

## *3. Como acontecem os Ataques*

# QUAL O PERFIL ATACANTE?



# QUAL O PERFIL ATACANTE?

## ■ Quem pode ser uma ameaça?

- É necessário identificar quem pode atacar a minha rede, e qual a capacidade e/ou objetivo desta pessoa.

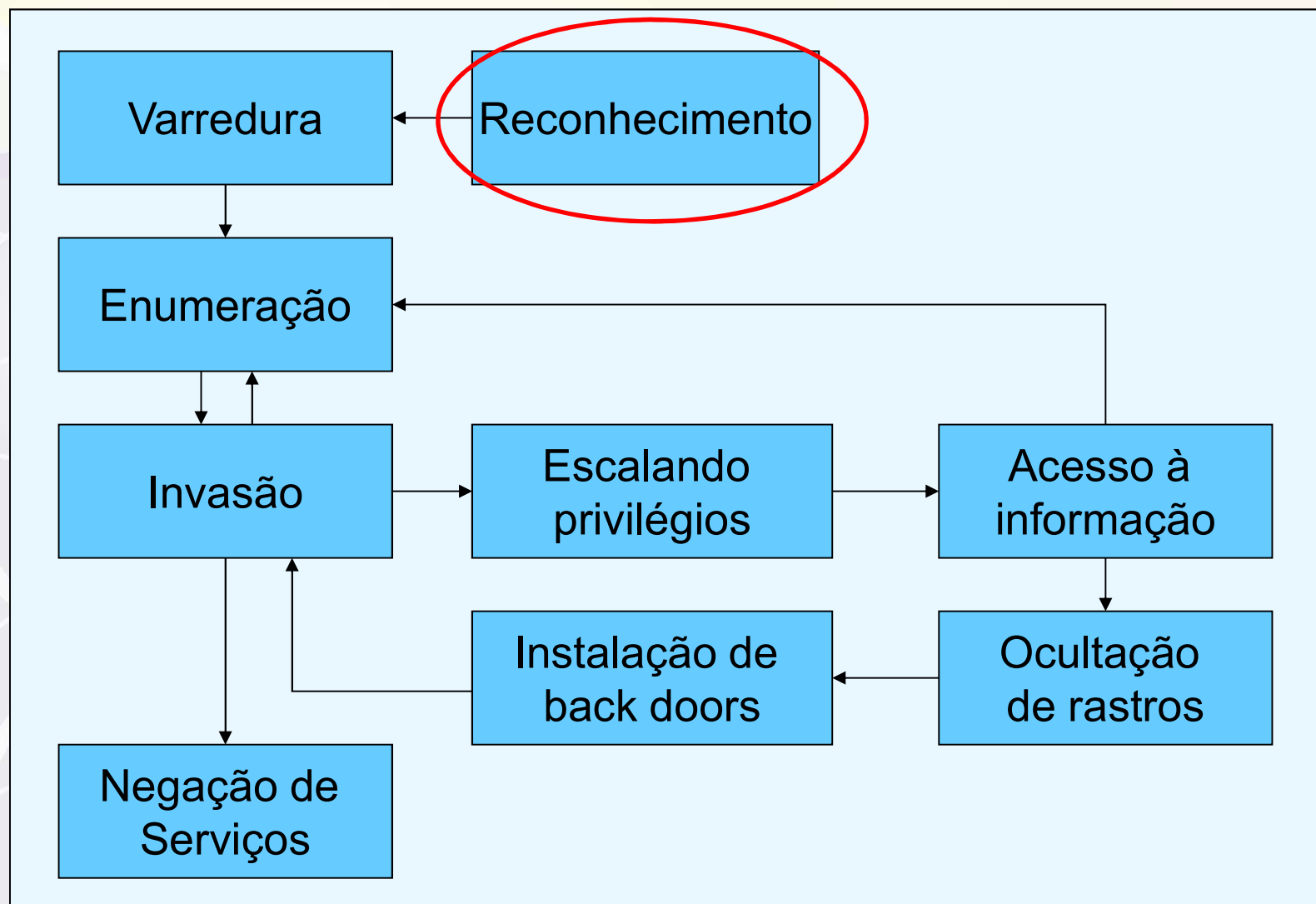
## ■ Perfil Atacante:

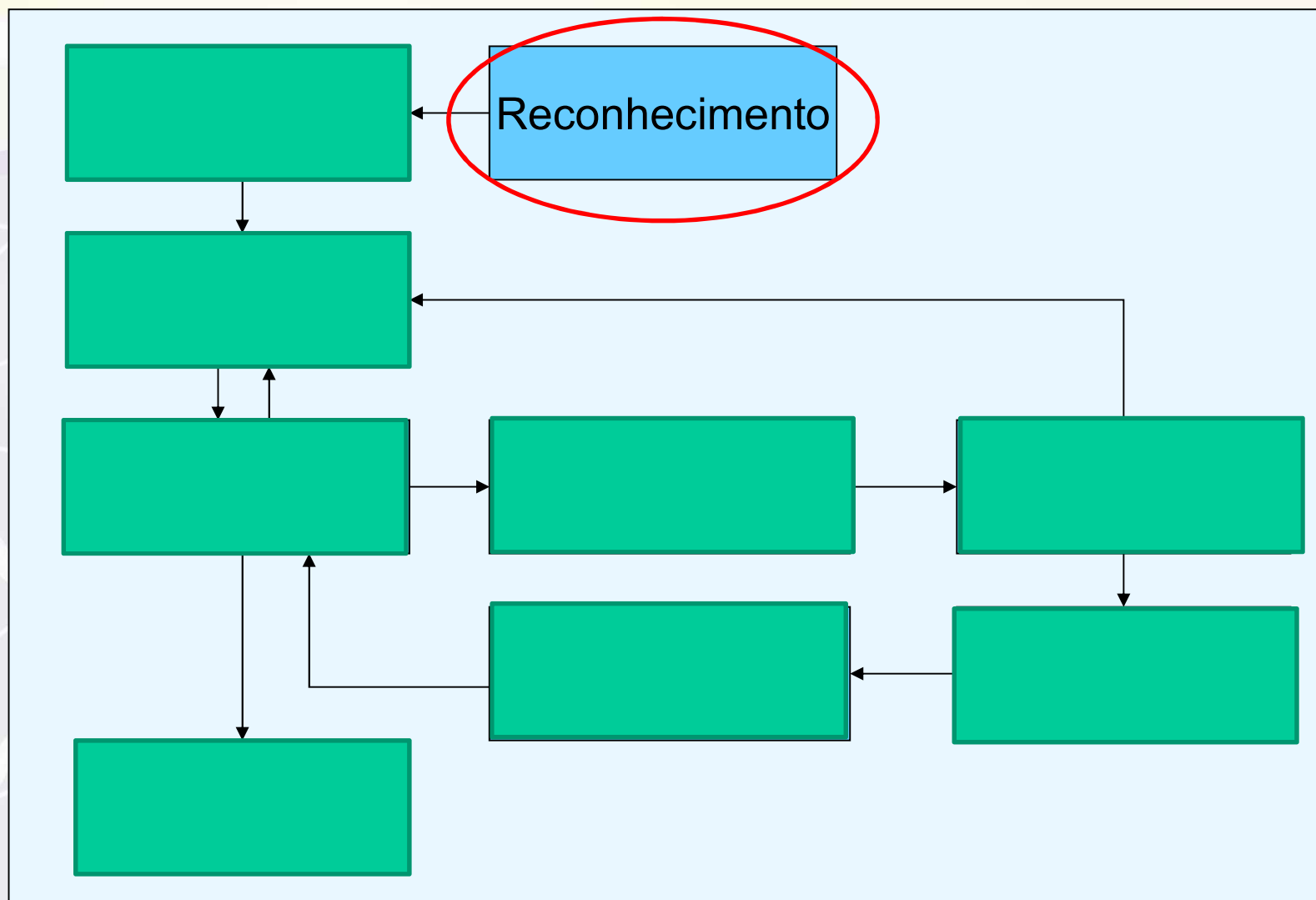
- **Principiante** – não tem nenhuma experiência em programação e usa ferramentas de terceiros. Geralmente não tem noção do que está fazendo ou das consequências daquele ato;
- **Intermediário** – tem algum conhecimento de programação e utiliza ferramentas usadas por terceiros. Esta pessoa pode querer algo além de testar um “Programinha Hacker”;
- **Avançado** – Programadores experientes, possuem conhecimento de Infraestrutura e Protocolos. Podem realizar ataques estruturados. Certamente não estão só testando os seus programas.

# Como acontecem os ataques Cibernéticos?



# Como acontecem os ataques Cibernéticos? Quais Etapas?





# 1. Footprinting (reconhecimento)

- Busca detalhada de informações sobre o alvo para uma intrusão.
- É a organização de idéias como um todo, tentando criar o melhor e mais completo perfil do alvo a ser atacado.
- O intuito é criar um perfil de uma máquina-alvo, para descobrir falhas que possam ser exploradas a partir de configurações e senhas padrões.

# 1. Footprinting (reconhecimento)

- A partir do resultado do Footprint é que é traçada a estratégia de ataque.
- Um Footprint dura o tempo que for necessário.
- Pode ser colocado em prática de muitas formas, e é limitado apenas pela imaginação do atacante.
- FingerPrint é a parte do Footprint que visa identificar o SO.



# 1. Footprinting (reconhecimento)

- Informações básicas podem indicar a postura e a política de segurança da empresa
- Coleta de informações essenciais para o ataque
  - ➔ Nomes de máquinas, nomes de login, faixas de IP, nomes de domínios, protocolos, sistemas de detecção de intrusão
- São usadas ferramentas comuns da rede
- Engenharia Social
  - ➔ Qual o e-mail de fulano?
  - ➔ Aqui é Cicrano. Poderia mudar minha senha?
  - ➔ Qual o número IP do servidor SSH? e o DNS?

# 1. Footprinting (reconhecimento)

- Consulta na Base Whois(Internic):  
→ Whois <domínio>
- Pesquisa registro.br  
→ (basedopaís) - <https://registro.br/>

# 1. Footprinting (reconhecimento)

## ■ Comando **dig**:

```
root@debianaula:~# dig ifpb.edu.br

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> ifpb.edu.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13662
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ifpb.edu.br.                IN      A

;; ANSWER SECTION:
ifpb.edu.br.                 600     IN      A      200.129.77.237

;; Query time: 137 msec
;; SERVER: 181.213.132.2#53(181.213.132.2)
;; WHEN: Mon Aug 29 16:31:09 -03 2022
;; MSG SIZE rcvd: 56
```

# 1. Footprinting (reconhecimento)

## ■ Comando **nslookup**:

```
root@debianaula:~# nslookup -q=ns ifpb.edu.br
Server:                181.213.132.2
Address:               181.213.132.2#53

Non-authoritative answer:
ifpb.edu.br           nameserver = ns2.ifpb.edu.br.
ifpb.edu.br           nameserver = ns3.ifpb.edu.br.
ifpb.edu.br           nameserver = ns4.ifpb.edu.br.
ifpb.edu.br           nameserver = ns1.ifpb.edu.br.

Authoritative answers can be found from:
```

# 1. Footprinting (reconhecimento)

## ■ Comando **host**:

```
root@debianaula:~# host pbagora.com.br
pbagora.com.br has address 104.26.2.89
pbagora.com.br has address 172.67.75.81
pbagora.com.br has address 104.26.3.89
pbagora.com.br has IPv6 address 2606:4700:20::681a:259
pbagora.com.br has IPv6 address 2606:4700:20::ac43:4b51
pbagora.com.br has IPv6 address 2606:4700:20::681a:359
pbagora.com.br mail is handled by 1 aspmx.1.google.com.
pbagora.com.br mail is handled by 5 alt2.aspmx.1.google.com.
pbagora.com.br mail is handled by 10 alt4.aspmx.1.google.com.
pbagora.com.br mail is handled by 10 alt3.aspmx.1.google.com.
pbagora.com.br mail is handled by 5 alt1.aspmx.1.google.com.
```

# Anatomia de um ataque

## 2. Scanning (Varredura ou Mapeamento)

- De posse das informações coletadas, determinar
  - Quais sistemas estão ativos e alcançáveis
  - Portas de entrada ativas em cada sistema
- Ferramentas
  - Nmap, system banners, informações via SNMP
- Descoberta da Topologia
  - Automated discovery tools: cheops, ntop, ...
  - Comandos usuais: ping, traceroute, nslookup
- Detecção de Sistema Operacional
  - Técnicas de fingerprint (nmap – [www.nmap.org](http://www.nmap.org))



## 2. Scanning (varredura ou mapeamento)

### Site do NMAP



NMAP.ORG

#### Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

#### Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

#### Security Tools



#### Downloading Nmap

Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older version (and sometimes newer test releases) are available from the [dist directory](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sigs directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the new book [Nmap Network Scanning](#)!



## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap

Scan Tools Perfil Ajuda

Alvo:


Perfil:


Comando:

Hosts

Services

OS Host

 www.ponto-r.com.

 www.ifsertao-pe.ec

Saída do Nmap

Ports / Hosts

Topology

Detalhes da Máquina

Scans

nmap -T4 -A -v www.ifsertao-pe.edu.br

Starting Nmap 7.40 ( <https://nmap.org> ) at 2017-03-05 10:04 Hora oficial do Brasil

**NSE:** Loaded 143 scripts for scanning.

**NSE:** Script Pre-scanning.

Initiating NSE at 10:04

Completed NSE at 10:04, 0.00s elapsed

Initiating NSE at 10:04

Completed NSE at 10:04, 0.00s elapsed

Initiating Ping Scan at 10:04

Scanning [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62) [4 ports]

Completed Ping Scan at 10:04, 0.80s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 10:04

Completed Parallel DNS resolution of 1 host. at 10:04, 0.47s elapsed

Initiating SYN Stealth Scan at 10:04

Scanning [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62) [1000 ports]

Discovered open port 443/tcp on 200.133.4.62

Discovered open port 21/tcp on 200.133.4.62

Discovered open port 80/tcp on 200.133.4.62

Discovered open port 8008/tcp on 200.133.4.62

Completed SYN Stealth Scan at 10:04, 17.21s elapsed (1000 total ports)

Initiating Service scan at 10:04

Scanning 4 services on [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62)

Completed Service scan at 10:05, 13.33s elapsed (4 services on 1 host)

Initiating OS detection (try #1) against [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62)

Retrying OS detection (try #2) against [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62)

Initiating Traceroute at 10:05

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap

Scan Tools Perfil Ajuda

Alvo:  Perfil:

Comando:

Hosts Services

OS Host

- www.ponto-r.com.
- www.ifsertao-pe.ec

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

nmap -T4 -A -v www.ifsertao-pe.edu.br

Completed NSE at 10:05, 10.31s elapsed  
Initiating NSE at 10:05  
Completed NSE at 10:05, 0.00s elapsed  
Nmap scan report for [www.ifsertao-pe.edu.br](http://www.ifsertao-pe.edu.br) (200.133.4.62)  
Host is up (0.19s latency).  
**Not shown:** 993 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD
80/tcp	open	http	Apache httpd

|\_http-favicon: Unknown favicon MD5: 7AC9958848DF8333BA0DF0D5BFFB2724  
|\_http-methods:  
|\_ Supported Methods: GET HEAD POST OPTIONS  
|\_ http-robots.txt: 15 disallowed entries  
|\_ /joomla/administrator/ /administrator/ /bin/ /cache/  
|\_ /cli/ /components/ /includes/ /installation/ /language/  
|\_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/  
|\_http-server-header: Apache  
|\_http-title: Instituto Federal do Sertão Pernambuco

113/tcp closed ident  
443/tcp open ssl/http Apache httpd

|\_http-methods:  
|\_ Supported Methods: GET HEAD POST OPTIONS  
|\_ http-robots.txt: 15 disallowed entries  
|\_ /joomla/administrator/ /administrator/ /bin/ /cache/  
|\_ /cli/ /components/ /includes/ /installation/ /language/  
|\_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/



## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap

Scan Tools Perfil Ajuda

Alvo:  Perfil:

Comando:

Hosts Services

OS Host

- www.ponto-r.com.
- www.ifsertao-pe.edu.br

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

nmap -T4 -A -v www.ifsertao-pe.edu.br

```
|_http-server-header: Apache
|_http-title: Instituto Federal do Sertão Pernambuco
|_ssl-cert: Subject: commonName=www.ifsertao-pe.edu.br/organizationName=INSTITUTO FEDERAL DE EDUC CIENCIA E TEC DO SERTAO PERNAMBUCANO/stateOrProvinceName=PE/countryName=BR
| Subject Alternative Name: DNS:www.ifsertao-pe.edu.br, DNS:ifsertao-pe.edu.br
| Issuer: commonName=ICPEdu/organizationName=Rede Nacional de Ensino e Pesquisa - RNP/stateOrProvinceName=Rio de Janeiro/countryName=BR
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-06-26T02:21:02
| Not valid after: 2019-06-27T02:21:02
| MD5: 154f 6f14 92b2 abcf d75b e780 53d3 0a13
|_SHA-1: 785b a210 c97e 0e11 fb7c d8cc 6a57 fb3f 8d62 aeb3
|_ssl-date: 2017-03-05T13:04:10+00:00; -1m15s from scanner time.
8008/tcp open http Fortinet FortiGuard block page
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www.ifsertao-pe.edu.br:8010/
9000/tcp closed cslistener
10000/tcp closed snet-sensor-mgmt
Device type: general purpose|specialized|firewall|router|WAP
Running (JUST GUESSING): Linux 2.6.X|2.4.X (90%), AVtech embedded (88%), Fortinet embedded (87%), Linksys embedded (87%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:fortinet:fortigate_1500d cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (90%), AVtech Room Alert 26W environmental monitor (88%), Fortinet FortiGate 1500D firewall (87%), Linksys BEFSR41 EtherFast router (87%), Fortinet FortiGate 100D firewall (86%), Tomato 1.27 - 1.28 (Linux 2.4.20) (85%), FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
```

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap



Scan Tools Perfil Ajuda

Alvo:  Perfil:

Comando:

Hosts Services

OS Host

-  www.ponto-r.com.
-  www.ifsertao-pe.ec

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

nmap -T4 -A -v www.ifsertao-pe.edu.br

No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 0.664 days (since Sat Mar 04 18:09:17 2017)  
Network Distance: 18 hops  
IP ID Sequence Generation: Randomized  
Service Info: Device: security-misc

Host script results:  
|\_clock-skew: mean: -1m15s, deviation: 0s, median: -1m15s

TRACEROUTE (using port 113/tcp)

HOP	RTT	ADDRESS
1	0.00 ms	192.168.0.1
2	0.00 ms	192.168.1.20
3	47.00 ms	192.0.0.254
4	47.00 ms	ip-168.196.53.129.redeatel.com.br (168.196.53.129)
5	...	6
7	78.00 ms	186-230-244-45.ded.intelignet.com.br (186.230.244.45)
8	93.00 ms	10.210.64.161
9	93.00 ms	10.239.255.173
10	93.00 ms	10.223.238.50
11	78.00 ms	as1916.riodejaneiro.rj.ix.br (200.219.138.101)
12	78.00 ms	sp2-rj-oi.bkb.rnp.br (200.143.253.221)
13	63.00 ms	sp-sp2.bkb.rnp.br (200.143.253.37)
14	110.00 ms	ce-sp-nau.bkb.rnp.br (200.143.253.25)
15	188.00 ms	pe-ce-tlbrs.bkb.rnp.br (200.143.253.106)
16	172.00 ms	lanpe-pe.bkb.rnp.br (200.143.255.194)

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

```
17 203.00 ms 200.133.31.218
18 219.00 ms www.ifsertao-pe.edu.br (200.133.4.62)
```

NSE: Script Post-scanning.

Initiating NSE at 10:05

Completed NSE at 10:05, 0.00s elapsed

Initiating NSE at 10:05

Completed NSE at 10:05, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 68.22 seconds

Raw packets sent: 2111 (96.544KB) | Rcvd: 69 (4.344KB)

Filter Hosts

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap

Scan Tools Perfil Ajuda

Alvo:  Perfil:

Comando:

Hosts Services

Service

- snet-sensor-mgmt
- smtp
- pop3
- mysql
- imap
- ident
- http
- ftp
- domain
- cslistener

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

Hostname	Port	Protocol	State	Version
www.ponto-r.com.br (67.23.234.191)	21	tcp	open	Pure-FTPd
www.ifsertao-pe.edu.br (200.133.4.62)	21	tcp	open	ProFTPD



## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Zenmap

Scan Tools Perfil Ajuda

Alvo:  Perfil:

Comando:

Hosts Services

Service

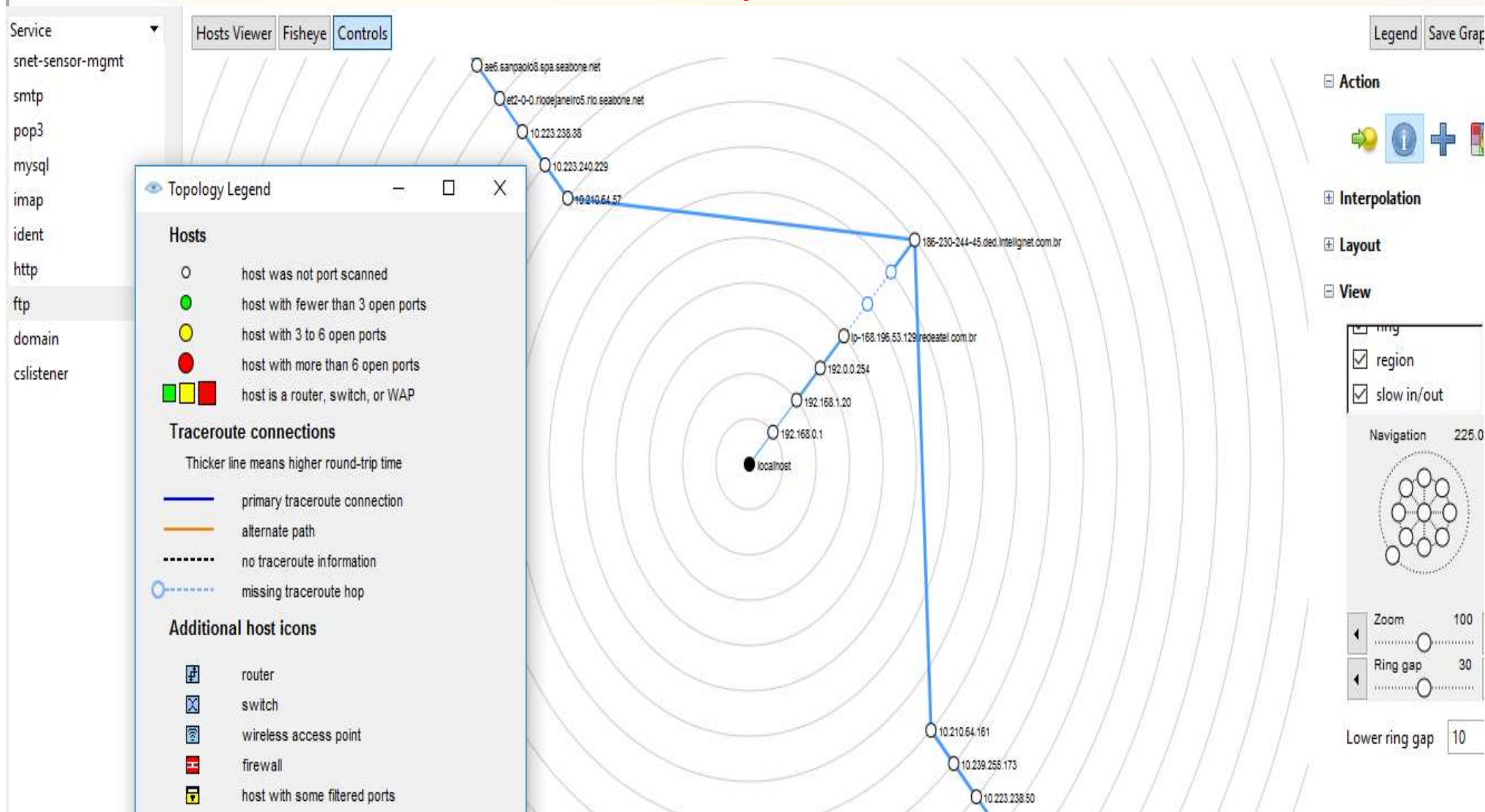
- snet-sensor-mgmt
- smtp
- pop3
- mysql
- imap
- ident
- http**
- ftp
- domain
- cslistener

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

Hostname	Port	Protocol	State	Version
www.ponto-r.com.br (67.23.234.191)	443	tcp	open	Apache httpd (PHP 5.5.38)
www.ponto-r.com.br (67.23.234.191)	80	tcp	open	Apache httpd
www.ifsertao-pe.edu.br (200.133.4.62)	80	tcp	open	Apache httpd
www.ifsertao-pe.edu.br (200.133.4.62)	443	tcp	open	Apache httpd
www.ifsertao-pe.edu.br (200.133.4.62)	8008	tcp	open	Fortinet FortiGuard block page

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows





## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Hosts Viewer

Hosts

www.ponto-r.com.br (67

www.ifsertao-pe.edu.br (

General Services Traceroute

TTL	RTT	IP	Hostname
1	0.00	192.168.0.1	
2	0.00	192.168.1.20	
3	47.00	192.0.0.254	
4	47.00	168.196.53.129	ip-168.196.53.129.redeatel.com.br
5		<unknown>	
6		<unknown>	
7	78.00	186.230.244.45	186-230-244-45.ded.intelignet.com.br
8	93.00	10.210.64.161	
9	93.00	10.239.255.173	
10	93.00	10.223.238.50	
11	78.00	200.219.138.101	as1916.riodejaneiro.rj.ix.br
12	78.00	200.143.253.221	sp2-rj-oi.bkb.rnp.br
13	63.00	200.143.253.37	sp-sp2.bkb.rnp.br
14	110.00	200.143.253.25	ce-sp-nau.bkb.rnp.br
15	188.00	200.143.253.106	pe-ce-tlbrs.bkb.rnp.br
16	172.00	200.143.255.194	lanpe-pe.bkb.rnp.br
17	203.00	200.133.31.218	
18	219.00	200.133.4.62	www.ifsertao-pe.edu.br

## 2. Scanning (varredura ou mapeamento)

### Interface NMAP para Windows

Comando: `nmap -T4 -A -v www.ifsertao-pe.edu.br`

Hosts Services

OS Host


- www.ponto-r.com.
- www.ifsertao-pe.ec

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

☒ www.ifsertao-pe.edu.br (200.133.4.62)


☒ **Status da Máquina**

Estado:	up
Open ports:	4
Portas Filtradas:	993
Portas Fechadas:	3
Portas analisadas:	1000
Tempo ligado:	57378
Última inicialização:	Sat Mar 04 18:09:17 2017



☒ **Endereços**

IPv4:	200.133.4.62
IPv6:	Indisponível
MAC:	Indisponível



☒ **Nomes das máquinas**

Nome - Tipo:	www.ifsertao-pe.edu.br - user
Nome - Tipo:	www.ifsertao-pe.edu.br - PTR

☒ **Sistema Operacional**

Nome:	Linux 2.6.18 - 2.6.22
Precisão:	<div><div>90%</div></div>

☒ **Portas usadas**

☒ **OS Classes**

## 2. Scanning (varredura ou mapeamento)

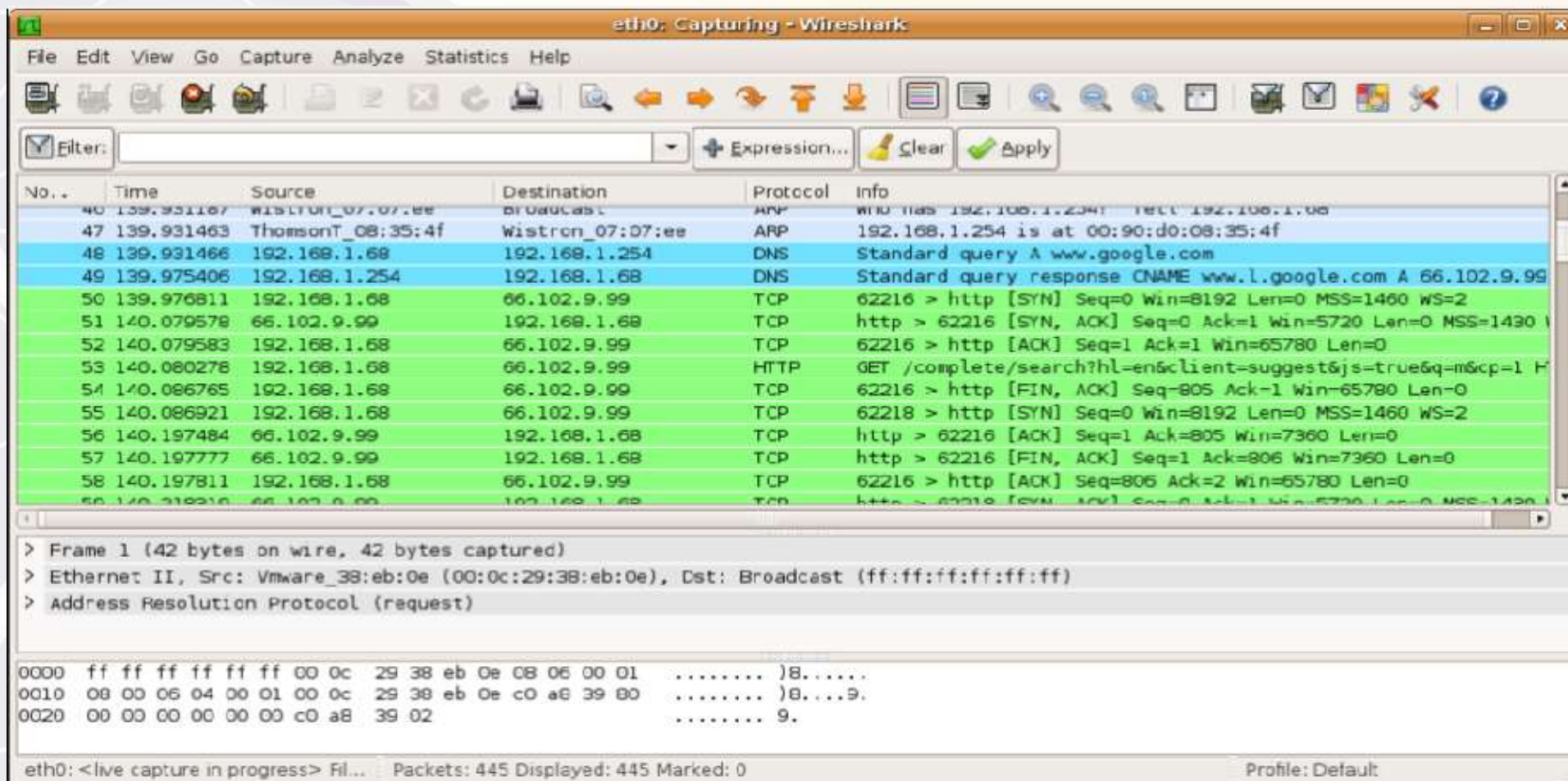
### NMAP fazendo varredura de rede

```
C:\Users\Paiva>nmap -sP 192.168.0.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-10 08:16 Hora oficial do Brasil
Nmap scan report for 192.168.0.1
Host is up (0.00s latency).
MAC Address: EC:08:6B:44:A5:E8 (Tp-link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.047s latency).
MAC Address: B8:5A:73:AB:D8:78 (Samsung Electronics)
Nmap scan report for 192.168.0.101
Host is up (0.047s latency).
MAC Address: 30:CB:F8:8E:59:9A (Samsung Electronics)
Nmap scan report for 192.168.0.103
Host is up (0.047s latency).
MAC Address: DC:53:60:0E:80:21 (Intel Corporate)
Nmap scan report for 192.168.0.102
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 16.95 seconds
```

## 2. Scanning (varredura ou mapeamento)

- Busca de senhas contidas em pacotes (sniffing)
  - ➔ Muitas das ferramentas são as mesmas usadas para gerenciamento e administração da rede



The screenshot shows the Wireshark interface with a live capture on the eth0 interface. The packet list pane displays several packets, including ARP requests, DNS queries, and HTTP traffic. The packet details pane shows the structure of the first packet (Frame 1), which is an Ethernet II frame with a broadcast destination and an ARP request payload. The packet bytes pane shows the raw hex and ASCII data of the first few bytes of the frame.

No.	Time	Source	Destination	Protocol	Info
40	139.931167	Wistron_07:07:ee	broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&sc=1 HTTP/1.1
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.218216	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1460

Frame 1 (42 bytes on wire, 42 bytes captured)  
 Ethernet II, Src: Vmware\_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01  ..... )8.....
0010  08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 00  ..... )8....9.
0020  00 00 00 00 00 00 c0 a8 39 02  ..... 9.
  
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default



# Mapeamento de rede

← → ↻ ↗ ⚠ Não seguro | cheops-ng.sourceforge.net/download.php



## Cheops-ng

"the network swiss army knife"

### Navigation

- Main
- Screenshots
- FAQ
- Download

### Links

- My Company
- Nmap

### Source Code

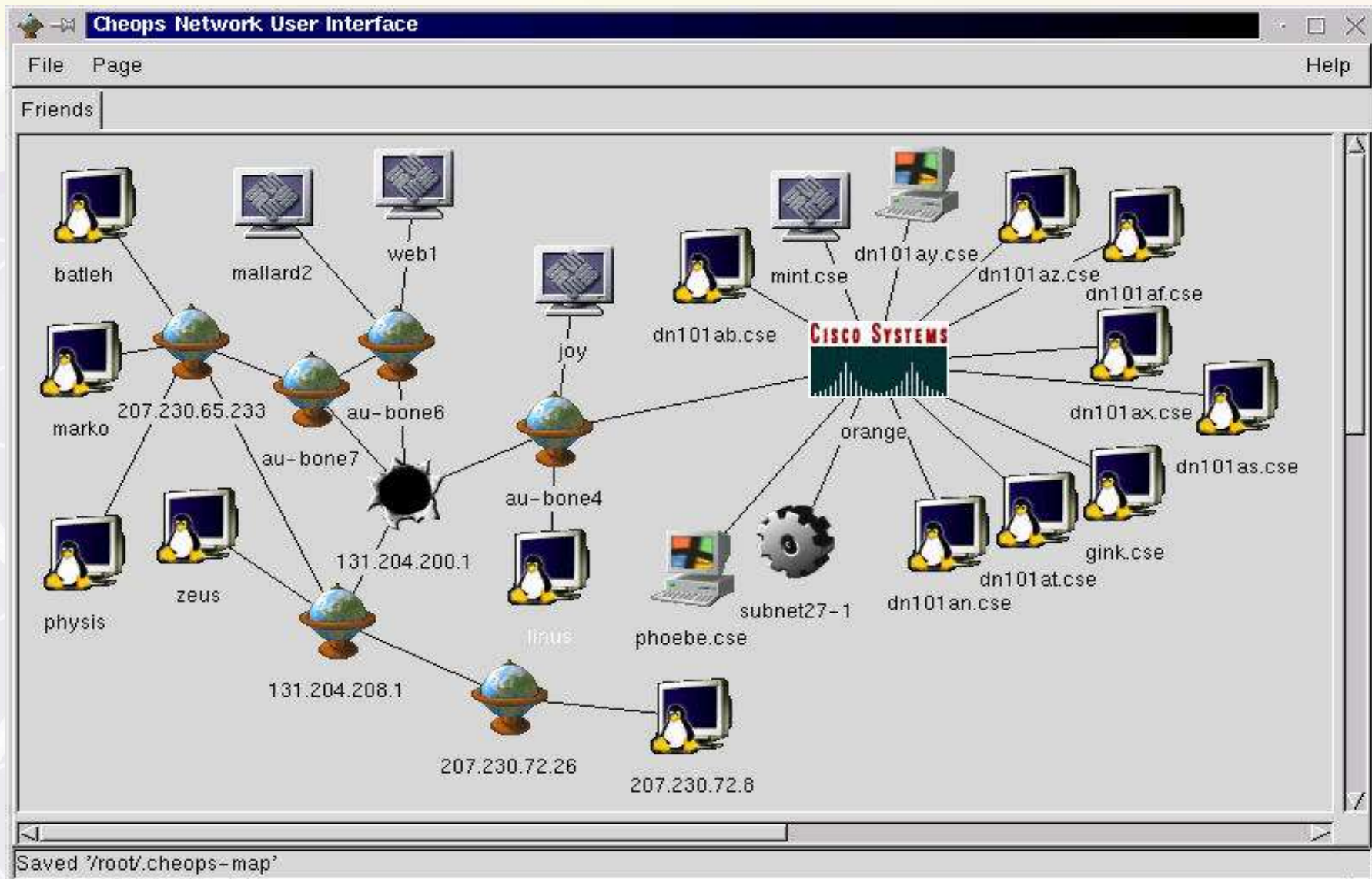
[FreeBSD Version](#)  
Current: 0.2.3  
[cvs/project](#) at sourceforge.net

### Requirements

- [nmap > 2.54BETA30](#)
- [gtk >= 1.2.0](#)
- [gnome](#)
- [gnome-xm1 >= 1.8.0](#)
- [glib >= 1.2.0](#)
- [glib-devel >= 1.2.0](#)

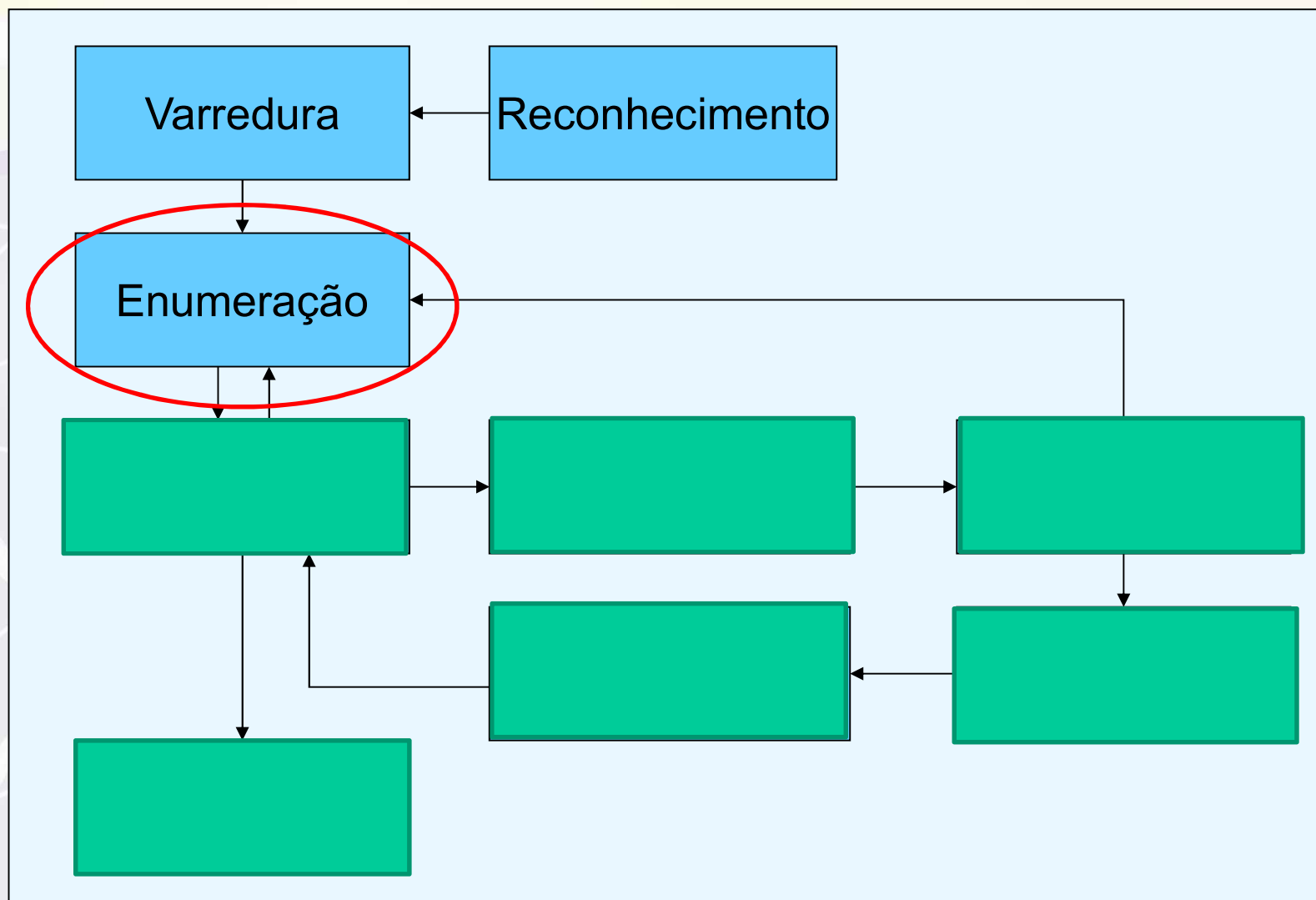
Tela do Cheops (<http://cheops-ng.sourceforge.net>)

# Mapeamento de rede



Tela do Cheops (<http://cheops-ng.sourceforge.net>)

# Anatomia de um ataque



### 3. Enumeration (enumeração)

- Extração de informações do ambiente-alvo, como os serviços de rede TCP e UDP, que requerem portas.
- Varreduras de Portas Clássicas:
  - TCP, UDP, ICMP.
- Port Scanners:
  - -NetStat(Windows)
  - -Netcat
  - -Nmap
  - -Amap(ideal para leitura de banners)
  - -Blaster-Hping2



### 3. Enumeration (enumeração)

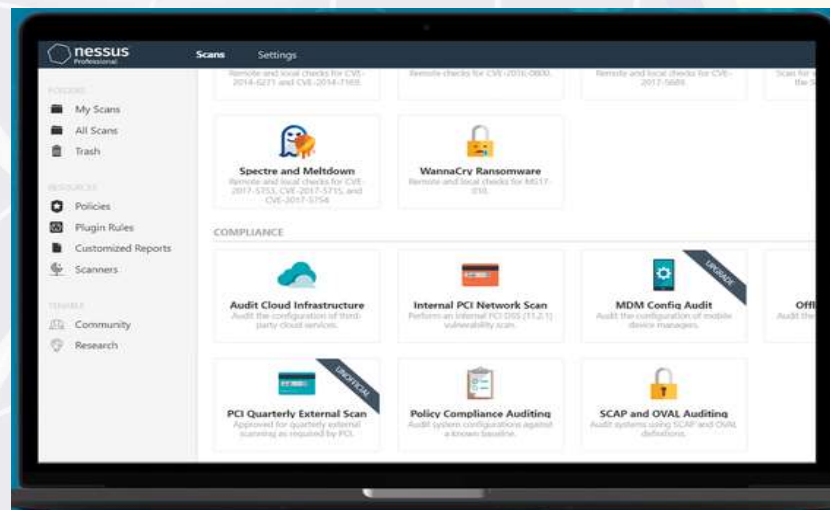
- Coleta de dados intrusiva
  - Consultas diretas ao sistema
  - Está conectado ao sistema e pode ser notado
- Identificação de logins válidos
- Banners identificam versões de HTTP, FTP servers
- Identificação de recursos da rede
  - Compartilhamentos (windows) - Comandos net view, nbtstat, openfiles, net
  - Exported filesystems (unix) - Comando showmount
- Identificação de permissões
- Identificação de Vulnerabilidades comuns – Ferramentas:
  - SATAN, Nessus, OpenVAS, SAINT, SARA, ...

### 3. Enumeration (enumeração)

■ **Nessus**



- **Nessus** é uma ferramenta amplamente usada por empresas e organizações para avaliar a segurança de seus sistemas e infraestrutura de rede.
- O software é capaz de verificar milhares de vulnerabilidades em uma ampla gama de sistemas operacionais e aplicativos, incluindo servidores, dispositivos de rede, bancos de dados e aplicativos web.

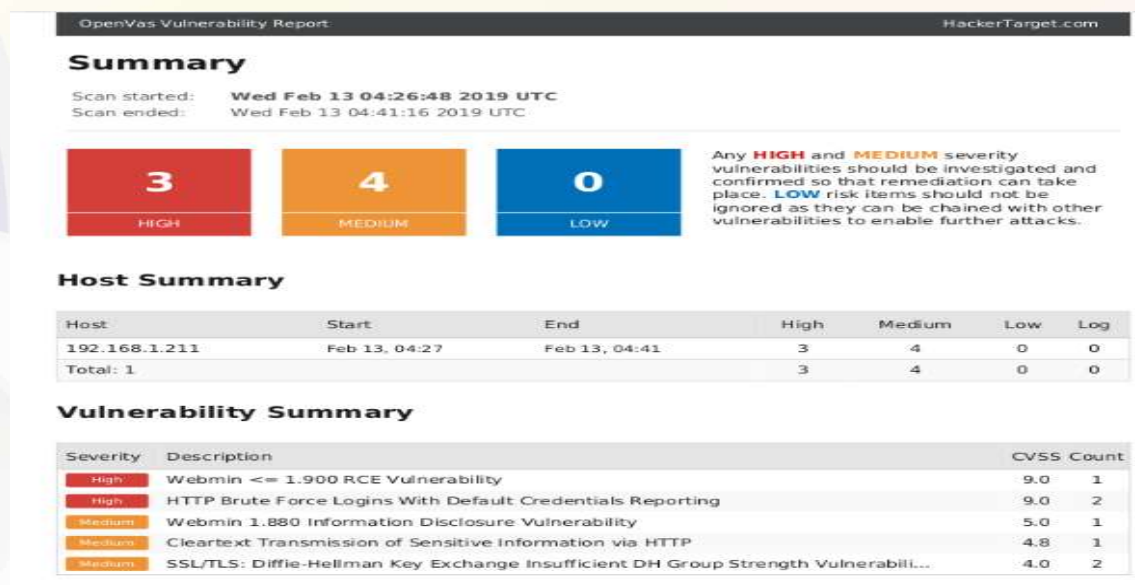


<https://pt-br.tenable.com/products/nessus>

# 3. Enumeration (enumeração)

## ■ OpenVAS

- O **OpenVAS** (Open Vulnerability Assessment System) é uma ferramenta de varredura de vulnerabilidades de código aberto usada para detectar vulnerabilidades em sistemas e aplicativos de rede. O OpenVAS é uma alternativa de código aberto ao Nessus, que é uma ferramenta de varredura de vulnerabilidades comercial. Ele usa uma variedade de técnicas para detectar vulnerabilidades, incluindo varreduras de portas, verificação de serviços em execução, identificação de vulnerabilidades conhecidas e testes de penetração automatizados.



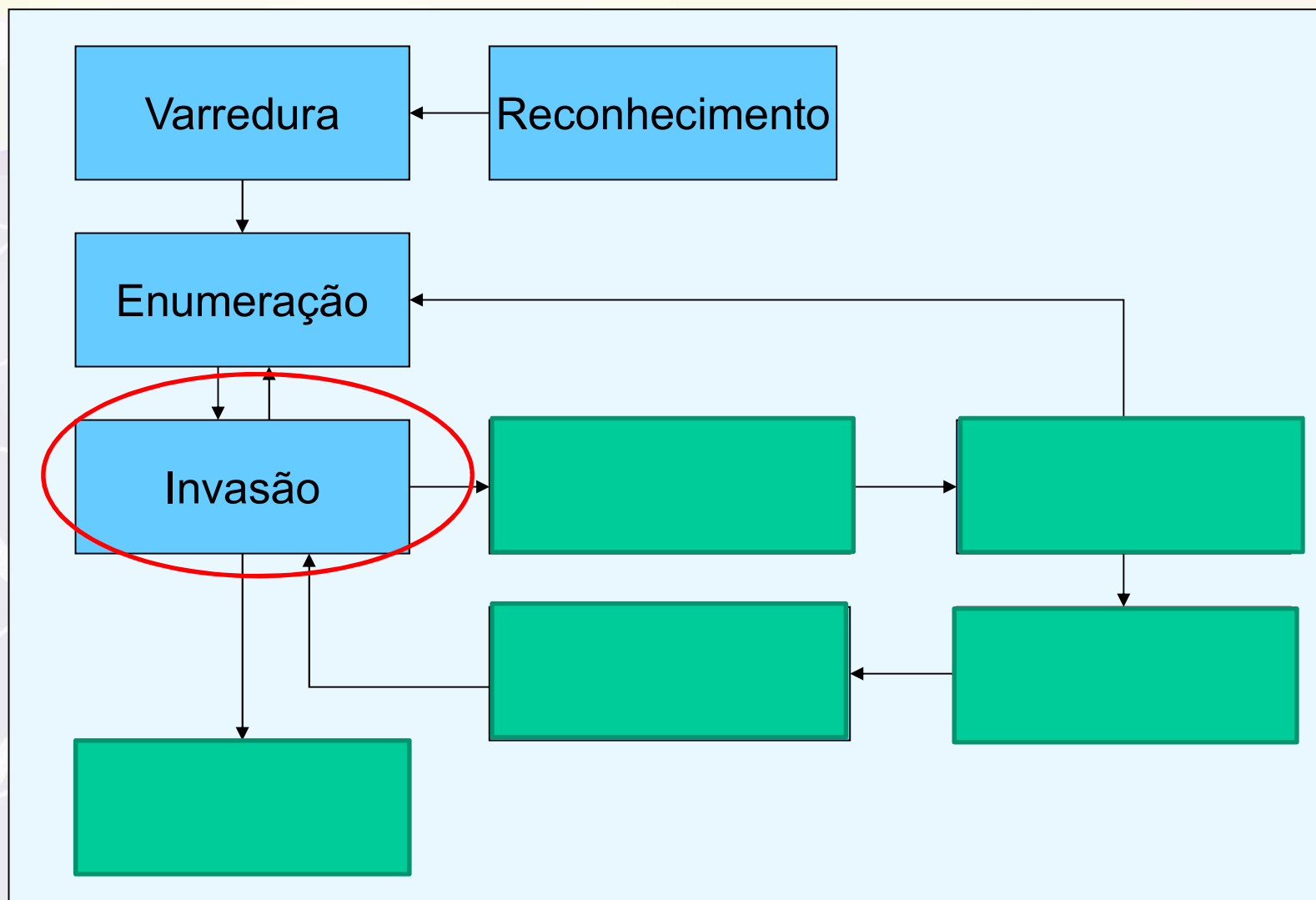
<https://www.openvas.org/>

### 3. Enumeration (enumeração)

#### ■ SAINT

- O **SAINT** Security Suite combina varredura de vulnerabilidade ativa, varredura de conteúdo, varredura de aplicativos da web, avaliações móveis, avaliações de firmware de dispositivo de rede, auditoria de configuração, teste de penetração, engenharia social e geração de relatórios em uma única solução totalmente integrada. Ele pode ser implantado por meio de download de software, dispositivo virtual, dispositivo de hardware pré-configurado ou como um serviço de nuvem.







## 4. Ganhando acesso (invasão)

- Ao determinar qual SO está rodando, o invasor pode organizar suas ferramentas de acordo com a plataforma-alvo;
- O invasor pode ter como objetivo, “rootear” a máquina-alvo, e deve sempre saber as diferenças dos formatos binários de cada sistema.

## 4. Ganhando acesso (invasão)

- Informações coletadas norteiam a estratégia de ataque
- Invasores tem uma “base” de vulnerabilidades
  - Bugs de cada SO, kernel, serviço, aplicativo – por versão
  - Tentam encontrar sistemas com falhas conhecidas
- Busca privilégio de usuário comum (pelo menos)
- Técnicas
  - Password sniffing, password crackers, password guessing (adivinhação)
  - Ferramentas para bugs conhecidos (buffer overflow)

## 4. Ganhando acesso (invasão)

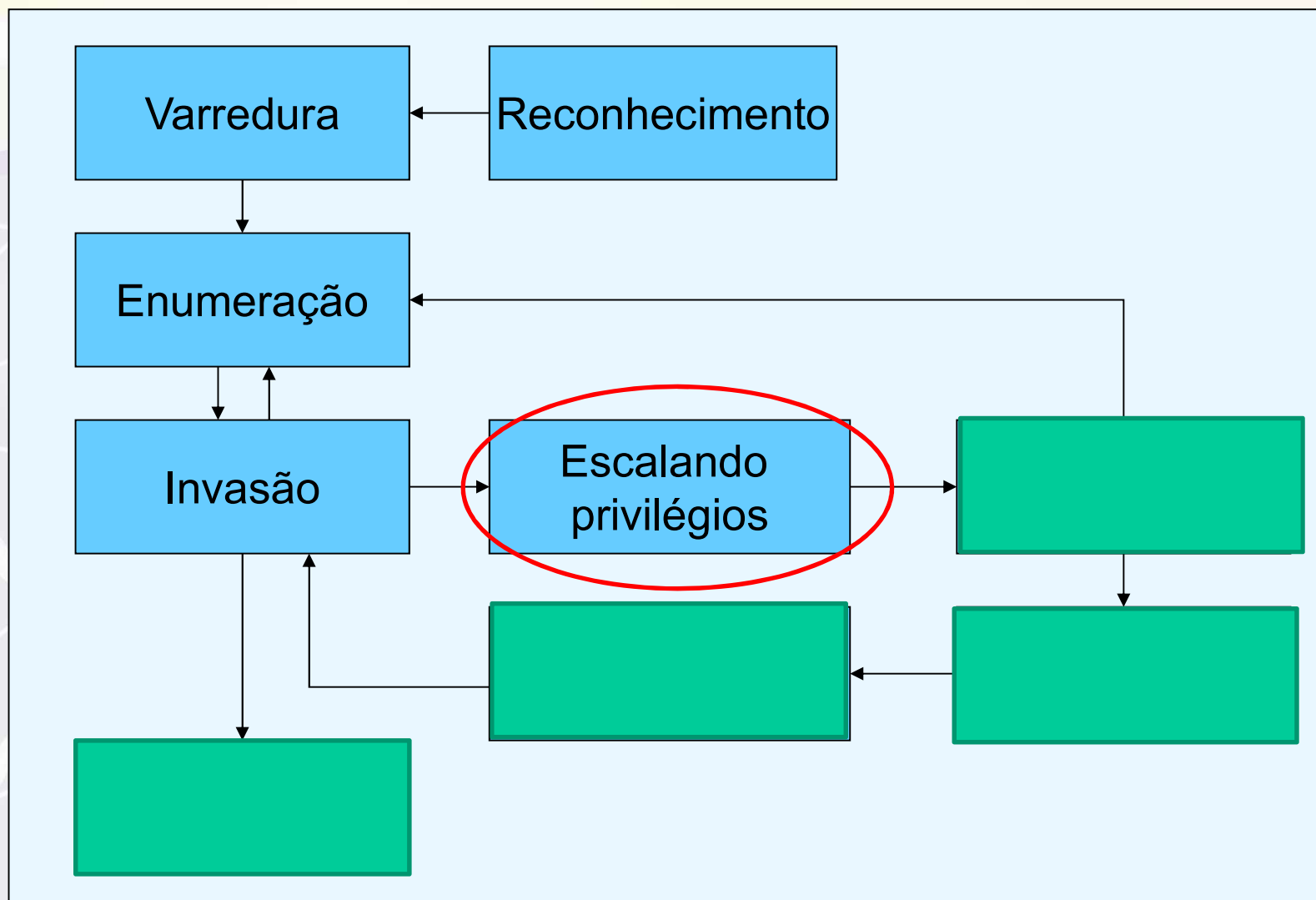
### ■ Técnicas

- ➔ Session hijacking (sequestro de sessão), também conhecido como "cookie hijacking" ou "cookie side-jacking", é uma técnica usada por hackers para roubar sessões de usuários autenticados em um site ou aplicação web.
- ➔ Essa técnica permite que o atacante assuma o controle da sessão de um usuário legítimo, obtendo acesso a informações sensíveis ou executando ações maliciosas em nome do usuário.

### ■ Hackers constróem suas próprias ferramentas



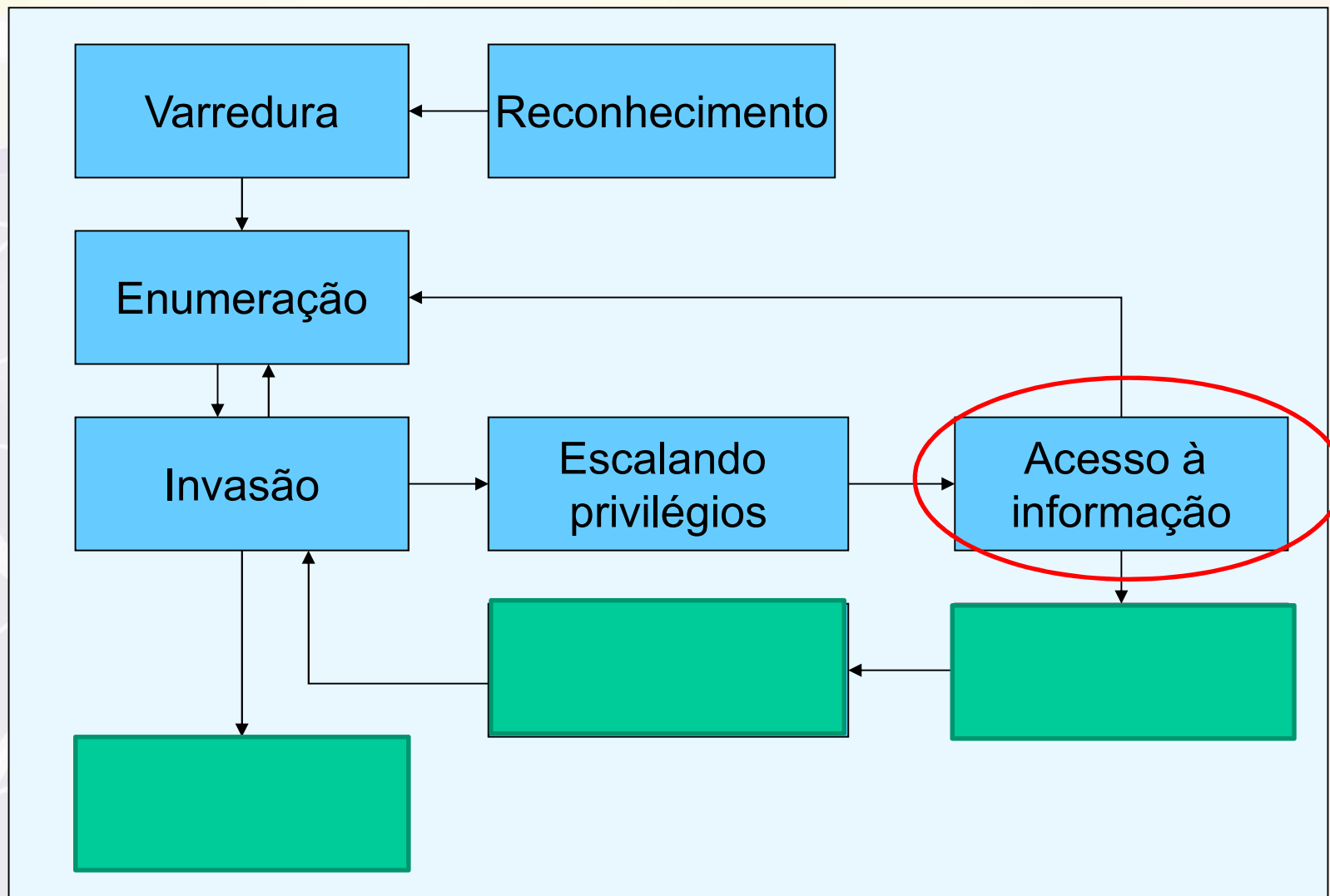
# Anatomia de um ataque



## 5. Escalada de privilégios

- Uma vez com acesso comum, busca acesso completo ao sistema (administrator, root)
- Ferramentas específicas para bugs conhecidos
  - "Exploits"
- Técnicas
  - Password sniffing, password crackers, password guessing
  - Session hijacking (sequestro de sessão)
  - Buffer overflow
  - Trojans

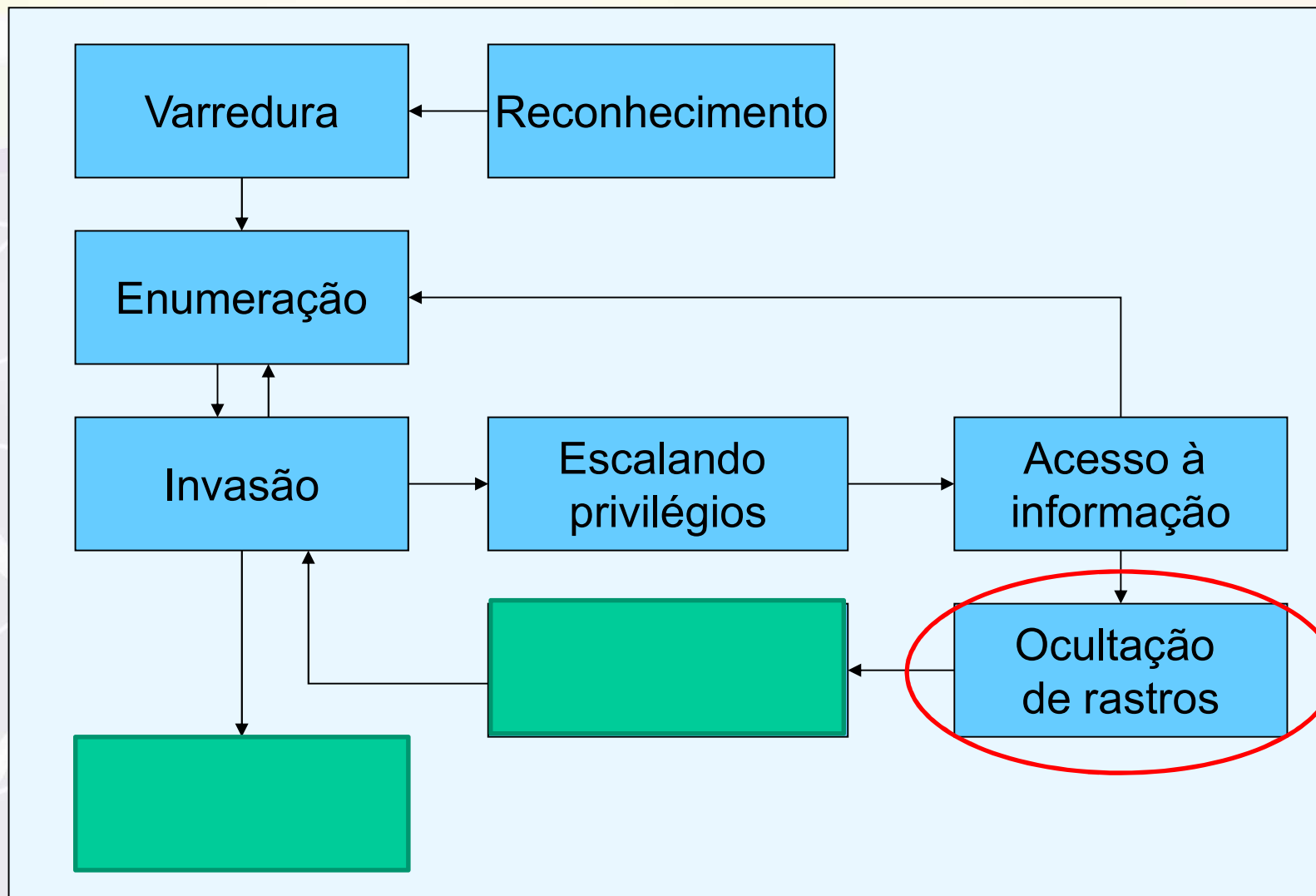
# Anatomia de um ataque



## 6. Acesso a informação

- Alguns conceitos relacionados à “informação”
  - Confidencialidade – trata do acesso autorizado
  - Integridade – trata da alteração autorizada
  - Autenticidade – trata da garantia da autoria da informação
  - Disponibilidade – disponível quando desejada, sem demora excessiva (com autorização)
  - Auditoria – trata do registro do acesso
  - Legalidade – trata aspectos legais
- Invasor pode atuar contra todos os conceitos acima, de acordo com seus interesses

# Anatomia de um ataque

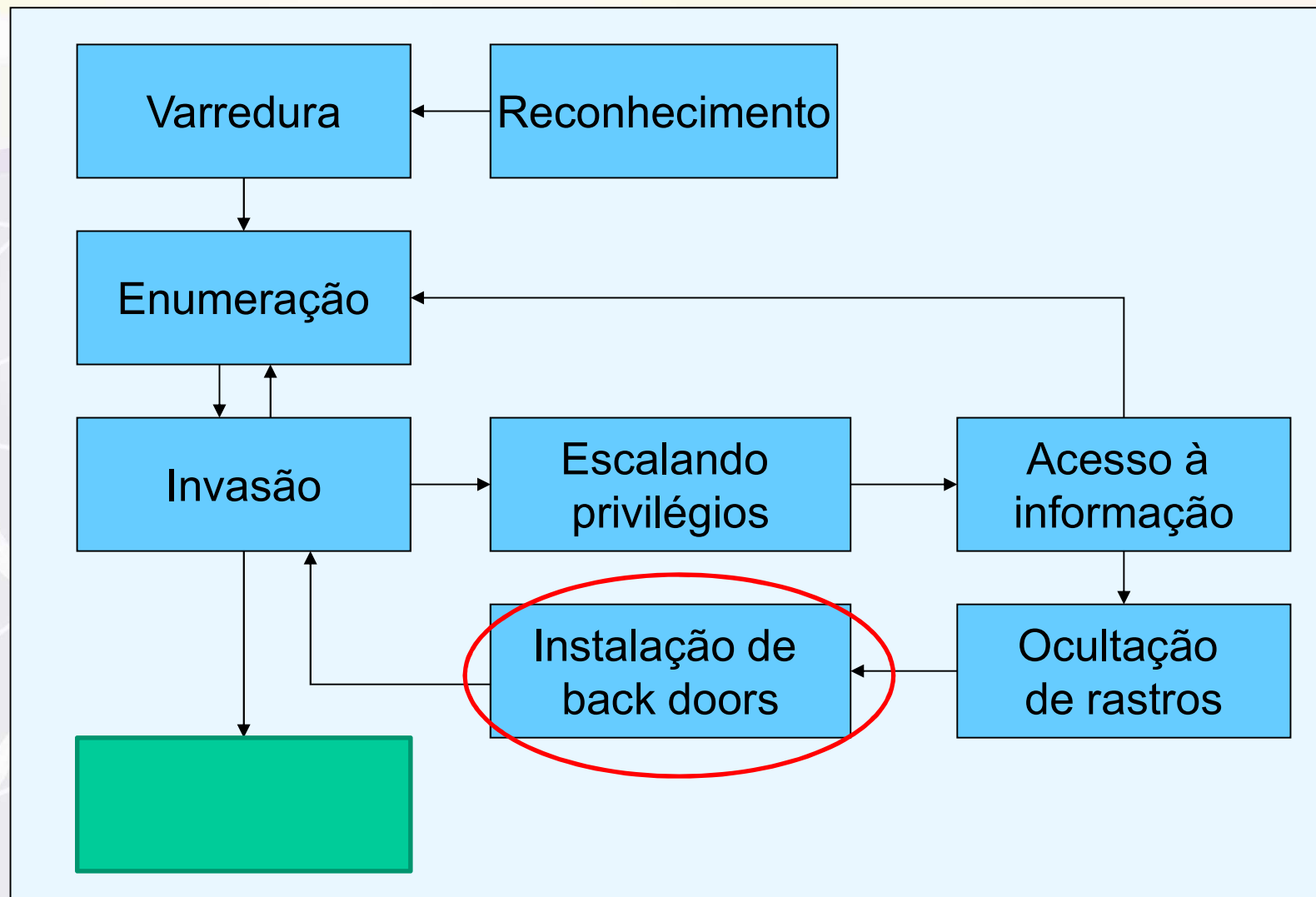


## 7. Ocultação de rastros

- Invasor tenta evitar detecção da presença
- Usa ferramentas do sistema para desabilitar auditoria
- Toma cuidados para não deixar “buracos” nos logs
  - excessivo tempo de inatividade vai denunciar um ataque
- Existem ferramentas para remoção **seletiva** do Event Log
- Esconde arquivos “plantados” (back doors)



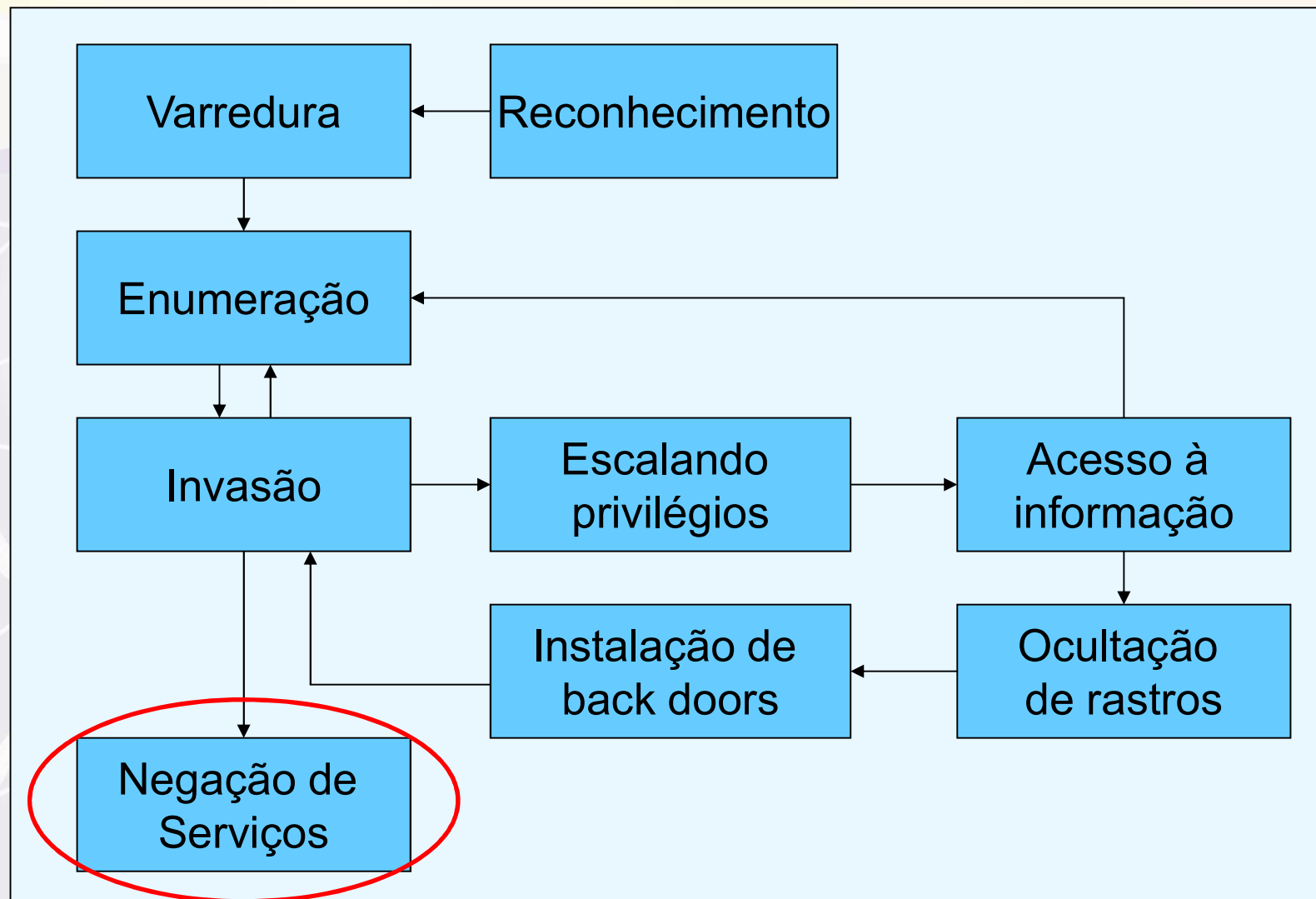
# Anatomia de um ataque



## 8. Instalação de Back doors

- Objetivo é a manutenção do acesso
  - Rootkits – ferramentas ativas, mas escondidas
  - Trojan horses – programas falsificados
  - Back doors – acesso/controlado remoto sem autenticação
- Trojans podem mandar informação para invasor
  - Captura teclado
  - Manda um e-mail com a senha
- Rootkits se confundem com o sistema
  - Comandos modificados para não revelar o invasor
- Back doors
  - Sistemas cliente/servidor
  - Cliente na máquina invasora controlando Servidor na máquina remota
  - Não aparecem na "Task List" do Windows Server

# Anatomia de um ataque

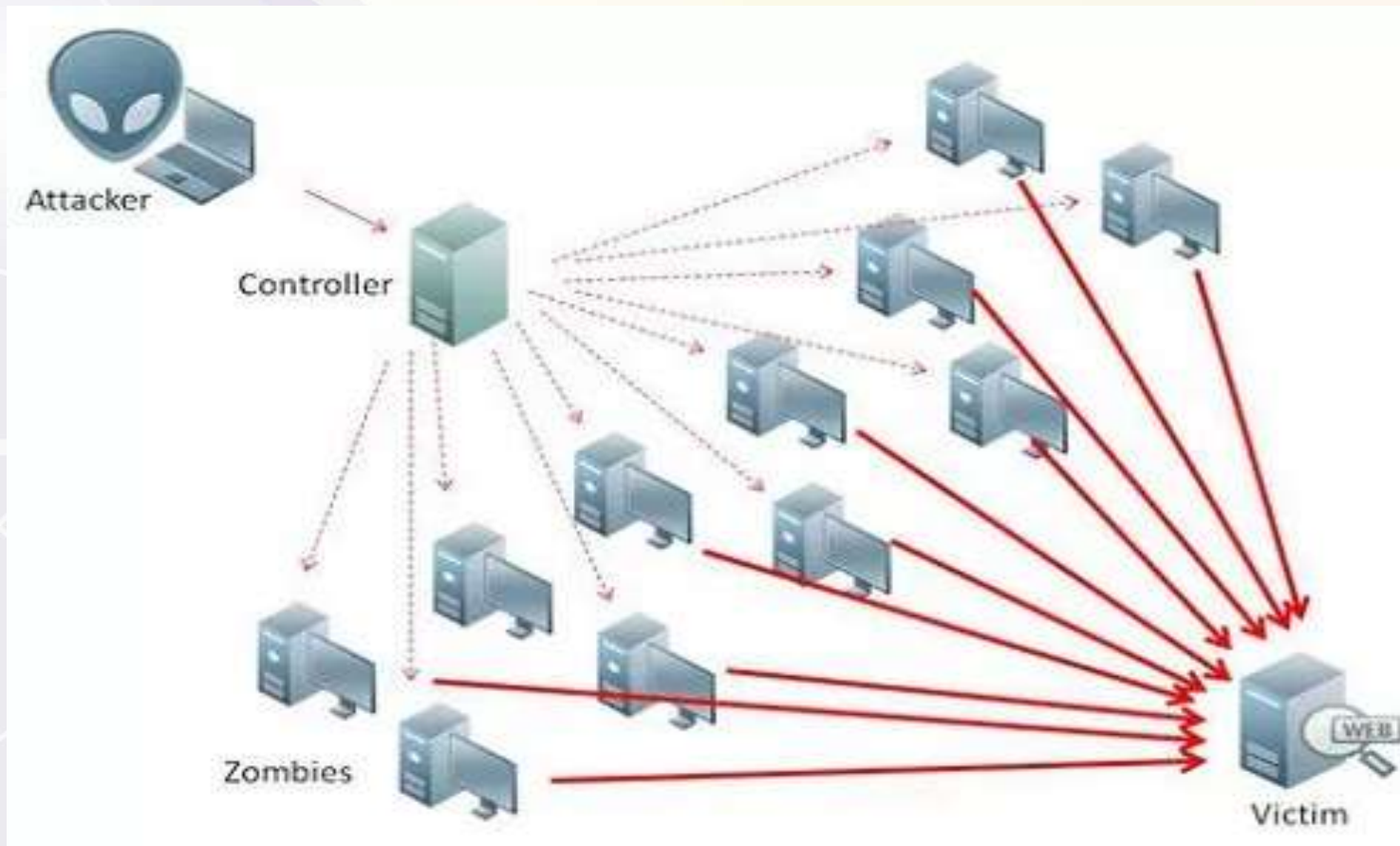


## 9. Denial of Service (Negação de Serviço)

- Ataques com objetivo de bloquear serviços, através de:
  - Consumo de banda de rede
  - Esgotamento de recursos
  - Exploração de falhas de programação (ex: ping da morte)
  - Sabotagem de Roteamento
  - Sabotagem no DNS

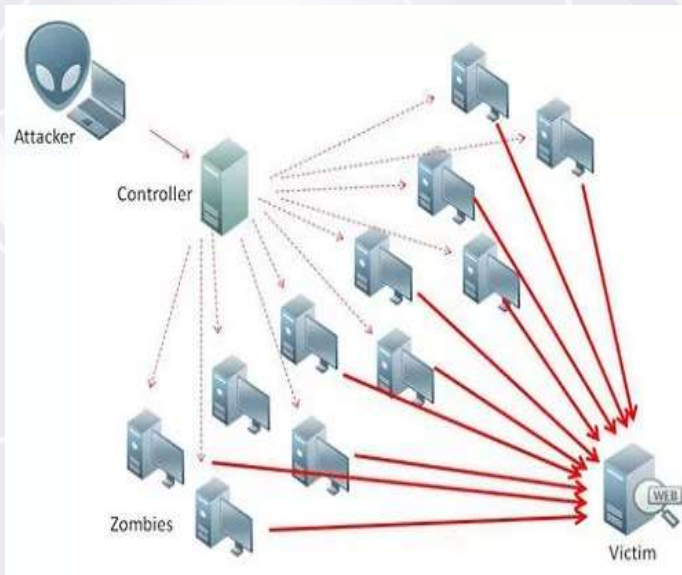
## 9. Denial of Service (Negação de Serviço)

- DDoS → Distributed Denial of Service
  - Ataques coordenados de múltiplas fontes



## 9. Denial of Service (Negação de Serviço)

- DDoS → Distributed Denial of Service
  - Ataques coordenados de múltiplas fontes



DDoS attack destination

