Footprinting for security auditors

Jose Manuel Ortega
@jmortegac

Agenda

FOSDEM'17

- Information gathering
- Footprinting tools
- Port scanning with nmap
- Nmap scripts

Security auditing phases

FOSDEM'17

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

Information Gathering

Information gathering

FOSDEM'17

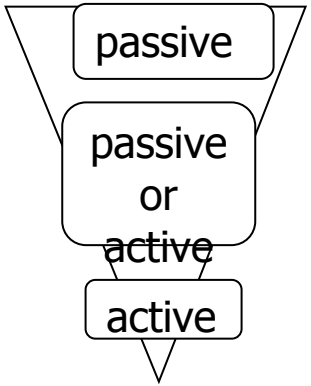
Footprinting (gather target information)
➔ names, addresses, system types, ...

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

- 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

Kali Linux

FOSDEM'17

Whois Online Tools

FOSDEM'17

- 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/

Netcraft

FOSDEM'17

- http://toolbar.netcraft.com/site_report/?url=fosdem.org

Network

Site	http://fosdem.org	Netblock Owner	FOSDEM infrastructure at bru-hdc.be
Domain	fosdem.org	Nameserver	ns1.fosdem.org
IP address	31.22.22.135	DNS admin	hostmaster@fosdem.org
IPv6 address	2001:67c:1808:0:0:0:0:5	Reverse DNS	*unknown*
Domain registrar	pir.org	Nameserver organisation	whois.pir.org
Organisation	FOSDEM VZW, Guldendelle 9, Nossegem, 1930, BE	Hosting company	tigron.be
Top Level Domain	Organization entities (.org)	DNS Security Extensions	Enabled
Hosting country	BE		

Whois

FOSDEM'17

Whois
Identity for everyone

DOMAINS HOSTING CLOUD NEW WEBSITES EMAIL SECURITY

Whois IP 31.22.22.135

Upc

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '31.22.22.128 - 31.22.22.159'

% Abuse contact for '31.22.22.128 - 31.22.22.159' is 'abuse@tigron.net'

inetnum:        31.22.22.128 - 31.22.22.159
netname:        BE-TIG-HDC-FOSDEM
descr:          FOSDEM infrastructure at bru-hdc.be
country:        BE
admin-c:        TGRN-RIPE
tech-c:         TGRN-RIPE
status:         ASSIGNED PA
mnt-by:         TGRN-MNT
mnt-lower:      TGRN-MNT
mnt-routes:     TGRN-MNT
created:        2014-04-30T15:42:47Z
last-modified:  2014-04-30T15:42:47Z
source:         RIPE
```

Whois & Quick Stats

Email	info@fosdem.org is associated with ~3 domains support@tigron.be is associated with ~68 domains dns@tigron.net is associated with ~4,217 domains
Registrant Org	FOSDEM VZW is associated with ~4 other domains
Dates	Created on 2001-06-22 - Expires on 2018-06-22 - Updated on 2016-09-13
IP Address	31.22.22.135 is hosted on a dedicated server
IP Location	- Vlaams-brabant - Zaventem - Tigron Bvba
ASN	AS56837 TIGRON-AS , BE (registered May 24, 2011)
Domain Status	Registered And Active Website
Whois History	70 records have been archived since 2006-02-09
IP History	9 changes on 6 unique IP addresses over 11 years
Hosting History	12 changes on 6 unique name servers over 14 years
Whois Server	whois.pir.org

Whois command

FOSDEM'17

```
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: Guldendelle 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

FOSDEM'17

- Ge IPv4,v6,mail server

```
fosdem.org has address 31.22.22.135
fosdem.org has IPv6 address 2001:67c:1808::5
fosdem.org mail is handled by 20 episteme.fosdem.org.
fosdem.org mail is handled by 10 apeiron.fosdem.org.
```

Network tools

FOSDEM'17

- http://network-tools.com/

Express
Ping
Trace
Whois (IDN Conversion Tool)
DNS Records (Advanced Tool)
Network Lookup
Spam Blacklist Check
URL Decode
URL Encode
HTTP Headers SSL
Email Tests

Convert Base-10 to IP

31.22.22.135

GO!

whois databases direct links. IP addresses Whois:
Americas (ARIN)
Europe (RIPE)
Asia-Pacific (APNIC)
Africa (AfriNIC)
Latin America/Carib. (LACNIC)
Subnet Calculator
Registrars:
Network Solutions
Godaddy
Tucows
ENOM
.biz .org
Country Code (2-letter) domains:
.ae | .au | .be | .br | .bs | .ca | .cl
.co | .de | .dz | .ec | .es | .hr | .hu | .id
.io | .kr | .my | .nl | .ph | .pk | .ru
.us | .za
Suggest a Link

31.22.22.135 is from Belgium (BE) in region Western Europe
Input: 31.22.22.135
canonical name: www-public.fosdem.org
aliases:
135.22.22.31.in-addr.arpa

Registered Domain: fosdem.org

TraceRoute from Network-Tools.com to 31.22.22.135 [www-public.fosdem.org]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	1	0	0	206.123.64.221	-
2	Timed out	1355	Timed	4.15.32.133	lag-127.ear1.dallas1.level3.net
3	Timed out	Timed out	Tin		
4	64	64			
5	69	69			s.net
6	146	146	1		s.net
7	142	141	1		s.net
8	176	176	1		gs.net
9	146	146	1		
10	177	178	1		n.net
11	176	176	1		

Trace complete

Save as (displaying dialog)
Save directly (using preferred file output settings)
Open in image editor
Copy to clipboard
Send to printer
Microsoft Outlook
Microsoft Powerpoint
Microsoft Word
Microsoft Excel
MS Paint
Paint.NET
Upload to Imgur
Close

Retrieving DNS records for ww

DNS servers
ns.gletsjer.net
ns0.x-net.be
ns.gletsjer.org
ns1.fosdem.org [31.22.22.132]

Answer records

www-public.fosdem.org	A	31.22.22.135	
www-public.fosdem.org	MX	preference: exchange:	0
www-public.fosdem.org	28	[16 bytes]	
www-public.fosdem.org	47	[20 bytes]	

Authority records

NETWORK Tools

FOSDEM'17

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

DNSSniffer Free Tools

Domain / IP

Domain / IP

Example example.com or 198.51.100.1

Lookup

Explanation

Lookup domain or IP WHOIS information.

Hostname / IP

Hostname / IP

Example www.example.com or 198.51.100.1

Ping

Explanation

Ping a hostname or IP.

Hostname

fosdem.org

Example www.example.com

Lookup

Explanation

Lookup the details (including expiration date) o

Port Test

Hostname / IP

Hostname / IP

Example www.example.com or 198.51.100.1

Port

Port

Heartbleed Test

Hostname / IP

Hostname / IP

Example www.example.com or 198.51.100.1

Port

Port

SIP Test

Hostname / IP

Hostname / IP

Example www.example.com or 198.51.100.1

Phone number

Phone number

MX TOOLBOX®

FOSDEM'17

MX Lookup | Blacklists | Diagnostics | Domain Health | Analyze Headers | Free Monitoring | DNS Lookup | More

SuperTool Beta7

fosdem.org MX Lookup

mx:fosdem.org Find Problems

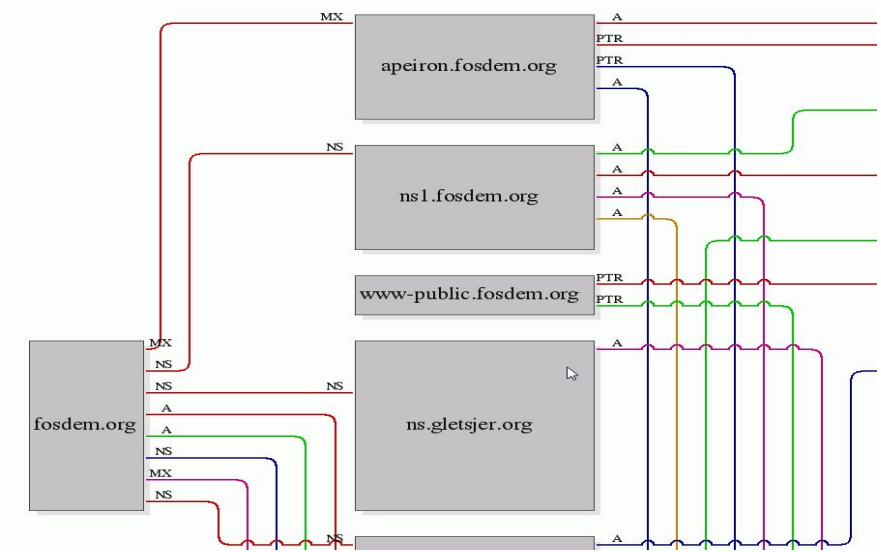
Pref	Hostname	IP Address	TTL		
10	apeiron.fosdem.org	31.22.22.130	10 min	Blacklist Check	SMTP Test
10	apeiron.fosdem.org	2001:67c:1808::2	10 min	Blacklist Check	
20	episteme.fosdem.org	148.251.159.37	10 min	Blacklist Check	SMTP Test
20	episteme.fosdem.org	2a01:4f8:210:3227:94fb:9f25:0:1	10 min	Blacklist Check	

dns lookup | dns check | whois lookup | spf lookup | dns propagation

Robtex

FOSDEM'17

- Provides graphical information from DNS and Whois
- https://www.robtex.com/dns-lookup/fosdem.org



Robtex

FOSDEM'17

On other domains (4 shown)

```
fosdem.be
fosdem.com
fosdem.eu
fosdem.net
```

Subdomains (13 shown)

```
*.fosdem.org
apeiron.fosdem.org
episteme.fosdem.org
mx1.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
```

Similarly typed (215 shown)

```
demo-sf.com
demoafs.com
```

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:c50
2a00:d880:5:41b::2
2a01:7c8:aab3:314::53
31.22.22.130
31.22.22.132
81.4.124.203
149.210.155.165
```

Nslookup

FOSDEM'17

- 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

```
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 38 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

FOSDEM'17

Query: fosdem.org

Server:

Type: A

Options

Response | Raw

Host	TTL	Class	Type	Answer
Answer:				
fosdem.org.	600	IN	A	31.22.22.135
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

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> +recurse +additional +authority +not
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42245
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;fosdem.org.                    IN      A

;; ANSWER SECTION:
fosdem.org.             600     IN      A       31.22.22.135

;; AUTHORITY SECTION:
fosdem.org.             600     IN      NS      ns0.x-net.be.
fosdem.org.             600     IN      NS      ns.gletsjer.net.
```

Dnsmap

FOSDEM'17

```
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
```

```
ns2.fosdem.org
IP address #1: 85.158.215.91

staging.fosdem.org
IPv6 address #1: 2001:67c:1808::5

staging.fosdem.org
IP address #1: 31.22.22.135

webmail.fosdem.org
IPv6 address #1: 2001:67c:1808::5

webmail.fosdem.org
IP address #1: 31.22.22.135

www.fosdem.org
IPv6 address #1: 2001:67c:1808::5

www.fosdem.org
IP address #1: 31.22.22.135

[+] 13 (sub)domains and 13 IP address(es) found
```

Dnsenum

```
root@kali:~# dnsenum fosdem.org
dnsenum.pl VERSION:1.2.3

-----   fosdem.org   -----

Host's addresses:

fosdem.org.                              600      IN    A        31.22.22.135

Name Servers:

ns.gletsjer.org.                         78960    IN    A        149.210.155.165
ns0.x-net.be.                            82883    IN    A        81.4.124.203
ns1.fosdem.org.                          86400    IN    A        31.22.22.132

Mail (MX) Servers:

apeiron.fosdem.org.                      600      IN    A        31.22.22.130
```

DnsRecon

FOSDEM'17

```
root@kali:~# dnsrecon -d fosdem.org
[*] Performing General Enumeration of Domain: fosdem.org
[*] DNSSEC is configured for fosdem.org
[*] DNSKEYs:
[*]     NSEC ZSK RSASHA256 03010001d907ba6f1833aba5344fb850 2366191
0acf95ca46c 4c319f195e95e52d3fcf5d4dfd3a0b86 d7a545b6d325a61dab9c5d
04ea5
[*]     NSEC ZSK RSASHA256 03010001bd84cc4da961fb69e176aba9 03fecc3
d4162c1504c bc93af2741ecde2b8ce5e970a6c69cb6 21e144c87ebedd8a08ace5
d1cff
[*]     NSEC KSk RSASHA256 03010001d55fbcbef97374b2d9125c42 794becf
a96cf2f7db2 cdda726dd4e88014f5ae2d2b9e1d2391 c4111d2233a26fe0e765b1
a7da87dea11e8577b4d6a1c9a69b2 e1c31cd79d9fcfbb4e799d89a7ae10d5 d843
cda803b0856f66 32d068765e13e328e1f086ce4cc28eda 917def0ead244deb09c
[*]     NSEC ZSK RSASHA256 03010001e46b4148b17afbd6ebf15033 06d3428
5e0b3543e27 2a2d650675e105c3efd64239b8ce6432 7626f4ab2068b98603315f
d8411
[*]     NSEC ZSK RSASHA256 03010001d93176185d8ed5abf414b3d1 4ef9b9e
5f560be2b4e e7719a952c195237ed39f495eb9892db 91dd5905194654b7ed16eb
8372f
[*]     NSEC KSk RSASHA256 03010001c39b119d082b186355bb62fc 932fb4a
858a9b70f7d 9c06d11b60453c12cd3dbeccf020eb7c ddd56cc60e510964078cb8
e7bcc432f5f8c381ee332f9f590cc ac5461929cca84f3ddf4ad1b46b90e4e 087f
35b1acae88fbee 6b16d2ce04ce676c980027eb07708d89 fe2035a0296bcbbda8d
[*]     NSEC ZSK RSASHA256 03010001d3cfc514545abf1fbd118944 f4e641e
3f8d9e3066a aaf122ec52aa325ccf7a8e59b775a966 c67d215f269f33b0230fc2
3271f
[*]      SOA ns1.fosdem.org 31.22.22.132
[*]      NS ns1.fosdem.org 31.22.22.132
[*]      NS ns1.fosdem.org 2001:67c:1808::4
[*]      NS ns.gletsjer.org 149.210.155.165
```

```
[*]      SOA ns1.fosdem.org 31.22.22.132
[*]      NS ns1.fosdem.org 31.22.22.132
[*]      NS ns1.fosdem.org 2001:67c:1808::4
[*]      NS ns.gletsjer.org 149.210.155.165
[*]      Bind Version for 149.210.155.165 unknown
[*]      NS ns.gletsjer.net 2a01:7c8:aab3:314::53
[*]      NS ns0.x-net.be 81.4.124.203
[*]      Bind Version for 81.4.124.203 A Fine DNS Server
[*]      NS ns0.x-net.be 2a00:d880:5:41b::2
[*]      MX apeiron.fosdem.org 31.22.22.130
[*]      MX episteme.fosdem.org 148.251.159.37
[*]      MX apeiron.fosdem.org 2001:67c:1808::2
[*]      MX episteme.fosdem.org 2a01:4f8:210:3227:94fb:9f25:0
[*]      A fosdem.org 31.22.22.135
[*]      AAAA fosdem.org 2001:67c:1808::5
[*]      TXT fosdem.org v=spf1 ip4:31.22.22.130 ip6:2001:67c:
[*] Enumerating SRV Records
[*]      SRV _kerberos._udp.fosdem.org episteme.fosdem.org 14
[*]      SRV _kerberos._udp.fosdem.org episteme.fosdem.org 2a
[*]      SRV _kerberos._udp.fosdem.org phronesis.fosdem.org 3
[*]      SRV _kerberos._udp.fosdem.org phronesis.fosdem.org 2
[*]      SRV _kerberos._tcp.fosdem.org phronesis.fosdem.org 3
[*]      SRV _kerberos._tcp.fosdem.org phronesis.fosdem.org 2
[*]      SRV _kerberos._tcp.fosdem.org episteme.fosdem.org 14
[*]      SRV _kerberos._tcp.fosdem.org episteme.fosdem.org 2a
[*]      SRV _kpasswd._udp.fosdem.org phronesis.fosdem.org 31
[*]      SRV _kpasswd._udp.fosdem.org phronesis.fosdem.org 20
[*] 10 Records Found
```

Zone Transfer

FOSDEM'17

- **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**

```
Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for fosdem.org on ns.gletsjer.org ...
AXFR record query failed: REFUSED

Trying Zone Transfer for fosdem.org on ns1.fosdem.org ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for fosdem.org on ns0.x-net.be ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for fosdem.org on ns.gletsjer.net ...
AXFR record query failed: no socket TCP[2a01:7c8:aab3:314:0:0:0:53] Network is u
nreachable
```

Subdomains

FOSDEM'17

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

```
fosdem.org,31.22.22.135
apeiron.fosdem.org,31.22.22.130
episteme.fosdem.org,148.251.159.37
lists.fosdem.org,31.22.22.130
live.fosdem.org,149.210.147.206
nanoc.fosdem.org,31.22.22.131
ns1.fosdem.org,31.22.22.132
sophos.fosdem.org,85.158.215.91
www-public.fosdem.org,31.22.22.135
```

The harvester

FOSDEM'17

- 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

FOSDEM'17

```
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

FOSDEM'17

```
[+] 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
        51.15.36.255Hosts found after reverse lookup:
---------------------------------
51.15.36.254:web0.video.fosdem.org
```

Maltego

FOSDEM'17

Maltego

FOSDEM'17

- 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)**

Maltego

FOSDEM'17

Home | New Graph (1)

Main View | Bubble View | Entity List

info@fosdem.org

ns1.fosdem.org

fosdem

W:2

"Key-systems Gmbh"

Verisign

dns@tigron.net

Transforms

- All Transforms
- DNS from Domain
- Domain owner detail
- Email addresses from Domain
- Files and Documents from Domain

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")
```

Overview | Machines

Footprint L3
[fosdem.org]

Machine failed

Detail View

Domain
maltego.Domain
fosdem.com

- Relationships
+ Incoming
+ Outgoing

Property View

Properties

Type	Domain
Domain Name	fosdem.com
WHOIS Info	Whois Server Versi...

Graph info

Weight	100

Shodan

FOSDEM'17

31.22.22.135 www-public.fosdem.org

Country	Belgium
Organization	Tigron BVBA
ISP	Tigron BVBA
Last Update	2017-01-05T01:13:01.403330
Hostnames	www-public.fosdem.org
ASN	AS56837

Ports

22 80 443

Services

22
tcp
ssh

OpenSSH Version: 7.2

```
SSH-2.0-OpenSSH_7.2 FreeBSD-20160310
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDDPIDNZi0wAqKsutiiksJNF2OiOInB3/DOYwfboax9V3MB
Mgjr3l6o3t1F5JPCbqmvHM9Aa7vsMSbFOckfnVzMnxKUC8NVk+gA7E5tVfDNTkYD7SLtM27FrFZQ
nXRGZwprvhhgozWuhZvGR/IZYfum8//G3JXwS0NI0mC5IE2/42XsxuEl6ULujWg0QzS6OeV0sOvH
```

Censys.io

FOSDEM'17

censys

fosdem.org

IPv4 Hosts | Top Million Websites | Certificates | Tools | Help

31.22.22.130 (apeiron.fosdem.org)

TIGRON-AS - , BE (56837) Belgium

143/imap, 25/smtp, 443/https, 80/http, 993/imaps

FOSDEM *.fosdem.org, fosdem.org

993.imaps.tls.tls.certificate.parsed.names: `fosdem.org`

443.https.tls.certificate.parsed.names: `fosdem.org`

http smtp imaps https

31.22.22.137

TIGRON-AS - , BE (56837) Belgium

443/https, 80/http

Index of /files/ *.fosdem.org, fosdem.org

443.https.tls.certificate.parsed.names: `fosdem.org`

http https

Mr looquer

FOSDEM'17

fosdem.org

EXPLORE ABOUT LOOQUERS MANAGE JMORTEGA API DOC LOGOUT

‹ Previous Page 1 of 1 pages Next ›

2001:67c:1808::2

lists.fosdem.org

31.22.22.130
80/tcp
Product: Apache httpd
cpe:/a:apache:http_server

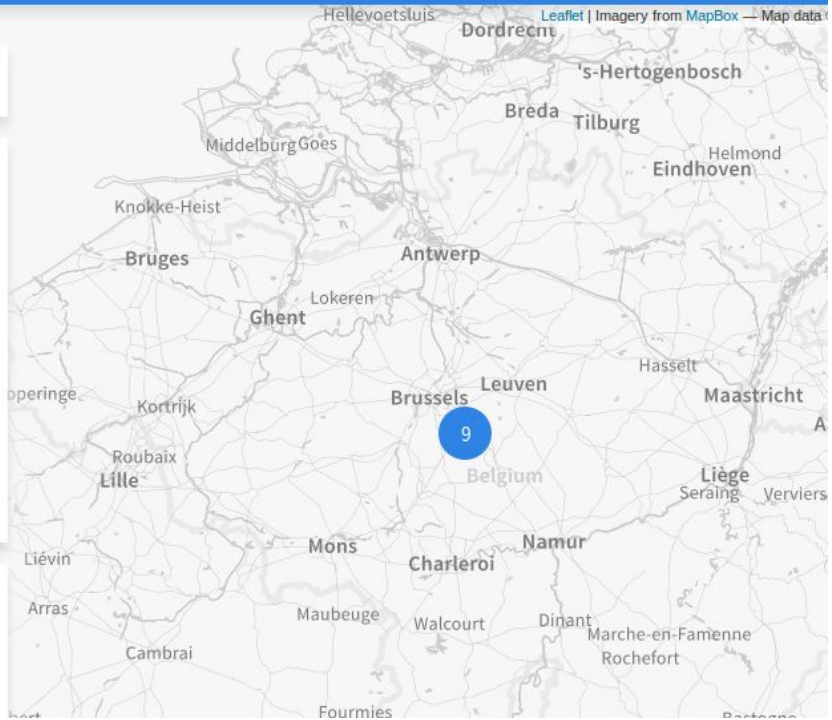
```
HTTP/1.1 200 OK
Date: Wed, 02 Nov 2016 16:49:31 GMT
Server: Apache
Last-Modified: Wed, 06 Feb 2013 16:12:33 GMT
ETag: "166077e-21e-4d51097fe08d0"
Accept-Ranges: bytes
```

02/11/2016 17:11

2001:67c:1808::2

lists.fosdem.org

31.22.22.130
80/tcp



Web robots

FOSDEM'17

- https://wordpress.com/robots.txt
- https://wordpress.com/sitemap.xml

Web Archive

FOSDEM'17

INTERNET ARCHIVE WayBackMachine

http://fosdem.org/ Go

1,560 captures
31 Oct 01 - 7 Jan 17

OCT NOV JAN
30
2000 2001 2003

Home
About Us
News
In the News
Schedule
Topics
Speakers
Register!
Where to stay
mailing list
Directions/Maps
Links

Current News

Richard Morrell comes back !

Richard Morrell will be at FOSDEM 2002. We had the chance to hear him at the first edition talking about SmoothWall.

Recent News

Philippe Aigrain

More speakers ...

2 new speakers

GNUstep

Graphist

About Us

Result of last year survey

Content writers

Our Sponsors

The birth of OSDEM

Spider foot

FOSDEM'17

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.

Spider foot

FOSDEM'17

SpiderFoot | New Scan | Scans | Settings

Browse > Account on External Site

Data Element	Source Data Element
Break (Category: video) http://www.break.com/user/fosdem	fosdem.org
COLOURlovers (Category: hobby) http://www.colourlovers.com/lover/fosdem	fosdem.org
CodePlex (Category: coding) http://www.codeplex.com/site/users/view/fosdem	fosdem.org
GitHub (Category: coding) https://api.github.com/users/fosdem	fosdem.org
ImageShack (Category: images) https://imageshack.com/user/fosdem	fosdem.org
Instagram (Category: images) https://instagram.com/fosdem/	fosdem.org
Internet Archive (Category: search) http://archive.org/search.php?query=fosdem	fosdem.org

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

FOSDEM'17

```
root@ubuntu:~# nmap

Starting Nmap 6.26SVN ( http://nmap.org )
Nmap scan report for
Host is up (1.1s latency).
Not shown: 978 closed ports
PORT      STATE    SERVICE
3/tcp     filtered compressnet
4/tcp     filtered unknown
9/tcp     filtered discard
13/tcp    filtered daytime
19/tcp    filtered chargen
21/tcp    open     ftp
25/tcp    open     smtp
26/tcp    open     rsftp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
465/tcp   open     smtps
514/tcp   filtered shell
587/tcp   open     submission
993/tcp   open     imaps
995/tcp   open     pop3s
2222/tcp  open     EtherNet/IP-1
3306/tcp  open     mysql
5060/tcp  filtered sip
```

- 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

FOSDEM'17

Command: nmap -T4 -A -v fosdem.org

Nmap Output | Ports / Hosts | Topology | Host Details | Sc

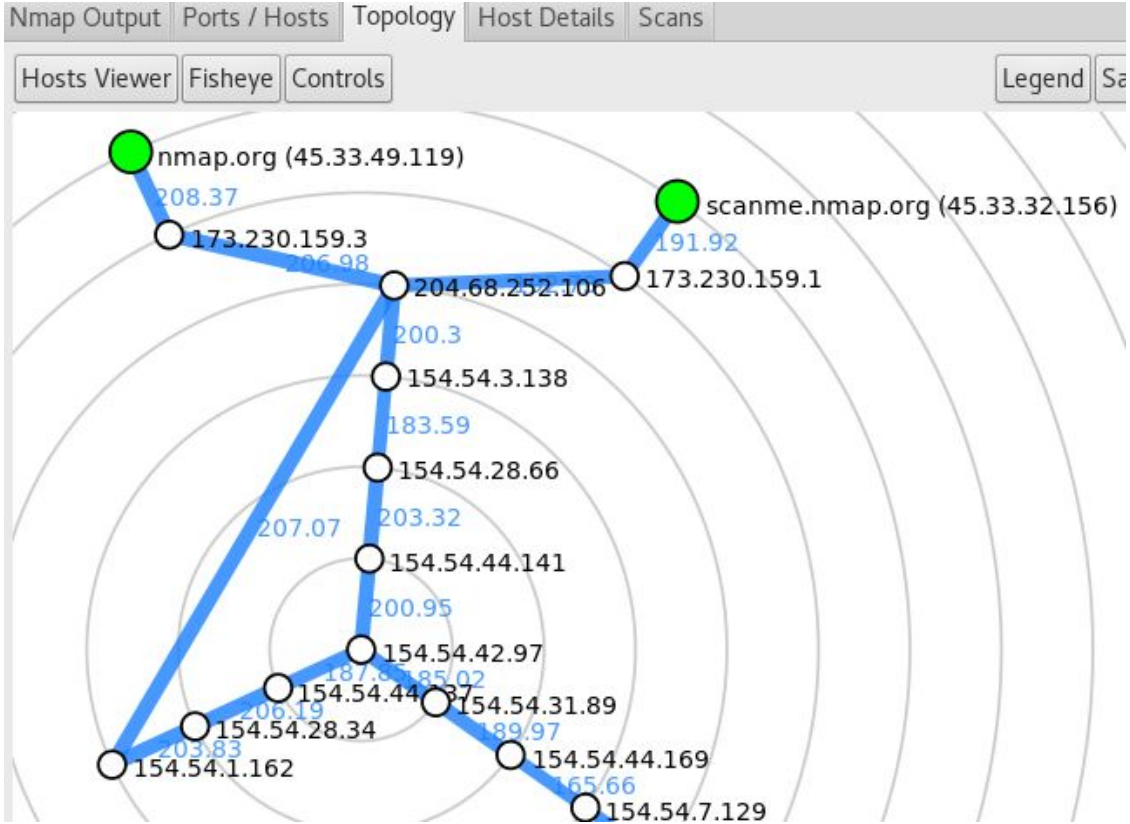
nmap -T4 -A -v fosdem.org

873	tcp	open	rsync	(protocol version 31)
443	tcp	open	http	nginx 1.10.1
80	tcp	open	http	nginx 1.10.1
22	tcp	open	ssh	OpenSSH 7.2 (FreeBSD 20160310; protoco

```
rDNS record for 31.22.22.135: www-public.fosdem.
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2 (FreeBSD 20160310; protocol 2.0)
| ssh-hostkey:
|   1024 67:69:58:d6:66:b9:fd:75:2e:d5:b6:06:d8:9b:55:9e (DSA)
|   2048 4a:b5:b2:82:d6:ce:f3:8c:c5:39:dd:42:19:07:37:2a (RSA)
|_  256 c0:34:55:3c:dd:0c:f2:8f:4c:83:45:ea:d0:d3:9a:38 (ECDSA)
80/tcp   open  http     nginx 1.10.1
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: nginx/1.10.1
|_http-title: Did not follow redirect to https://fosdem.org/
443/tcp open  ssl/http nginx 1.10.1
|_http-favicon: Unknown favicon MD5: 5F4B3426BCF762E75D5D39FC1050B2BE
|_http-generator: nanoc
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.10.1
| http-title: FOSDEM 2017 - Home
|_Requested resource was https://fosdem.org/2017/
| ssl-cert: Subject: commonName=*.fosdem.org
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/
organizationName=COMODO CA Limited/stateOrProvinceName=Greater
```

Zenmap Port Scanner

FOSDEM'17



Sparta

FOSDEM'17

SPARTA 1.0.2 (BETA) - untitled - /root/

File Help

Scan Brute

Hosts Services Tools

OS	Host
?	31.22.22.135 (fosde...

fosdem.org

Services Scripts Information Notes nikto (80/tcp) nikto (443/tcp) screenshot (80/tcp)

Port	Protocol	State	Name	Version
22	tcp	open	ssh	OpenSSH 7.2 (FreeBSD 20160310; protocol 2.0)
80	tcp	open	http	nginx 1.10.1
443	tcp	open	http	nginx 1.10.1

Log

Progress	Tool	Host	Start time	End time	Status
	nmap (stage 4)	fosdem.org	29 Jan 2017 09:23:42		Running
	nmap (stage 3)	fosdem.org	29 Jan 2017 09:22:00	29 Jan 2017 09:23:42	Finished

Nmap whois

FOSDEM'17

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
873/tcp  open  rsync

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

FOSDEM'17

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

```
                script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
```

```
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
873/tcp open  rsync
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X|9.X|7.X|10.X|8.X (95%), OpenBSD 4.X (94%), Linux 2.6.X (
.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.3 cpe:/o:openbsd:openbsd:4.0 cpe:/o:freebsd:freebsd:9.0 cpe:
bsd:7.0 cpe:/o:freebsd:freebsd:10 cpe:/o:freebsd:freebsd:8.0 cpe:/o:linux:linux_kernel:2.6 cp
1
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%), FreeBS
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

FOSDEM'17

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

FOSDEM'17

usr/local/share/nmap/scripts

```
/usr/share/nmap/scripts/ike-version.nse
/usr/share/nmap/scripts/http-put.nse
/usr/share/nmap/scripts/dns-check-zone.nse
/usr/share/nmap/scripts/http-vuln-cve2010-2861.nse
/usr/share/nmap/scripts/hbase-region-info.nse
/usr/share/nmap/scripts/snmp-info.nse
/usr/share/nmap/scripts/http-vuln-cve2012-1823.nse
/usr/share/nmap/scripts/jdwp-info.nse
/usr/share/nmap/scripts/targets-ipv6-multicast-mld.nse
/usr/share/nmap/scripts/http-useragent-tester.nse
/usr/share/nmap/scripts/smb-vuln-conficker.nse
/usr/share/nmap/scripts/upnp-info.nse
/usr/share/nmap/scripts/whois-domain.nse
/usr/share/nmap/scripts/http-svn-enum.nse
/usr/share/nmap/scripts/icap-info.nse
/usr/share/nmap/scripts/nfs-statfs.nse
/usr/share/nmap/scripts/hnap-info.nse
/usr/share/nmap/scripts/ipidseq.nse
/usr/share/nmap/scripts/stun-version.nse
/usr/share/nmap/scripts/broadcast-avahi-dos.nse
/usr/share/nmap/scripts/krb5-enum-users.nse
/usr/share/nmap/scripts/broadcast-netbios-master-browser.nse
/usr/share/nmap/scripts/mysql-query.nse
/usr/share/nmap/scripts/http-csrf.nse
/usr/share/nmap/scripts/mrinfo.nse
/usr/share/nmap/scripts/lexmark-config.nse
/usr/share/nmap/scripts/imap-capabilities.nse
/usr/share/nmap/scripts/http-sql-injection.nse
/usr/share/nmap/scripts/http-backup-finder.nse
/usr/share/nmap/scripts/openvas-otp-brute.nse
/usr/share/nmap/scripts/traceroute-geolocation.nse
/usr/share/nmap/scripts/snmp-win32-users.nse
/usr/share/nmap/scripts/http-vuln-cve2015-1427.nse
```

Nmap Script Engine

FOSDEM'17

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

http-trace.nse	Merge 6.x and 7.x scripts into a new folder
http-trendnet-tvip110w.nse	Merge 6.x and 7.x scripts into a new folder
http-vuln-cve2012-1823.nse	Merge 6.x and 7.x scripts into a new folder
http-vuln-cve2013-0156.nse	Merge 6.x and 7.x scripts into a new folder
http-vuln-cve2015-1635.nse	Merge 6.x and 7.x scripts into a new folder
http-waf-detect.nse	Merge 6.x and 7.x scripts into a new folder
http-wordpress-brute.nse	Merge 6.x and 7.x scripts into a new folder
http-wordpress-enum.nse	Merge 6.x and 7.x scripts into a new folder
huawei5xx-udp-info.nse	Merge 6.x and 7.x scripts into a new folder
mikrotik-routeros-brute.nse	Merge 6.x and 7.x scripts into a new folder
mysql-vuln-cve2012-2122.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-conficker.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-cve2009-3103.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-ms06-025.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-ms07-029.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-ms08-067.nse	Merge 6.x and 7.x scripts into a new folder
smb-vuln-regsvc-dos.nse	Merge 6.x and 7.x scripts into a new folder
smtp-dovecot-exim-exec.nse	Merge 6.x and 7.x scripts into a new folder
vulscan.nse	Merge 6.x and 7.x scripts into a new folder

Banner grabbing with nmap script

FOSDEM'17

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
PORT    STATE SERVICE
22/tcp  open  ssh
|_banner: SSH-2.0-OpenSSH_7.2 FreeBSD-20160310
80/tcp  open  http
443/tcp open  https
873/tcp open  rsync
|_banner: @RSYNCD: 31.0
```

http-enum script

FOSDEM'17

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

```
NSE: Script scanning 31.22.22.135.
Initiating NSE at 16:31
Completed NSE at 16:32, 31.03s elapsed
Nmap scan report for fosdem.org (31.22.22.135)
Host is up (0.060s 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
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp open  https
| http-enum:
|_  /atom.xml: RSS or Atom feed
873/tcp open  rsync

NSE: Script Post-scanning.
Initiating NSE at 16:32
Completed NSE at 16:32, 0.00s elapsed
```

↘ mysql-databases

FOSDEM'17

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

```
PORT     STATE SERVICE REASON
3306/tcp open  mysql   syn-ack
| mysql-databases:
|   information_schema
|   dvwa
|   metasploit
|   mysql
|   owasp10
|   tikiwiki
|_  tikiwiki195
```

↘ mysql-databases

FOSDEM'17

```
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
```

Find vulnerabilities with nmap

FOSDEM'17

- XSS / SQL Injection

↘ nmap -p80 –script **http-unsafe-output-escaping** <target>

↘ http://svn.dd-wrt.com/browser/src/router/nmap/scripts/http-unsafe-output-escaping.nse?rev=28293

↘ https://nmap.org/nsedoc/scripts/http-unsafe-output-escaping.html

Vulnerability Scanner

Nessus Vulnerability Scanner

FOSDEM'17

Nessus | Scans | Policies | jmoc

wordpress.com

CURRENT RESULTS: TODAY AT 11:35 AM

Configure | Audit Trail | Launch | Export | Filter Vulnerabilities

Hosts > wordpress.com > Vulnerabilities 23

Severity	Plugin Name	Plugin Family	Count
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
LOW	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
INFO	Service Detection	Service detection	3
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Nessus SYN scanner	Port scanners	2
INFO	Web Server No 404 Error Code Check	Web Servers	2

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

Arachni Vulnerability Scanner

FOSDEM'17

http://testhtml5.vulnweb.com/

Edit description

Scanning

Currently auditing:
- http://testhtml5.vulnweb.com/#/contact

Pages discovered	124	Requests performed	10157	Requests per second	79.87011317915239	Request concurrency	20
Running for	00:02:18	Responses received	9673	Timed out requests	0	Response times	0.295 s

Issues [13]

Issues may be missing some context while the scan is running.
You better wait until the scan is over to review them as the meta-analyses phase will flag probable false-positives and other untrusted issues accordingly.

All [13] | Fixed [0] | Verified [0] | Pending verification [0] | False positives [0] | Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset | Show all | Hide all

- High 6
- Medium 2
- Low 1
- Informational 6

NAVIGATE TO

- Cross-Site Scripting (XSS) 3
- DOM-based Cross-Site Scripting (XSS) 1
- Cross-Site Request Forgery 1
- Unencrypted password form 1
- Common directory 1
- Password field with auto-complete 1
- Allowed HTTP methods 1
- Interesting response 4

URL	Input	Element
Cross-Site Scripting (XSS) 3		
Client-side code (like JavaScript) can be injected into the web application which is then returned to the user's browser. This can lead to a compromise of the client's system or serve as a pivoting point for other attacks. (CWE)		
http://testhtml5.vulnweb.com/like	id	Link
http://testhtml5.vulnweb.com/comment	id	Link
http://testhtml5.vulnweb.com/report	id	Link
DOM-based Cross-Site Scripting (XSS) 1		
Client-side code (like JavaScript) can be injected into the web application which is then returned to the user's browser. This can lead to a compromise of the client's system or serve as a pivoting point for other attacks. (CWE)		
http://testhtml5.vulnweb.com/	url	Link_dom
Cross-Site Request Forgery 1		
The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. This is due to a lack of secure anti-CSRF tokens to verify the freshness of the submitted data. (CWE)		
http://testhtml5.vulnweb.com/contact		Form
Unencrypted password form 1		
Transmission of password does not use an encrypted channel. (CWE)		
http://testhtml5.vulnweb.com/login	password	Form

Linux

You can download self-contai

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

Attention: *The packages need GLIBC >= 2.12, if you g*

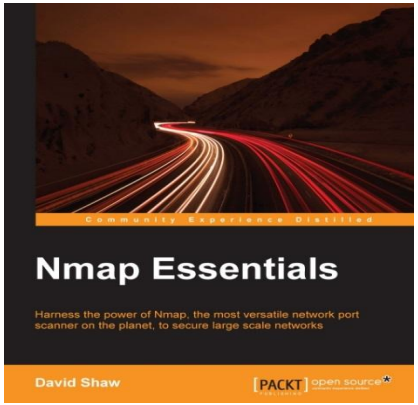
Links & References

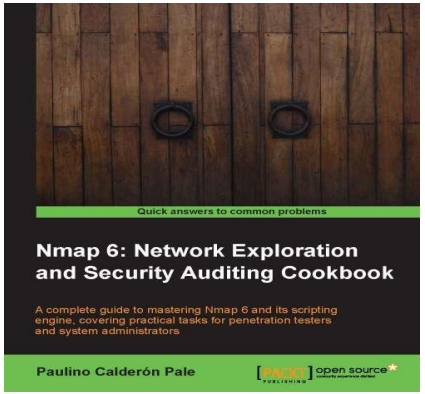
FOSDEM'17

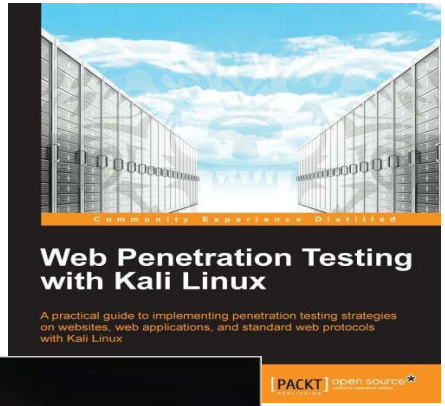
- http://www.0daysecurity.com/penetration-testing/network-footprinting.html
- http://nmap.org/nsedoc/
- https://secwiki.org/w/Nmap/External_Script_Library
- https://nmap.org/book/man-os-detection.html
- https://hackertarget.com/7-nmap-nse-scripts-recon/

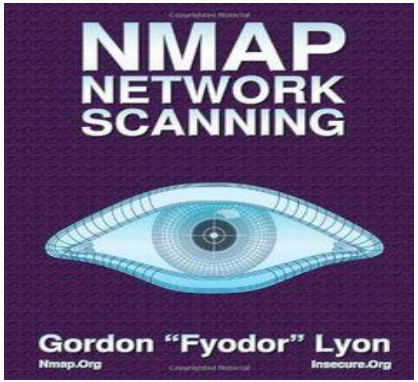
Books

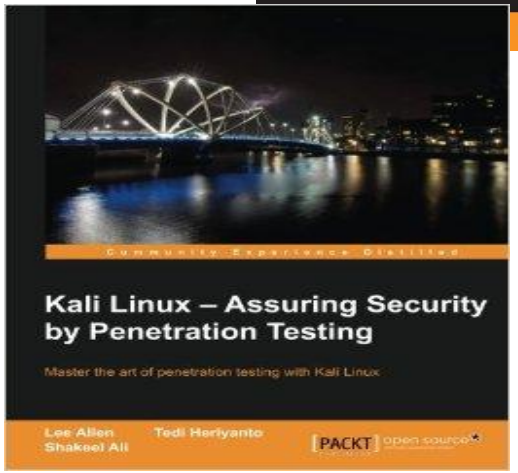
FOSDEM'17











Thank you!

Jose Manuel Ortega
@jmortegac