookup and other security checks.

## MX Lookup

The tool shows MX records for `mx:fosdem.org`.

<table>
<thead>
<tr>
<th>Prof</th>
<th>Hostname</th>
<th>IP Address</th>
<th>TTL</th>
<th>Blacklist Check</th>
<th>SMTP Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>apeiron.fosdem.org</td>
<td>31.22.22.130</td>
<td>10 min</td>
<td>Blacklist Check</td>
<td>SMTP Test</td>
</tr>
<tr>
<td>10</td>
<td>apeiron.fosdem.org</td>
<td>2001:67c:1808::2</td>
<td>10 min</td>
<td>Blacklist Check</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>episteme.fosdem.org</td>
<td>146.251.159.37</td>
<td>10 min</td>
<td>Blacklist Check</td>
<td>SMTP Test</td>
</tr>
<tr>
<td>20</td>
<td>episteme.fosdem.org</td>
<td>2a01:4f8:210:3227:941b:9f25:0:1</td>
<td>10 min</td>
<td>Blacklist Check</td>
<td></td>
</tr>
</tbody>
</table>

The tool also includes links for various security checks such as DNS lookup, DNS check, WHOIS lookup, SPF lookup, and DNS propagation.
Robtex

- Provides graphical information from DNS and Whois
- [https://www.robtex.com/dns-lookup/fosdem.org](https://www.robtex.com/dns-lookup/fosdem.org)
## On other domains (4 shown)

- fosdem.be
- fosdem.com
- fosdem.eu
- fosdem.net

## Subdomains (13 shown)

- *.fosdem.org
- apollo.fosdem.org
- episeme.fosdem.org
- mail.fosdem.org
- mx2.fosdem.org
- mx3.fosdem.org
- nanoc.fosdem.org
- ns1.fosdem.org
- ns2.fosdem.org
- sophos.fosdem.org
- video.fosdem.org
- www.fosdem.org
- www-public.fosdem.org

## The IP addresses of the mail servers of this domain name (4 shown)

- 2001:67c:1808::2
- 2a01:4f8:210:3227:94fb:9f25::1
- 31.22.22.130
- 148.251.159.37

## Domains using the same mail servers as this domain name (4 shown)

- fosdem.be
- fosdem.com
- fosdem.eu
- fosdem.net

## IP addresses of name servers of this domain name (9 shown)

- 2001:67c:1808::2
- 2001:67c:1808::4
- 2a00:d880:3:1::4dfb:e50
- 2a00:d880:5:41b::2
- 2a01:7c8:aaab:3:314::53
- 31.22.22.130
- 31.22.22.132
- 81.4.124.203
- 149.210.155.165
Nslookup

- Query DNS server in order to extract valuable information about the host machine.
- Find names of machines through a **domain/zone transfer**
- **Nslookup -d** → list all associated records for the domain

```plaintext
Got answer:
HEADER:
    opcode = QUERY, id = 2, rcode = NOERROR
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 2, authority records = 0, additional = 0

QUESTIONS:
  135.22.22.31.in-addr.arpa type = PTR, class = IN

ANSWERS:
  -> 135.22.22.31.in-addr.arpa
      canonical name = 135.128-159.22.22.31.in-addr.arpa
      ttl = 1598 (26 mins 36 secs)
  -> 135.128-159.22.22.31.in-addr.arpa
      name = www-public.fosdem.org
      ttl = 84398 (23 hours 26 mins 38 secs)

Nombre: www-public.fosdem.org
Address: 31.22.22.135
Aliases: 135.22.22.31.in-addr.arpa
```
# Dig /DNS Resolver

## Query

<table>
<thead>
<tr>
<th>Host</th>
<th>TTL</th>
<th>Class</th>
<th>Type</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>fosdem.org</td>
<td>600</td>
<td>IN</td>
<td>A</td>
<td>31.22.22.135</td>
</tr>
</tbody>
</table>

## Authority

- fosdem.org: 600 IN NS ns0.x-net.be.
- fosdem.org: 600 IN NS ns.gletsjer.net.
- fosdem.org: 600 IN NS ns1.fosdem.org.
- fosdem.org: 600 IN NS ns.gletsjer.org.

## Additional

- ns.gletsjer.net: 155288 IN AAAA 2a01:7c8:aab3:314::53
- ns.gletsjer.org: 8398 IN A 149.210.155.165

---

Footprinting for security auditors
Dnsmap

```
root@kali:~# dnsmap fosdem.org
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)
[+] searching (sub)domains for fosdem.org using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests
m.fosdem.org
IPv6 address #1: 2001:67c:1808::2
m.fosdem.org
IP address #1: 31.22.22.130
mail.fosdem.org
IPv6 address #1: 2001:67c:1808::2
mail.fosdem.org
IP address #1: 31.22.22.130
ns1.fosdem.org
IPv6 address #1: 2001:67c:1808::4
ns1.fosdem.org
IP address #1: 31.22.22.132
```
Dnsenum

root@kali:~# dnsenum fosdem.org
dnsenum.pl VERSION:1.2.3
usage: dnsenum <target-domain> [options]
options:
--wordlist <regular-results-file>
-c <csv-results-file>
-i <ips to ignore> (useful if you're obtaining false positives)

Host's addresses:
fosdem.org.

dnsmap target-domain.foo
nsmap target-domain.foo -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap target-domain.foo -r /tmp/ -d 3000
dnsmap target-domain.foo -r ./domainbf_results.txt

ns.gletsjer.org.
ns0.x-net.be.
ns1.fosdem.org.

Name Servers:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>fosdem.org</td>
<td>A</td>
<td>31.22.22.135</td>
</tr>
<tr>
<td>ns.gletsjer.org</td>
<td>A</td>
<td>149.210.155.165</td>
</tr>
<tr>
<td>ns0.x-net.be</td>
<td>A</td>
<td>81.4.124.203</td>
</tr>
<tr>
<td>ns1.fosdem.org</td>
<td>A</td>
<td>31.22.22.132</td>
</tr>
<tr>
<td>apeiron.fosdem.org</td>
<td>A</td>
<td>31.22.22.130</td>
</tr>
</tbody>
</table>

Mail (MX) Servers:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>fosdem.org</td>
<td>A</td>
<td>31.22.22.130</td>
</tr>
</tbody>
</table>
Footprinting for security auditors
Zone Transfer

- How does one provide security against DNS Interrogation?
- Restrict zone transfers to authorized servers.
- Set your firewall or router to deny all unauthorized inbound connections to **TCP port 53**
- Best practice to restrict Zone transfers is review file configuration `/etc/bind/named.conf.local`
Subdomains

- https://api.hackertarget.com/hostsearch/?q=fosdem.org
The harvester

• Catalogue email address and subdomains from a specific domain.
• It works with all the major search engines including Bing and Google.
• The objective is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.
The harvester

Usage: theharvester options

-\(d\): Domain to search or company name
-\(b\): data source: baidu, bing, bingapi, dogpile, google, googleCSE,
googleplus, google-profiles, linkedin, pgp, twitter, vhost,
yahoo, all

-\(s\): Start in result number X (default: 0)
-\(v\): Verify host name via dns resolution and search for virtual hosts
-\(f\): Save the results into an HTML and XML file (both)
-\(n\): Perform a DNS reverse query on all ranges discovered
-\(c\): Perform a DNS brute force for the domain name
-\(t\): Perform a DNS TLD expansion discovery
-\(e\): Use this DNS server
-\(l\): Limit the number of results to work with (bing goes from 50 to 50 results,
google 100 to 100, and pgp doesn't use this option)
-\(h\): use SHODAN database to query discovered hosts

Examples:
theHarvester.py -d microsoft.com -l 500 -b google -h myresults.html
theHarvester.py -d microsoft.com -b pgp
theHarvester.py -d microsoft -l 200 -b linkedin
theHarvester.py -d apple.com -b googleCSE -l 500 -s 300
The harvester

Emails found:
- devrooms@fosdem.org
- feedback@fosdem.org
- info@fosdem.org
- stands@fosdem.org

Hosts found in search engines:
- resolving hostnames IPs...
- 31.22.22.135:Archive.fosdem.org
- 31.22.22.130:Lists.fosdem.org
- 31.22.22.135:Video.fosdem.org
- 31.22.22.135:archive.fosdem.org
- 31.22.22.130:lists.fosdem.org
- 51.15.36.254:live.fosdem.org
- 31.22.22.135:penta.fosdem.org
- 31.22.22.135:staging.fosdem.org
- 31.22.22.135:video.fosdem.org
- 31.22.22.135:volunteers.fosdem.org
- 31.22.22.135:www.fosdem.org

Starting active queries:
- Performing reverse lookup in :31.22.22.0/24
- 31.22.22.255[ - ] Performing reverse lookup in :51.15.36.0/24
- 51.15.36.255

Hosts found after reverse lookup:
- 51.15.36.254:web0.video.fosdem.org
Footprinting for security auditors

Maltego

Footprint L1
This performs a level 1 (fast, basic) footprint of a domain.

Footprint L2
This performs a level 2 (mild) footprint of a domain.

Footprint L3
This performs a level 3 (complete) footprint of a domain.

Show on startup
Show on empty graph click

Please select a machine to run.
Maltego

- Company Stalker (this gathers email information)
- Footprint L1 (basic information gathering)
- Footprint L2 (moderate amount of information gathering)
- Footprint L3 (intense and the most complete information gathering)
Footprinting for security auditors

Maltego

Output - Transform Output

Transform To Phone numbers [From whois info] done (from entity "fosdem.com")
Using the whois information obtained during previous operations.. (from entity "fosdem.com")
Transform To Entities from whois [Alchemy] returned with 3 entities (from entity "fosdem.com")
Transform To Entities from whois [Alchemy] done (from entity "fosdem.com")
# Shodan

**Footprinting for security auditors**

## Example Findings

### 31.22.22.135 - www-public.fosdem.org

<table>
<thead>
<tr>
<th>Country</th>
<th>Belgium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Tigron BVBA</td>
</tr>
<tr>
<td>ISP</td>
<td>Tigron BVBA</td>
</tr>
<tr>
<td>Last Update</td>
<td>2017-01-05T01:13:01.403330</td>
</tr>
<tr>
<td>Hostnames</td>
<td>www-public.fosdem.org</td>
</tr>
<tr>
<td>ASN</td>
<td>A556837</td>
</tr>
</tbody>
</table>

### Ports

- **22**
- **80**
- **443**

### Services

- **OpenSSH Version: 7.2**
  - Key type: ssh-rsa
  - Key: AAAA83N2aC3yc2EAAAMGQABAAAASQIDDP10Nz10wAqKsuti11ksJNF2010InB3JDO7wboxxWZMB
  - MgjJrSlO31F5cJQbpmzVM9A7v5zR6bF0ckfOxvNv0x00C8NVx+qA7EStVFDNYkYD7SLm27FrFZQ
  - nX8El20prvVnh05AhV2GVR/12ÝYUMr/0G3UJW60N19mC51E2/42XvxE16JLr7Wp0Q25580v0H

---

[Map of Brussels](https://www.mapbox.com) © 2017 Mapbox © OpenStreetMap Improve this map © DigitalGlobe
Footprinting for security auditors
Mr looquier)

2001:67c:1808::2
lists.fosdem.org
31.22.22.130
80/tcp
Product: Apache
CPE: a:apache:http_server

HTTP/1.1 200 OK
Date: Wed, 02 Nov 2016 16:49:31 GMT
Server: Apache
Last-Modified: Wed, 06 Feb 2013 16:12:33 GMT
ETag: "166877e-21e-4d51897fe88d0"
Accept-Ranges: bytes

2001:67c:1808::2
lists.fosdem.org
31.22.22.130
80/tcp
Web robots

- https://wordpress.com/robots.txt
- https://wordpress.com/sitemap.xml
Footprinting for security auditors
New Scan

Scan Name
Descriptive name for this scan.

Seed Target
Starting point for the scan.

By Use Case  By Required Data  By Module

- **All**
  
  *Get anything and everything about the target.*
  
  All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

- **Footprint**
  
  *Understand what information this target exposes to the Internet.*
  
  Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

- **Investigate**
  
  *Best for when you suspect the target to be malicious but need more information.*
  
  Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

- **Passive**
  
  *When you don't want the target to even suspect they are being investigated.*
  
  As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan

*Note: Scan will be started immediately.*
### Data Element

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Source Data Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Break (Category: video)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="http://www.break.com/user/fosdem">http://www.break.com/user/fosdem</a></td>
<td></td>
</tr>
<tr>
<td>COLOURlovers (Category: hobby)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="http://www.colourlovers.com/lover/fosdem">http://www.colourlovers.com/lover/fosdem</a></td>
<td></td>
</tr>
<tr>
<td>CodeFlex (Category: coding)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="http://www.codeflex.com/site/users/view/fosdem">http://www.codeflex.com/site/users/view/fosdem</a></td>
<td></td>
</tr>
<tr>
<td>GitHub (Category: coding)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="https://api.github.com/users/fosdem">https://api.github.com/users/fosdem</a></td>
<td></td>
</tr>
<tr>
<td>Imageshack (Category: images)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="https://imageshack.com/user/fosdem">https://imageshack.com/user/fosdem</a></td>
<td></td>
</tr>
<tr>
<td>Instagram (Category: images)</td>
<td>fosdem.org</td>
</tr>
<tr>
<td><a href="https://instagram.com/fosdem/">https://instagram.com/fosdem/</a></td>
<td></td>
</tr>
<tr>
<td>Internet Archive (Category: search)</td>
<td>fosdem.org</td>
</tr>
</tbody>
</table>
Scanning tools

• **Active** footprinting

• Number and type of opened ports

• Type of services running in the servers

• Vulnerabilities of the services and software

• Nmap is a great tool for discovering Open ports, protocol numbers, OS details, firewall details, etc.
NMAP
Nmap Port Scanner

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/tcp</td>
<td>open</td>
<td>ftp</td>
</tr>
<tr>
<td>4/tcp</td>
<td>filtered</td>
<td>unknown</td>
</tr>
<tr>
<td>9/tcp</td>
<td>filtered</td>
<td>discard</td>
</tr>
<tr>
<td>13/tcp</td>
<td>filtered</td>
<td>daytime</td>
</tr>
<tr>
<td>19/tcp</td>
<td>filtered</td>
<td>chargen</td>
</tr>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
</tr>
<tr>
<td>26/tcp</td>
<td>open</td>
<td>rsftp</td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop3</td>
</tr>
<tr>
<td>139/tcp</td>
<td>filtered</td>
<td>netbios-ssn</td>
</tr>
<tr>
<td>143/tcp</td>
<td>open</td>
<td>imap</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>465/tcp</td>
<td>open</td>
<td>smtps</td>
</tr>
<tr>
<td>514/tcp</td>
<td>filtered</td>
<td>shell</td>
</tr>
<tr>
<td>587/tcp</td>
<td>open</td>
<td>submission</td>
</tr>
<tr>
<td>993/tcp</td>
<td>open</td>
<td>imaps</td>
</tr>
<tr>
<td>995/tcp</td>
<td>open</td>
<td>pop3s</td>
</tr>
<tr>
<td>2222/tcp</td>
<td>open</td>
<td>EtherNet/IP-1</td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
</tr>
<tr>
<td>5060/tcp</td>
<td>filtered</td>
<td>sip</td>
</tr>
</tbody>
</table>

- Unix-based port scanner
- Support for different scanning techniques
- Detects operating system of remote hosts
- Many configuration options
  - timing
  - scanned port range
  - scan method
- Various front ends for easier handling
Zenmap Port Scanner

Footprinting for security auditors
Zenmap Port Scanner

Footprinting for security auditors
Nmap whois

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>873/tcp</td>
<td>open</td>
<td>rsync</td>
</tr>
</tbody>
</table>

Host script results:

- whois-ip: Record found at whois.ripe.net
- inetnum: 31.22.22.128 - 31.22.22.159
- netname: BE-TIG-HDC-FOSDEM
- descr: FOSDEM infrastructure at bru-hdc.be
- country: BE
- role: Tigron Hostmaster
- email: hostmaster@tigron.net
## Guessing the Operating System

- We can use the `--osscan-guess` option to force Nmap into discovering the OS.

```plaintext
<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>873/tcp</td>
<td>open</td>
<td>rsync</td>
</tr>
</tbody>
</table>
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port.

Device type: general purpose


Aggressive OS guesses: FreeBSD 6.3-RELEASE (95%), OpenBSD 4.0 (94%), FreeBSD 9.0-RELEASE (92% RELEASE-p5 (91%), FreeBSD 9.0-RELEASE - 10.1-RELEASE (91%), FreeBSD 7.0-RELEASE (88%), FreeBSD 88%), FreeBSD 8.1-RELEASE (88%), FreeBSD 6.2-RELEASE (88%), FreeBSD 9.1-RELEASE (87%)

No exact OS matches for host (test conditions non-ideal).
Banner Grabbing

`nmap -p80 -sV -sT fosdem.org`

Starting Nmap 7.01 (https://nmap.org) at 2017-01-14 23:23 CET
Nmap scan report for fosdem.org (31.22.22.135)
Host is up (0.044s latency).
Other addresses for fosdem.org (not scanned): 2001:67c:1808::5
rDNS record for 31.22.22.135: www-public.fosdem.org
PORT STATE SERVICE VERSION
80/tcp open  http  nginx 1.10.1
Nmap Script Engine

• Simple scripts to automate a wide variety of networking tasks

• Are written in Lua programming language.

• Network discovery

• Vulnerability detection

• Backdoor detection

• Vulnerability exploitation
Nmap Script Engine

usr/local/share/nmap/scripts
Nmap Script Engine

- https://github.com/cldrn/nmap-nse-scripts/tree/master/scripts

<table>
<thead>
<tr>
<th>Script Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-trace.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-trendnet-tvip.110w.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-vuln-cve2012-1823.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-vuln-cve2013-0156.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-vuln-cve2015-1635.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-waf-detect.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-wordpress-brute.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>http-wordpress-enum.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>huawei5xx-udp-info.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>mikrotik-routeros-brute.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>mysql-vuln-cve2012-2122.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-conficker.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-cve2009-3103.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-ms06-023.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-ms07-029.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-ms08-057.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smb-vuln-regsvc-dos.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>smtp-dovecot-exim-exec.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
<tr>
<td>vulscan.nse</td>
<td>Merge 6.x and 7.x scripts into a new folder</td>
</tr>
</tbody>
</table>
Banner grabbing with nmap script

```bash
nmap --script banner fosdem.org
```

Nmap scan report for fosdem.org (31.22.22.135)
Host is up (0.047s latency).
Other addresses for fosdem.org (not scanned): 2001:67c:1808::5
rDNS record for 31.22.22.135: www-public.fosdem.org
Not shown: 996 filtered ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>__banner: SSH-2.0-OpenSSH_7.2 FreeBSD-20160310</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
</tr>
<tr>
<td>873/tcp</td>
<td>open</td>
<td>rsync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>__banner: @SYNCD: 31.0</td>
</tr>
</tbody>
</table>
The document provides an example of using the `nmap` command with the `http-enum` script to perform a footprinting scan for security auditors. The command used is:

```
nmap -v --script http-enum.nse fosdem.org
```

The output from running this command includes information about the script scanning 31.22.22.135, initiating NSE at 16:31, completing NSE at 16:32 with a 31.03s elapsed time. It notes the host is up with 0.060s latency and provides other addresses for fosdem.org (not scanned) as 2001:67c:1808::5, a rDNS record for 31.22.22.135 as www-public.fosdem.org, and mentions 996 filtered ports.

The scan details also show open ports:

- 22/tcp open ssh
- 80/tcp open http
- 443/tcp open https
- / http-enum:
  - /atom.xml: RSS or Atom feed
- 873/tcp open rsync

The NSE: Script Post-scanning message indicates the script scanning is complete at 16:32 with 0.00s elapsed time.
mysql-databases

```
nmap -v -d -p3306 --script mysql-databases.nse
--script-args='mysqluser=root' 192.168.100.8
```

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td>syn-ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mysql-databases:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>information_schema</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>dvwa</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>metasploit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>owasp10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tikiwiki</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tikiwiki195</td>
<td></td>
</tr>
</tbody>
</table>
dependencies = {"mysql-brute", "mysql-empty-password"}
-- Version 0.1
-- Created 01/23/2010 - V0.1 - created by Patrik Karlsson
portrule = shortport.port_or_service(3306, "mysql")
action = function( host, port )
    local socket = nmap.new_socket()
    local catch = function() socket:close() end
    local try = nmap.new_try(catch)
    local result, response, dbs = {}, nil, {}
    local users = {}
    local nmap_args = nmap.registry.args
    local status, rows

    -- set a reasonable timeout value
    socket:set_timeout(5000)

    -- first, let's see if the script has any credentials as arguments?
    if nmap_args.mysqluser then
        users[nmap_args.mysqluser] = nmap_args.mysqlpass or ""
    -- next, let's see if mysql-brute or mysql-empty-password brought us anything
    elseif nmap.registry.mysqlusers then
        -- do we have root credentials?
        if nmap.registry.mysqlusers['root'] then
            users['root'] = nmap.registry.mysqlusers['root']
        else
            we didn't have root, so let's make sure we loop over them all
            users = nmap.registry.mysqlusers
        end
    -- last, no dice, we don't have any credentials at all
    else
        stdnse.debug1("No credentials supplied, aborting ...")
        return
    end
end
Find vulnerabilities with nmap

• XSS / SQL Injection

```bash
nmap -p80 --script http-unsafe-output-escaping <target>
```

Vulnerability Scanner
Footprinting for security auditors

Nessus Vulnerability Scanner

wordpress.com

CURRENT RESULTS: TODAY AT 11:35 AM

Host Details
IP: 192.0.78.17
DNS: wordpress.com
Start: Today at 11:24 AM
End: Today at 11:35 AM
Elapsed: 11 minutes
KB: Download

Vulnerabilities
- SSL Medium Strength Cipher Suites Supported: General - 1
- SSL 64-bit Block Size Cipher Suites Supported (SWEET32): General - 1
- Service Detection: Service detection - 3
- HTTP Server Type and Version: Web Servers - 2
- HyperText Transfer Protocol (HTTP) Information: Web Servers - 2
- Nessus SYN scanner: Port scanners - 2
- Web Server No 404 Error Code Check: Web Servers - 2
Arachni Vulnerability Scanner

http://testhtml5.vulnweb.com

Issues

Issues may be missing some context while the scan is running.

You may see some errors in the report as the scan progresses.

You can download self-contained

- Linux x86 32bit (SHA1)
- Linux x86 64bit (SHA1)

Attention: The packages need GLIBC >= 2.12, if you run the software on Ubuntu.

Footprinting for security auditors
Footprinting for security auditors

Links & References

- [http://www.0daysecurity.com/penetration-testing/network-footprinting.html](http://www.0daysecurity.com/penetration-testing/network-footprinting.html)
- [http://nmap.org/nsedoc/](http://nmap.org/nsedoc/)
- [https://secwiki.org/w/Nmap/External_Script_Library](https://secwiki.org/w/Nmap/External_Script_Library)
- [https://hackertarget.com/7-nmap-nse-scripts-recon/](https://hackertarget.com/7-nmap-nse-scripts-recon/)
Footprinting for security auditors
Thank you!

Jose Manuel Ortega
@jmortegac