

Ferramentas de Segurança

Prof. Gustavo neves



INSTITUTO FEDERAL

Sul de Minas Gerais
Campus Muzambinho

Obstrução de segurança

- A entidade maliciosa empenha na exploração a um sistema ou recursos de forma desautorizada
- Buscam as vulnerabilidade no sistema
 - Apropriar-se de dados: pessoais, cartões de crédito, etc.
 - Instalar softwares maliciosos
 - Desconfigurar equipamentos, sistemas em servidores web
- Ferramentas de penetração (Pentest - Penetration Test)
 - Os próprios administradores da rede podem utilizar com a finalidade de verificar as vulnerabilidades
 - Consegue prever como invasores poderia agir

Ferramentas de intrusão

- Descobrindo o IP
 - Antes de identificar possíveis alvos é interessante conhecer seus endereços IP
 - Alguns comandos utilizados para descobrir o IP de um domínio, ou vice-versa.
 - nslookup
 - ping
 - dig
 - ipconfig / ifconfig
 - Utilizando esses comando evita que passe pelo servidor dns, pois já se tem o conhecimento do IP

```
C:\Windows\system32\cmd.exe - nslookup

C:\Users\gusta>nslookup
Servidor Padrão: 13.240.120.187.static.milbr.net
Address: 187.120.240.13

> google.com.br
Servidor: 13.240.120.187.static.milbr.net
Address: 187.120.240.13

Não é resposta autoritativa:
Nome: google.com.br
Addresses: 2800:3f0:4001:812::2003
           172.217.30.163

> uol.com.br
Servidor: 13.240.120.187.static.milbr.net
Address: 187.120.240.13

Não é resposta autoritativa:
Nome: uol.com.br
Addresses: 2804:49c:3101:401:ffff:ffff:ffff:45
           2804:49c:3102:401:ffff:ffff:ffff:36
           200.147.35.149

> 8.8.8.8
Servidor: 13.240.120.187.static.milbr.net
Address: 187.120.240.13

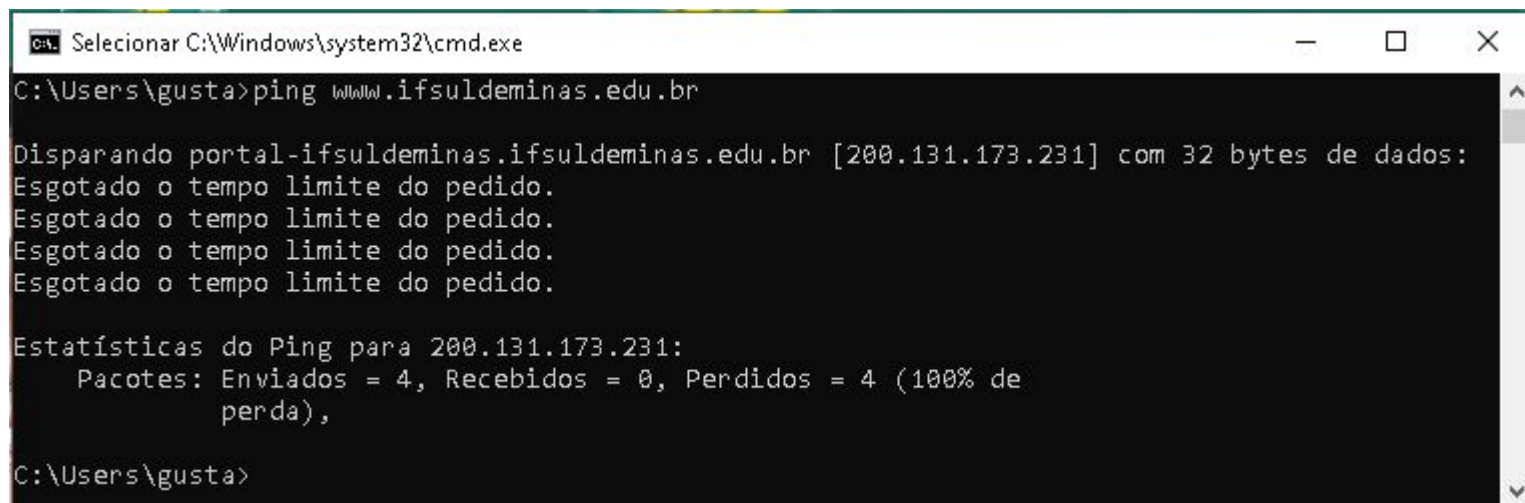
Nome: dns.google
Address: 8.8.8.8
```

Mostra quem é o meu provedor

IP do Google = 172.217.30.163

IP do Uol = 200.147.35.149

o IP 8.8.8.8 = DNS do Google



A screenshot of a Windows Command Prompt window. The title bar at the top reads "Selecionar C:\Windows\system32\cmd.exe". The command prompt shows the user "C:\Users\gusta" entering the command "ping www.ifsuldeminas.edu.br". The output shows that the ping failed for all four attempts, with the message "Esgotado o tempo limite do pedido." (Request timed out). It also displays the IP address of the target: "portal-ifsuldeminas.ifsuldeminas.edu.br [200.131.173.231] com 32 bytes de dados:". Finally, it shows the ping statistics: "Estatísticas do Ping para 200.131.173.231: Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de perda),". The prompt ends with "C:\Users\gusta>".

```
C:\Users\gusta>ping www.ifsuldeminas.edu.br

Disparando portal-ifsuldeminas.ifsuldeminas.edu.br [200.131.173.231] com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.

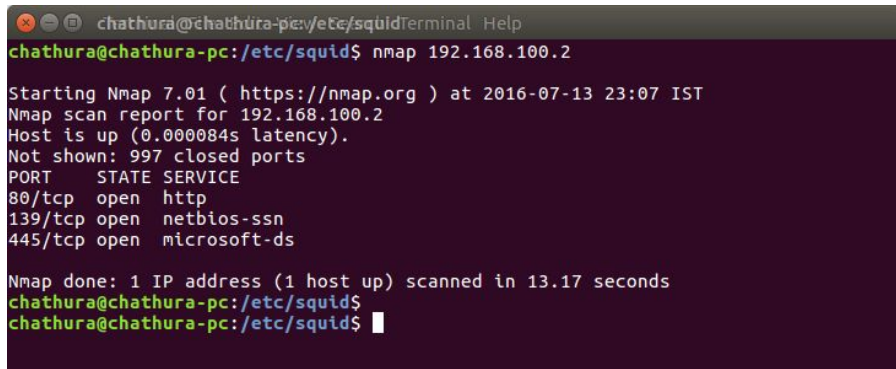
Estatísticas do Ping para 200.131.173.231:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de
                perda),

C:\Users\gusta>
```

Ao utilizar o comando ping ele mesmo realiza a consulta ao dns para saber o IP

Port scanners

- Ferramentas que verificam as portas em máquinas ativas
 - Fica testando as portas, enviam pacotes e aguardam a resposta do estado da porta
 - Portas UDP e/ou TCP se estão abertas
 - Podem pesquisar um range de portas. Ex. portas de 25 a 80
 - Nmap (Network Mapper)
 - Se for usar o proprietário terá que fornecer autorização prévia

A terminal window with a dark purple background. The title bar shows 'chathura@chathura-pc: /etc/squid Terminal Help'. The prompt is 'chathura@chathura-pc: /etc/squid\$'. The command 'nmap 192.168.100.2' has been executed. The output shows the Nmap scan report for 192.168.100.2, indicating the host is up and listing open ports 80, 139, and 445. The prompt is now 'chathura@chathura-pc: /etc/squid\$' again.

```
chathura@chathura-pc: /etc/squid$ nmap 192.168.100.2

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-13 23:07 IST
Nmap scan report for 192.168.100.2
Host is up (0.000084s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
chathura@chathura-pc: /etc/squid$
chathura@chathura-pc: /etc/squid$
```

Serviços vulneráveis

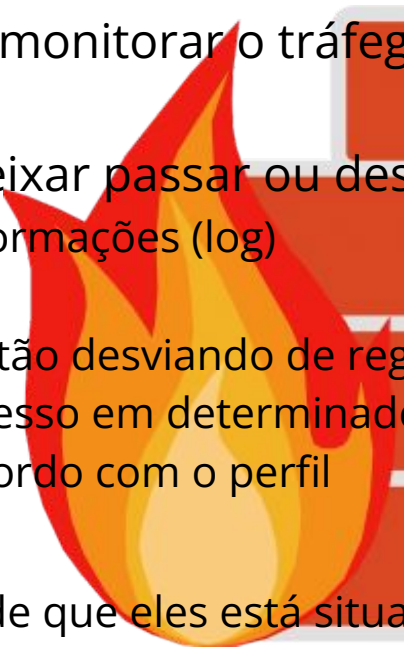
- Ferramentas de varredura de vulnerabilidades, scanners de vulnerabilidades
- Verificam o estados das portas e analisam as vulnerabilidades
- testam script e verificam se funciona
- verificar bugs, configurações erradas
- Softwares
- OpenVAS (Open Vulnerability Assessment System)

Serviços vulneráveis

- Nessus
- Exibem relatórios do status das máquinas, soluções para cada problema encontrado
- Utilizam bases de dados de vulnerabilidade CVE (Common Vulnerabilities and Exposures)
- <https://cve.mitre.org/>

Firewall

- São equipamentos ou softwares filtram o tráfego nas redes conectadas
- Através de regras é possível monitorar o tráfego em uma determinada rede
- analisa os pacotes e pode deixar passar ou descartar
 - Registra ou não as informações (log)
 - envio de notificações
 - Verifica se usuários estão desviando de regras de uso da rede
 - Qual frequência de acesso em determinados sites
 - Controla acesso de acordo com o perfil
- Algumas desvantagens:
 - Monitora apenas a rede que eles está situado
 - As falhas de configuração pelo usuário não serão alertadas



Packet filtering

- Filtragem de pacotes
 - Camadas: Transporte e Rede
 - análise é realizada apenas no cabeçalho dos pacotes:
 - IP de origem e destino
 - Porta de origem e destino
 - Protocolos: UDP ou TCP
 - São mais leves

Proxy services

- Firewall de aplicação ou Proxy de serviços
 - Camadas: Aplicação, transporte e Rede
 - Análise é realizada em todo fluxo de dados
 - Faz a intermediação entre rede interna e externa
 - Solicitações oriundas da rede interna ao servidor proxy, que por sua vez se comunica com a Internet

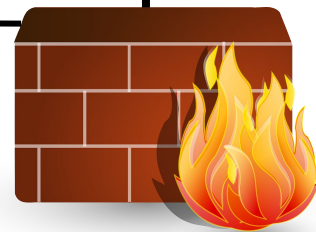
Localização do Firewall

- Firewall entre a rede local e a internet
 - Proteção contra ataques externos
 - Proteção interna fica comprometida
 - Ação de *malwares*, usuários mal intencionados etc

Servidor

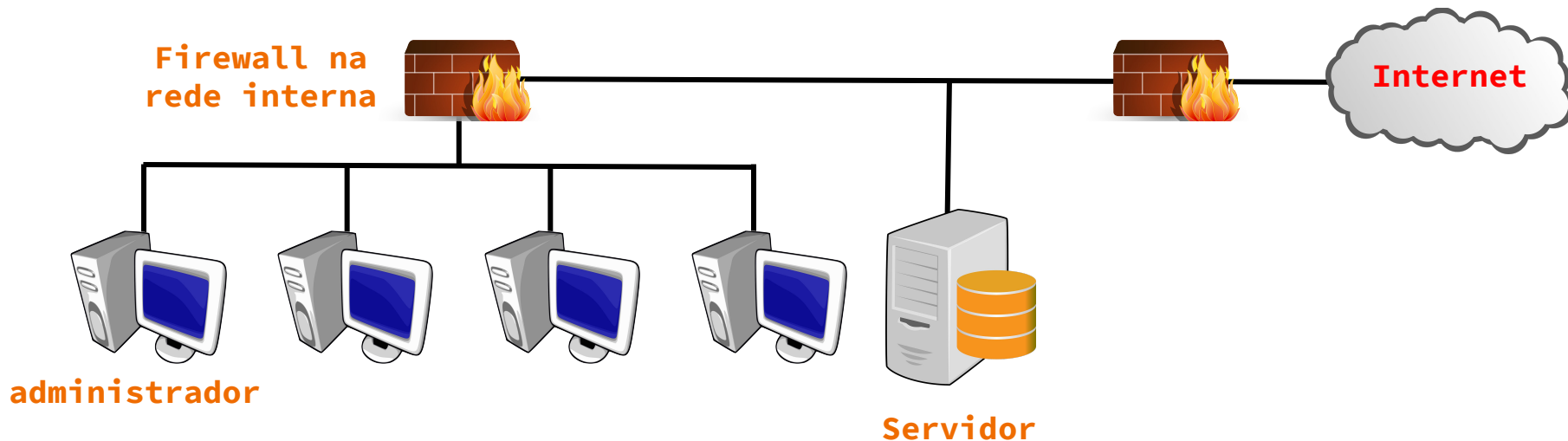


Desktops, LAN



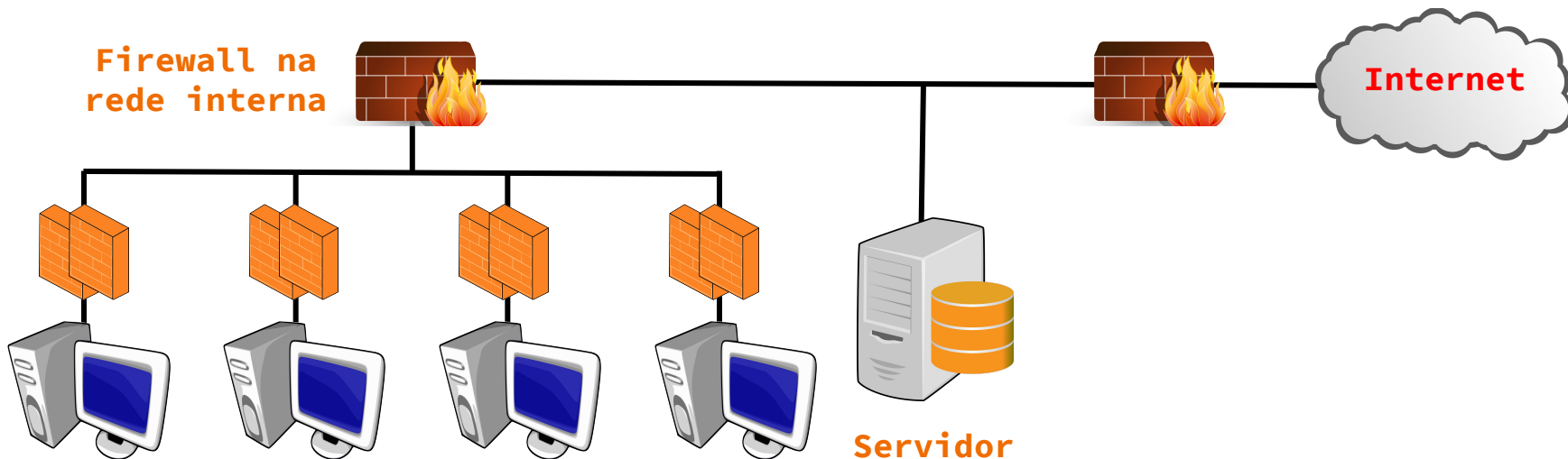
Localização do Firewall

- Firewall na rede interna
 - **DMZ:** Zona desmilitarizada
 - proteção contra ataques internos e externos
 - as configurações de cada firewall podem ser diferentes



Localização do Firewall

- Firewall para cada estação de trabalho
 - Sistemas Operacionais já oferecem
 - evita ataques entre as estações
 - monitora os pacotes e pode detectar e impedir uma atividade de malwares.



Sistemas de detecção e prevenção de intrusos

- **IDS** - Sistema de detecção de intrusos: apenas enviará um alerta
- **IPS** - Sistema de prevenção de intrusos: prevenir o ataque, realiza ações contra os ataques
- através do monitoramento da rede pode verificar se há indícios de intrusão
 - realizar varreduras nas portas
 - verificar os pacotes que estão trafegando na rede
 - reconfiguração do firewall

Sistemas de detecção e prevenção de intrusos

- Alguns métodos utilizados na detecção:
 - Anomalias: comportamentos fora do comum
 - Assinaturas: conferem com as bases comuns a fim de detectar ações que caracterizam uma ataque

Sistemas de detecção e prevenção de intrusos

- Localização do IDS
 - estação: execução na própria máquina
 - em rede: analisa os pacotes que estão trafegando na rede
 - podem detectar ataques que passam despercebidos nas estações
 - sensores:
 - em linha: ficam entre os segmentos de rede (firewall, switch)
 - passivos: analisa cópias de pacotes