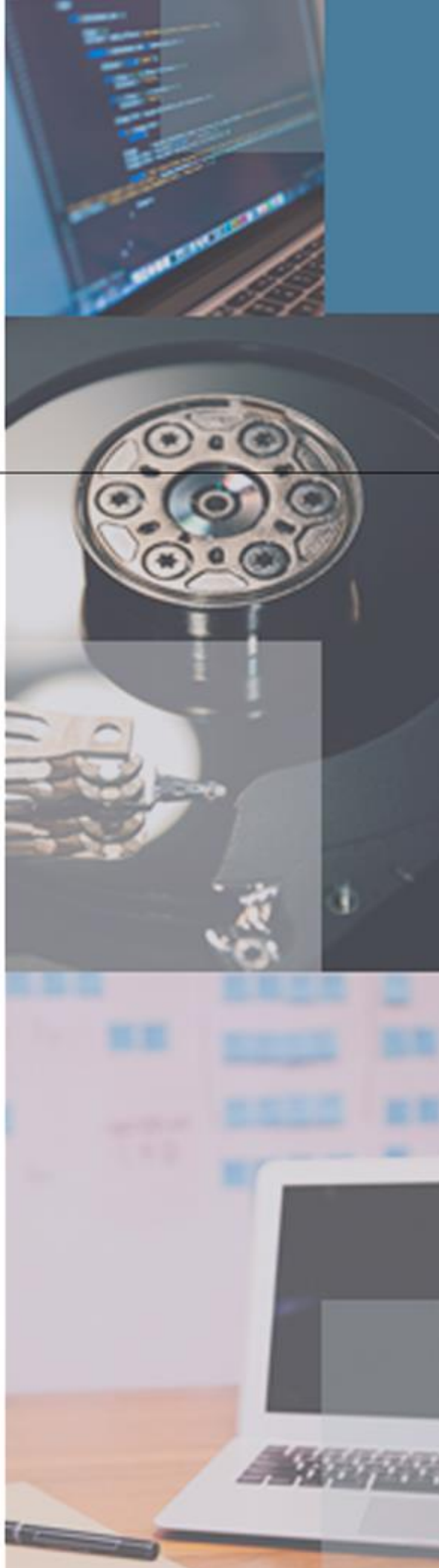
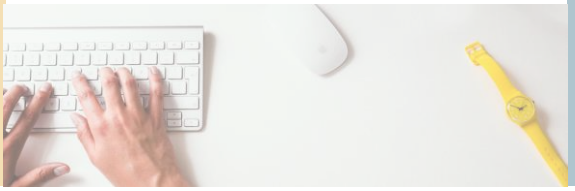
FUNDAMENTOS
DE ETHICAL HACKING



MATERIAL COMPLEMENTAR

Principios básicos
de redes e segurança

marcosflavio.com.br



Princípios básicos de redes e segurança

1. INTRODUÇÃO

Todo sistema informatizado deve ser devidamente protegido nos dias atuais, pois os crimes cibernéticos estão cada vez mais freqüentes.

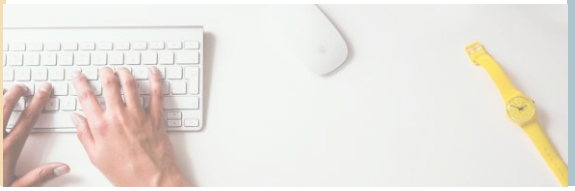
Segurança é o estado de boa conservação da informação de tal modo que a possibilidade de sucesso de ataques como roubo e vazamento de informações seja mantido em nível pequeno ou tolerável.

Os elementos fundamentais da segurança da informação são divididos em:

- **Confidencialidade:** Ocultamento de informações ou recursos.
- **Integridade:** Confiança nos dados de maneira a evitar alterações impróprias.
- **Disponibilidade:** a informação ou recurso desejado deve estar disponível sempre que necessário.

Algumas das ameaças contra à informação enfrentadas pelas empresas:

- Vírus
- Crackers
- Cyberterrorismo
- Engenharia Social
- Acesso não autorizado
- Roubo de Dados
- Desastres Naturais
- Indisponibilidade de Dados



2. Fundamentos de TCP/IP

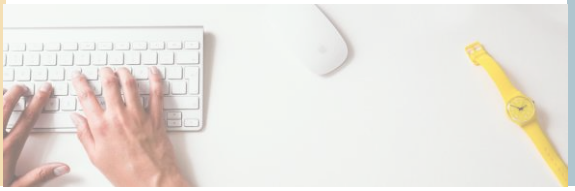
O conjunto de protocolos TCP/IP foi desenvolvido pela Defense Advanced Research Projects Agency (DARPA). Posteriormente, o TCP/IP foi incluído no Berkeley Software Distribution da Unix. O modelo TCP/IP é dividido em quatro camadas (não confundir com as sete camadas do modelo OSI), que são: Aplicação, Transporte, Internet e Interface com a Rede.

2.1 - Camada de Aplicação

Contém os protocolos de alto nível (HTTP, FTP, SMTP etc.). Todas as operações com esses protocolos e suas propriedades, sessões e controle de diálogos são realizadas nessa camada. Após o término, os dados empacotados são enviados para a camada seguinte. A seguir, alguns dos muitos protocolos utilizados nessa camada.

SMTP e POP

O Simple Mail Transfer Protocol é o protocolo responsável por entregar mensagens de e-mail a um destinatário. Toda vez que seus e-mails são enviados, um servidor SMTP se encarrega de encaminhá-los ao seu destino. Essas mensagens vão ser recuperadas depois, através do servidor POP ou IMAP. No geral, o SMTP é utilizado para enviar a mensagem de um cliente para um servidor,

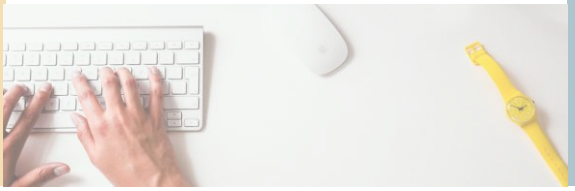


necessitando, portanto, que você especifique esse servidor ao configurar o seu programa de e-mail.

Esse protocolo é o responsável pelo recebimento dos e-mails. O IMAP (Internet Message Access Protocol) também é utilizado para isso, mas não é tão popular quanto o POP (Post Office Protocol). Ele geralmente se localiza na porta 113. Existem duas versões do POP. A primeira, chamada POP2, tornou-se um padrão na década de 1980 e dependia do SMTP. A versão mais nova, POP3, pode ser usada com ou sem SMTP.

Telnet e SSH

Um programa de emulação de terminal para redes TCP/IP, como a Internet. O programa Telnet roda no seu computador e se conecta a um servidor na rede. Você poderá, então, entrar com comandos diretamente no programa Telnet e eles serão executados como se você estivesse entrando com eles diretamente no shell do sistema (prompt de comando). Isso possibilita a você controlar o servidor e se comunicar com outros computadores na rede. Para iniciar uma sessão de Telnet, você precisa se logar no servidor, entrando com nome de usuário e senha válidos. Às vezes, você não precisa nem se autenticar (exemplo: ao utilizar Telnet para se conectar à porta do SMTP).



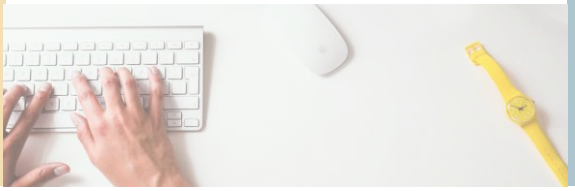
O SSH (Secure Shell) foi desenvolvido para permitir que você se conecte a uma máquina remota, execute comandos e mova arquivos entre uma máquina e outra. Ele possui um excelente sistema de autenticação e criptografia em meios inseguros (Internet, por exemplo). O SSH é o substituto de programas como Rlogin, Rsh, e o próprio Telnet (que não utiliza criptografia).

O SSh também protege uma rede de ataques, tais como o IP Spoofing e o DNS Spoofing (vistos mais à frente no livro). Se alguém conseguir tomar o controle da rede, só consegue forçar o SSh a desconectar e não consegue obter nenhum dado importante. Até na hora de se logar usando esse protocolo a transmissão da senha é criptografada, o que impede que alguém a capture.

HTTP

Abreviação de Hyper Text Transfer Protocol, o HTTP é o protocolo usado pela World Wide Web, a rede mundial de websites da Internet. Ele é quem define como as páginas são formatadas e transmitidas e que ações servidores Web e navegadores (browsers) devem tomar ao responder a certos comandos. Por exemplo, quando você entra com uma URL no seu browser, este envia automaticamente um comando HTTP (comando GET) ao servidor Web, dizendo a ele para transmitir a página Web requisitada.

O HTTP é um protocolo chamado de “sem estado”, pois cada comando é

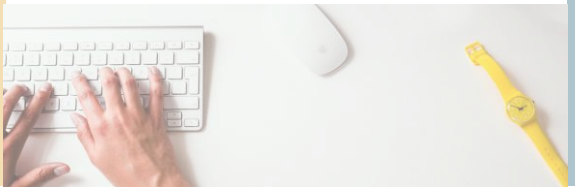


executado independentemente, sem nenhum conhecimento dos comandos que vieram antes dele. Por isso, é difícil implementar sites Web que reajam de modo inteligente à entrada de dados de um usuário. Esse problema do HTTP está sendo melhorado pode diversas novas tecnologias, incluindo ActiveX, Flash, Java, Javascript e Cookies.

O SSL (Secure Sockets Layer) foi desenvolvido pela Netscape para transmitir documentos privados pela Internet. Ele trabalha enviando uma chave privada para criptografar os dados que serão transmitidos durante a conexão SSL. Atualmente, quase todos os browsers suportam esse protocolo, e muitos sites Web o utilizam para obter informações confidencias de um cliente, como, por exemplo, números de cartão de crédito. As URLs que requerem uma conexão SSL começam com HTTPS ao invés de HTTP.

FTP

Protocolo que permite a transferência de arquivos através da rede. Você acessa um servidor FTP com seu nome de usuário e senha, e coloca ou pega arquivos ali dentro. É uma maneira fácil e rápida de transferir dados, muito usada para colocar um site no ar rapidamente. Existe também o TFTP, que é por UDP (visto em camada de transporte), mas esse não possui autenticação nem confiabilidade, além de ser visto por muitos como um risco de segurança.

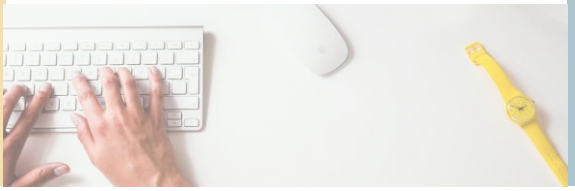


DNS

Domain Name System é um sistema usado na Internet para converter os nomes de domínios em endereços numéricos (IPs). Isso porque é mais fácil lembrar de um nome do que um número. Cada vez que você digita um nome de domínio (www.marcosflavio.com.br), um serviço DNS deve traduzir o nome para o seu endereço IP correspondente. É como se o sistema de DNS tivesse a sua própria rede. Se um servidor não consegue traduzir um nome de domínio, ele pergunta a outro que, se não souber, pergunta a um terceiro servidor e, assim, sucessivamente, até que o endereço IP seja obtido. Um domínio pode ser colocado em um *subdomínio*.

Alguns exemplos de domínios comuns são:

- **COM**: Organizações Comerciais.
- **GOV**: Organizações Governamentais.
- **EDU**: Organizações Educacionais.
- **ORG**: Outras Organizações.
- **NET**: Organizações relacionadas com a Internet.
- **Identificador do País**: São duas letras que representam um país em particular. Exemplo: *br* (Brasil).



2.2 - Camada de Transporte

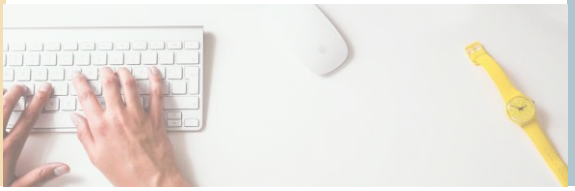
Essa camada é responsável pelo controle do fluxo, confiabilidade e possível correção de erros na entrega dos dados. São esses protocolos que fazem a comunicação nas redes TCP/IP tão estáveis hoje. O próprio TCP no nome do protocolo corresponde a um dos excelentes recursos dessa camada.

TCP

Transmission Control Protocol ou TCP é um protocolo confiável para a transmissão de dados. Dizemos “confiável” porque ele se assegura de conseguir a conexão antes de enviar as informações; caso não consiga, retorna um erro. O TCP também garante que todos os pacotes sejam entregues e na exata ordem em que eles foram enviados. É fácil perceber a ação desse protocolo. Quando nos conectamos a um Messenger instantâneo, um servidor de FTP, uma página Web ou mesmo enviamos um e-mail, estamos usando o TCP.

UDP

UDP ou User Datagram Protocol é um protocolo de transporte de dados que, ao contrário do TCP, não faz nenhum tipo de conexão. Ele também possui poucos serviços de recuperação de erros, oferecendo, ao invés disso, uma maneira direta de



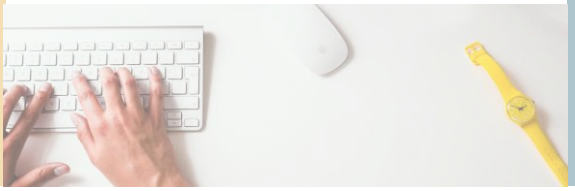
enviar e receber dados em uma rede. É usado principalmente para o broadcast de mensagens em uma rede. Uma das utilizações em que você pode notar isso é no streaming de vídeo pela Internet. Neste você pode perceber que há pequenas falhas, alguns cortes etc. Isso é UDP, utilizado, nesse caso, porque a velocidade de transmissão é maior que a do TCP.

Portas

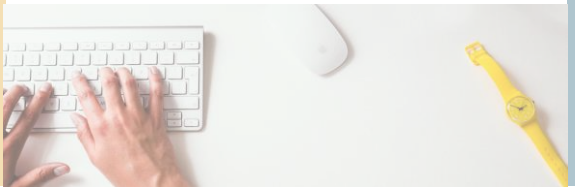
Para conseguir manipular múltiplas conexões ao mesmo tempo, tanto o TCP quanto o UDP utilizam números de portas. O intervalo numérico utilizado vai de 0 a 65.535. Muitos tipos de conversações usam portas específicas, como o FTP, que utiliza a porta 21. Mas muitas dessas portas não têm uma descrição e podem ser aleatoriamente utilizadas.

- Os números anteriores a 255 são para aplicativos públicos.
- Os números de 255 a 1.023 são usados por aplicativos comerciais.
- Os números acima de 1.023 não são regulamentados.

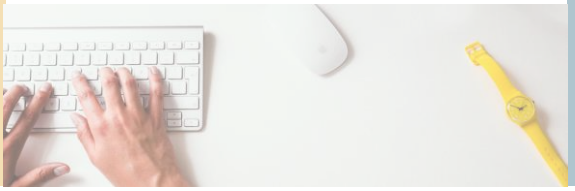
A seguir, você verá algumas portas e alguns serviços comumente utilizados nelas:



PORTA	PROTOCOLO	SERVIÇO
7	TCP	Echo
11	TCP	Systat
13	TCP	Daytime
19	TCP	Chargen
20	TCP	FTP Data
21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
43	TCP	Whois
49	UDP	Tacacs
53	TCP	DNS-zone
53	UDP	DNS-lookup
66	TCP	Oracle Sqlnet
69	UDP	TFTP
79	TCP	Finger
80	TCP	HTTP
110	TCP	Pop3
111	TCP	SunRPC
119	TCP	NNTP



135	TCP	NT_RPC
139	TCP	Netbios
143	TCP	IMAP
161	UDP	SNMP
162	UDP	SNMP-TRAP
179	TCP	Bgp
389	TCP	LDAP
443	TCP	HTTPS
1080	TCP	Socks
1433	TCP	MS_SQL
1498	TCP	Sybase-Sql-Anywhere
1525	TCP	Oracle-Srv
1527	TCP	Oracle-Tli
1723	TCP	PPTP
1745	TCP	Winsock_Proxy
2049	TCP	NFS
3128	TCP	Proxy
8080	TCP	Proxy/Socks



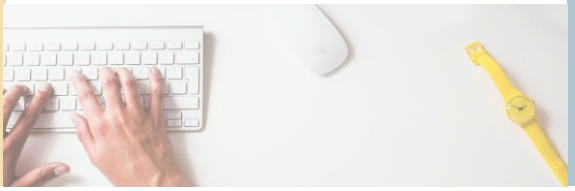
2.3 - Camada de Internet

O objetivo dessa camada é assegurar que os dados cheguem ao seu destino, independente do caminho e das redes que utilizem para isso. O protocolo específico que governa essa camada é chamado Protocolo de Internet (IP). A determinação do melhor caminho e a comutação de pacotes acontecem nessa camada. Pense nisso em termos do sistema postal. Quando envia uma carta, você não sabe como ela vai chegar ao seu destino (existem várias rotas possíveis), mas o que realmente importa é que ela chegue. Vejamos alguns protocolos dessa camada a seguir.

IP

O *endereço IP* é um conjunto de números que identificam seu computador em uma rede. Inicialmente, você pode imaginar o IP como um número de telefone. Por padrão, cada computador ou equipamento ligado à Internet possui um endereço desse tipo. Também é permitido que o mesmo endereço IP seja usado em mais de uma interface (placa de rede) de um mesmo computador.

A porção dos endereços que são comuns entre todos os endereços de uma rede é chamada de "*porção da rede*". Os dígitos restantes são chamados de "*porção dos hosts*". O número de bits que são compartilhados por todos os endereços dentro da rede é chamado de "*máscara de rede*" (netmask) e o papel dela é determinar quais endereços pertencem ou não à rede. Por exemplo:



Endereço do Host	192.168.0.125
Máscara da Rede	255.255.255.0 (/24)
Endereço da Rede	192.168.0.0
Endereço Broadcast	192.168.0.255

A máscara de sub-rede indica a classe que o host se encontra:

255.0.0.0 -> Classe A

255.255.0.0 -> Classe B

255.255.255.0 -> Classe C

A máscara também pode ser representada na notação CIDR:

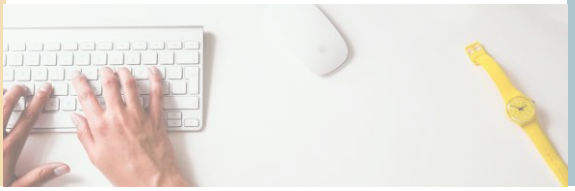
/8 -> Classe A (8 bits)

/16 -> Classe B (16 bits)

/24 -> Classe C (32 bits)

Uma prática comum também é dividir uma rede de uma classe padrão em mais sub-redes ou VLSMs (sub-rede de sub-rede). Exemplo:

A rede 192.168.0.0 / 255.255.255.0 (/24) permite 254 hosts (máquinas). Vai de 192.168.0.1 a 192.168.0.254 (0 e 255 não podem ser utilizados pois são os endereços de rede e broadcast).



Se eu mudar a máscara de sub-rede para 255.255.255.192, posso dividir essa rede em 4 sub-redes de 64 endereços IP cada, ficando a primeira rede no intervalo 192.168.0.0 -> 192.168.0.63. (Lembre que 0 e 63 não podem ser usados pra máquinas). A máscara padrão seria /26.

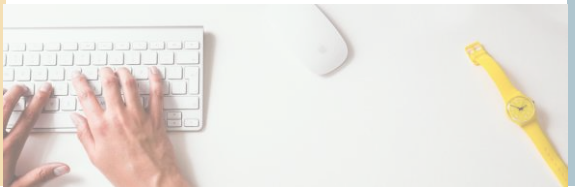
Temos três tipos de endereços em uma rede IPv4: Unicast, Broadcast e Multicast:

Unicast

Em uma transmissão unicast, uma cópia separada dos dados é enviada de sua origem para cada computador cliente que os requisite. Nenhum outro computador na rede recebe o tráfego. No entanto, em uma rede com muitos computadores, o unicast não é sempre eficiente, pois muitas vezes o computador de origem terá que transmitir múltiplas cópias dos dados.

Broadcast

Nesse tipo de transmissão, os dados são enviados apenas uma vez, mas para toda a rede. Esse processo não é muito eficiente, pois faz a velocidade cair bastante, já que todos os computadores irão receber os dados. Mesmo os hosts que não fizeram o pedido receberão os dados. Somente não irão processar esses pedidos e enviá-los ao sistema operacional. O protocolo ARP é um dos que utiliza bastante o modo de broadcast.

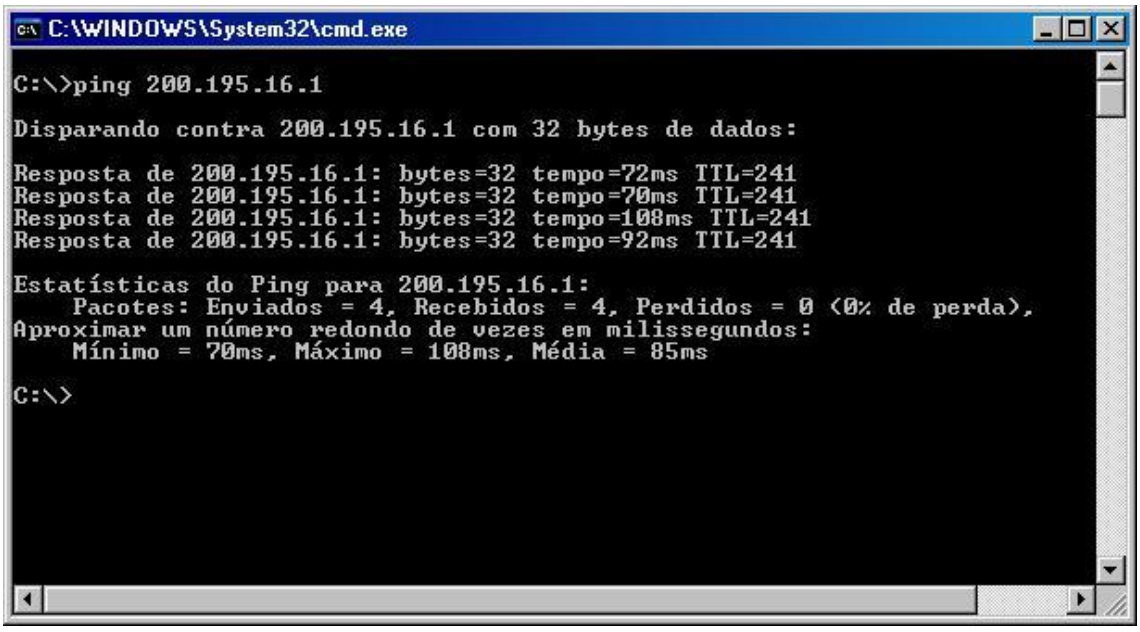


Multicast

É uma mistura dos dois. É enviada apenas uma cópia dos dados e somente os computadores que fizeram o pedido os recebem, evitando, assim, um tráfego muito intenso e, conseqüentemente, um congestionamento na rede. Muitos serviços de Internet usam multicast para se comunicar com clientes. Inclusive, é nesse tipo de comunicação que se baseia o protocolo IGMP (Internet Group Message Protocol, uma espécie de ICMP baseado em multicast).

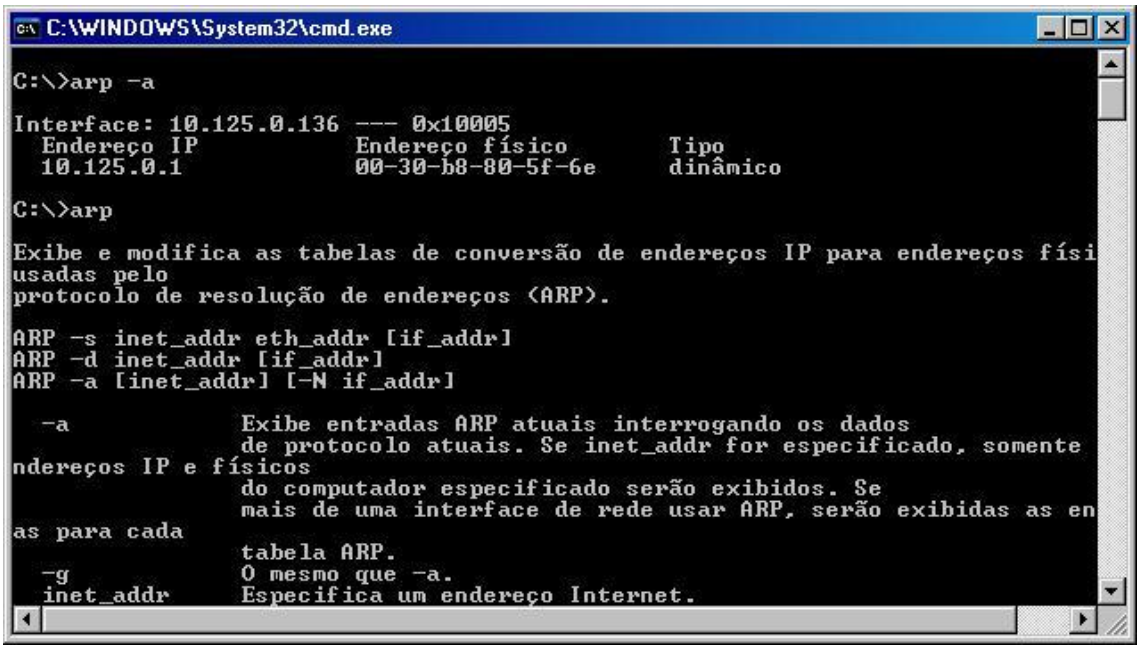
ICMP

Abreviatura de Internet Control Message Protocol. A função do ICMP é enviar pacotes avisando possíveis erros ou informações. É muito utilizado pelo comando Ping, que pode ser usado para testar se um computador está on-line ou não (se está respondendo).



ARP

Abreviatura de Address Resolution Protocol, protocolo usado para converter um endereço IP em endereço físico, como um endereço Ethernet (MAC). Um computador, querendo saber o endereço físico de outro, faz um broadcast na rede e o sistema procurado responde com a informação requisitada. Também existe o Reverse ARP (RARP), que pode ser usado por um host para descobrir seu endereço IP. Dessa maneira, o computador faz um broadcast do seu endereço físico e um servidor RARP responde com o endereço IP do computador procurado.



3. Tipos de Invasores

Existem vários tipos de nomes dados aos invasores do mundo da internet. Quem são os responsáveis pelos perigos digitais?

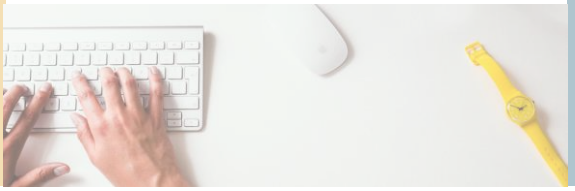
Hacker → Individuo com muito conhecimento de redes, sistemas e programação.

Hacker ético → Hacker que usa seus conhecimentos de forma não criminosa

Hacker White-Hat → A mesma finalidade que hacker ético.

Cracker → Usa os conhecimentos deforma criminosa.

Hacker Black-hat → Mesmo que Cracker.



4. Penetration Test

Teste que visa “atacar” uma rede ou sistema para descobrir vulnerabilidades da mesma. Etapas de um pentest:

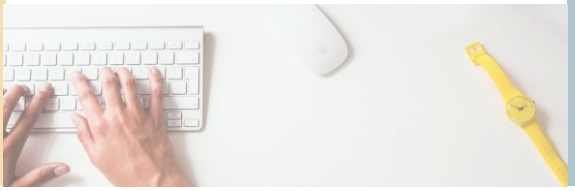
- Pesquisa (Google)
- Varredura (Ips, portas, enumeração)
- Ganho de acesso
- Manutenção de acesso
- Apagar Rastros

4. Tipos de Vírus e Softwares Maliciosos

São os chamados *Malwares* que causam os maiores problemas enfrentados hoje em dia. Podem infectar milhões de computadores no mundo todo causando o caos.

4.1 Vírus

São pequenos programas criados por criminosos cibernéticos para causar algum dado ao computador alvo. Seja apagando pastas e arquivos, capturando informações ou senhas importantes, corrompendo arquivos de sistema para alterar o funcionamento correto da máquina, entre outras ações.



Esses vírus se disseminam ou agem por meio de falhas ou limitações de determinados programas, se espalhando como uma infecção. Eles se utilizam principalmente de aplicativos e sites do tipo “sensação do momento” como whatsapp, facebook, etc para se espalharem e capturarem mais vítimas possíveis. Um outro exemplo é o *fake mail* (remetente falso), fazendo o destinatário do e-mail acreditar que se trata de uma mensagem verdadeira.

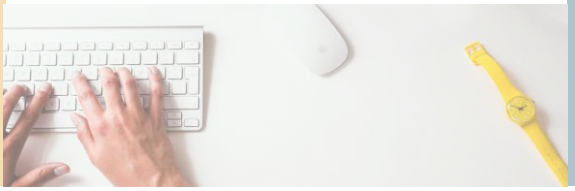
4.2 Worms

São apelidados de vermes pela forma de propagação. É diferente do vírus por ser considerado mais “inteligente” que os demais. Eles podem capturar endereços de e-mail em arquivos de usuário, usar serviços de envio de e-mails próprios, acessar compartilhamentos remotos de pastas, etc. Ainda há aqueles que exploram falhas de programação para tentar atacar por alguma porta aberta ou algo assim.

Softwares desse tipo permitem o compartilhamento de arquivos entre internautas ou usuários de uma mesma rede.

4.2.2 – Ransomware

É um tipo de malware que criptografa os arquivos do seu computador e lhe envia um e-mail pedindo dinheiro de resgate. Se você efetuar o pagamento, a chave para descriptografar os arquivos lhe será enviada.

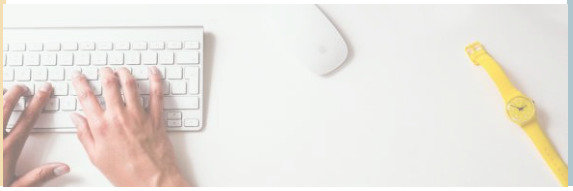


4.3 Spywares e Hijackers

São tipos de softwares maliciosos que ficam espionando as atividades dos internautas ou capturam informações sobre eles. Para infectar um PC eles podem vir embutidos em softwares desconhecidos ou serem baixados automaticamente quando se visita uma página de conteúdo duvidoso.

4.4 Cavalos de Tróia

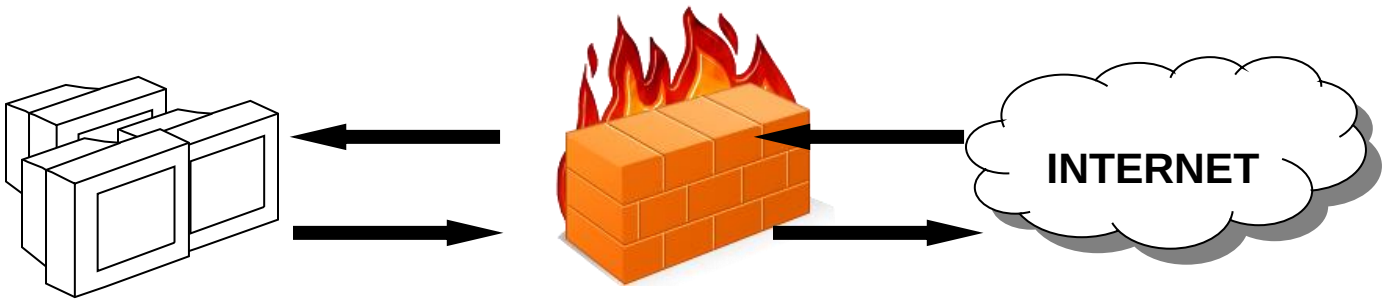
Conhecidos também como Trojan, é criado a partir de um código malicioso inserido em um arquivo aparentemente inofensivo (um jogo, por exemplo) que, quando executado em um sistema, geralmente abre uma porta TCP ou UDP para receber conexões externas fornecendo Shell do sistema para o invasor. Então, um cavalo de tróia é criado basicamente inserindo-se um backdoor (porta dos fundos) em um outro arquivo, podendo ser um executável, documento PDF, planilha do excel, etc.



5. Firewalls

Um Firewall é um recurso misto de software e hardware que controla o tráfego que entra e sai de uma rede. Existem três tipos:

- Filtro de Pacotes



FIREWALL | Acesso a Internet (NAT)

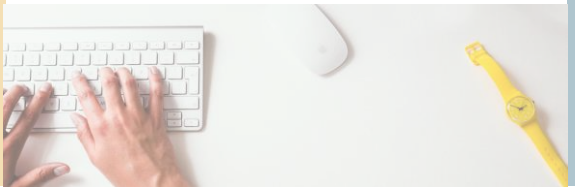
|

O Filtro de Pacotes “peneira” os pacotes que entram e saem da rede. Algumas soluções também permitem o acesso à internet através do recurso de NAT (Tradução automática de endereços).

Software: Iptables

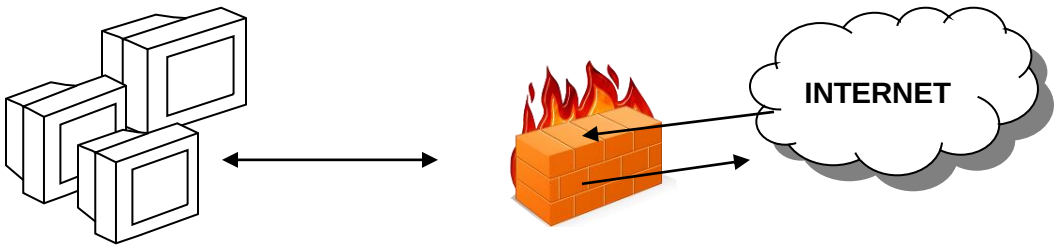
Exemplo de Regras:

- Bloquear acesso à porta 21
- Bloquear acesso ao IP 10.0.0.1
- Liberar acesso à porta 80



Obs: O filtro de pacotes atua na camada de rede do modelo OSI (Três), portanto, só trabalha por IP, Portas, e ICMP.

- Servidor Proxy



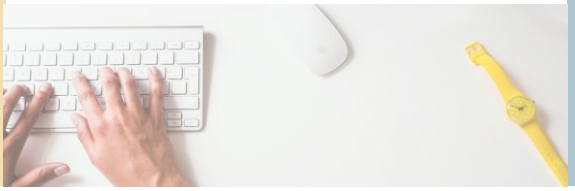
| Acesso à Internet |

O proxy funciona como um “portão” para o acesso à internet diretamente. Trabalha na camada 7 (Aplicação) do modelo OSI, utilizando-se de usuários para autenticação.

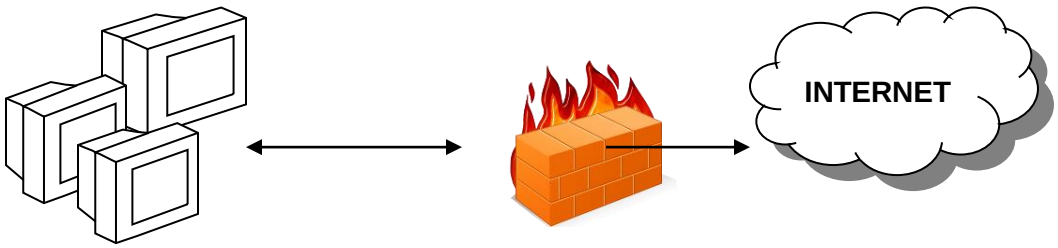
Software: Squid

Exemplo de Regras:

- Bloquear facebook.com.br
- Bloquear termo “jogos”
- Bloquear acesso a gov.br



- Firewall Híbrido



| Acesso à Internet |

Um firewall híbrido funciona tanto com filtro de pacotes quanto como Proxy.

Software: Isa Server

Exemplo de Regras:

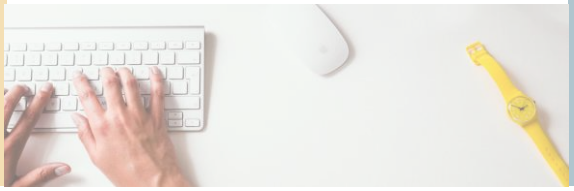
- Usuário Marcos não acessa porta 25.

- IP 192.168.10.1 não acessa jogos.com.br

5.1 Listas Brancas Vs. Listas Negras

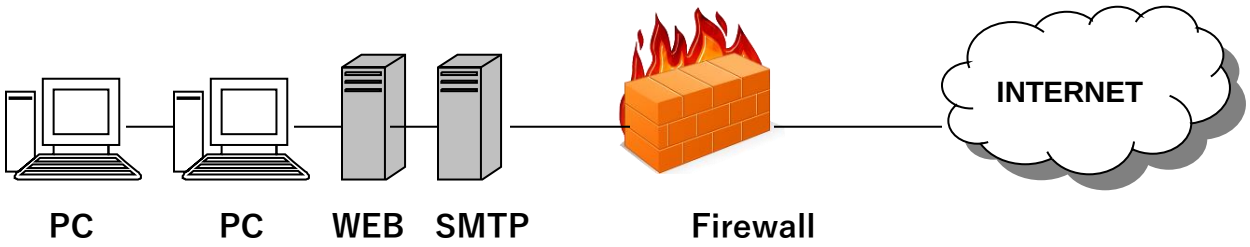
Por padrão, podemos trabalhar com o firewall de duas formas:

1. Liberando todo o tráfego e bloqueando o que não é necessário. (Listas Negras)



2. Bloqueando todo o tráfego e liberando apenas ou estritamente o necessário (Listas Brancas)

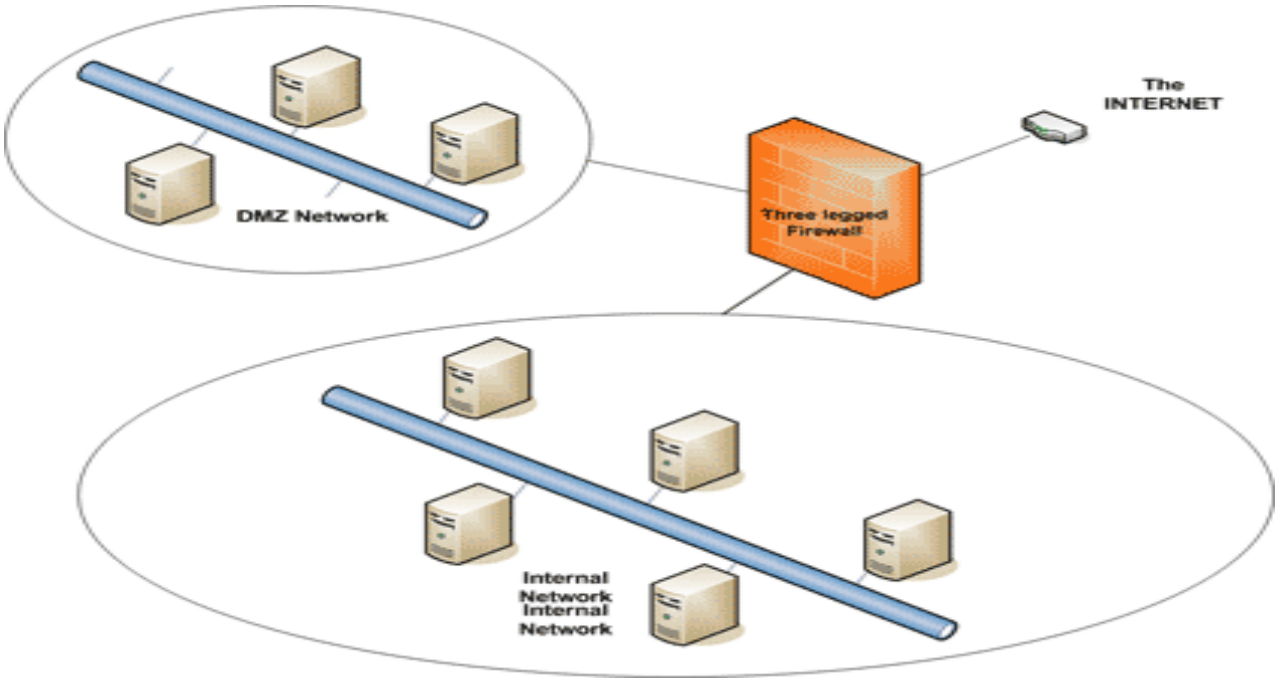
7.2 Posicionamento do Firewall



- Firewall único → No modelo acima há apenas um firewall protegendo a rede. Não há separação dos servidores do resto da rede interna, o que gera um problema de segurança. Veja o próximo modelo:

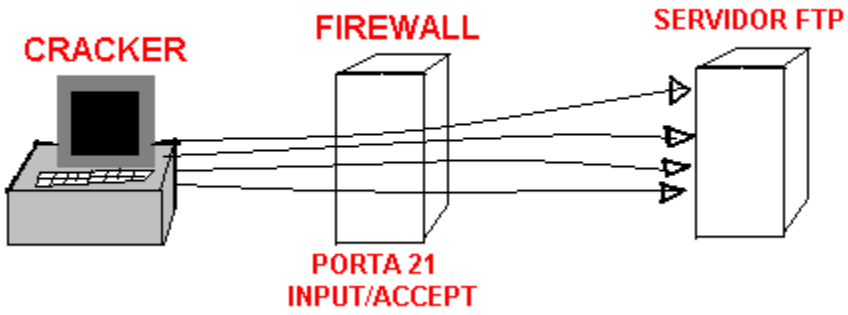
- Múltiplos Firewalls (DMZ – ZONA DESMILITARIZADA):

Utilizar mais de um Firewall. É criada a "zona desmilitarizada" onde ficam os servidores de acesso público (WEB, SMTP, FTP, ETC.). A rede interna será separada dos servidores por um segundo Firewall. Quando apenas um servidor for colocado na DMZ ele é chamado de **Bastion Host.**



6. IDS (Sistema de detecção de intrusos)

O IDS é uma ferramenta que auxilia o Firewall na segurança da rede, chegando até onde ele não alcança. A função do IDS então é monitorar o tráfego e detectar alguma atividade maliciosa. Para isso ele possui um banco de dados de regras que são consultadas e cruzadas com o tráfego em questão. Se esse cruzamento “bater”, significa que um possível ataque foi detectado. Veja um exemplo:



Neste exemplo, o Firewall não conseguirá proteger contra o ataque de força-bruta. Apenas o IDS poderá fazê-lo (ou o serviço atacado, se bloquear o usuário após um n número de tentativas).

6.1 Tipos de IDS

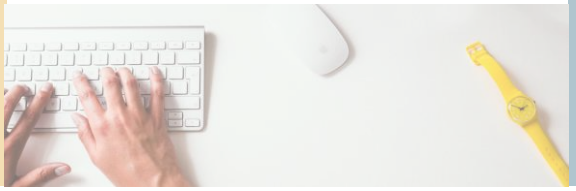
- **NIDS** (Network IDS) →

É um Sniffer (farejador). Analisa o tráfego da rede e procura/detecta ataques em potencial.

- **HIDS** (Host IDS) →

Não analisa o tráfego da rede, e sim de um único Host. Consegue ataques mais avançados, mas deve ser instalado em todas as máquinas.

- **HoneyPot →**



Pode funcionar como HIDS ou NIDS. Seu diferencial é enganar o invasor fazendo-o pensar que invadiu o sistema.

- **IPS** (Intrusion Prevention System) →

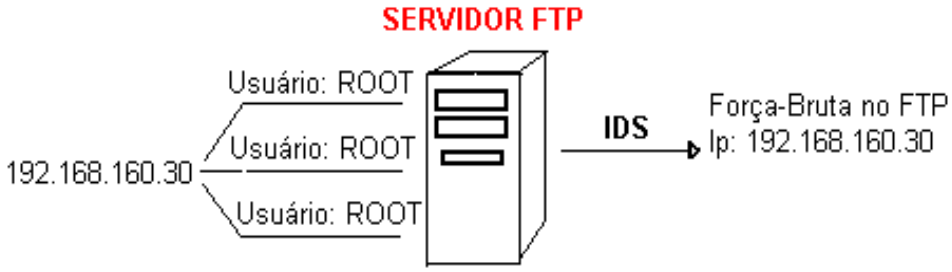
É um NIDS que além de detectar os ataques consegue impedí-los bloqueando IPs no Firewall.

6.2 Métodos de Detecção

- Assinatura →

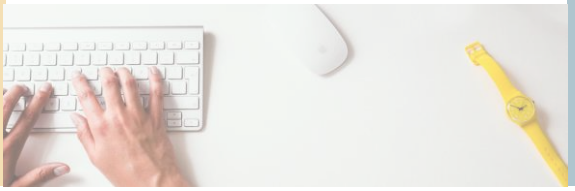
O tráfego é comparado a um banco de dados de assinaturas de ataque se o mesmo ocorrer. Esta assinatura vai "bater" e o ataque será reportado.

Ex:



- Anomalia →

Neste método é analisado o que pode ser chamado de "nível normal de tráfego" é usado como comparação. Se houver algum pico ou anormalidade, é considerado um problema.



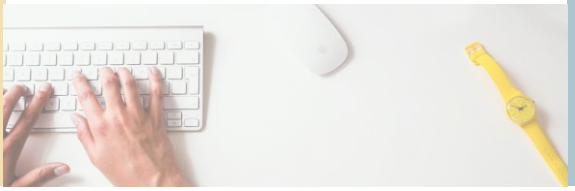
6.3 Problemas dos IDS

- Falso Positivo → É um alerta falso que o IDS emite. No caso, não ocorre ataque algum, mas o IDS alerta que sim.

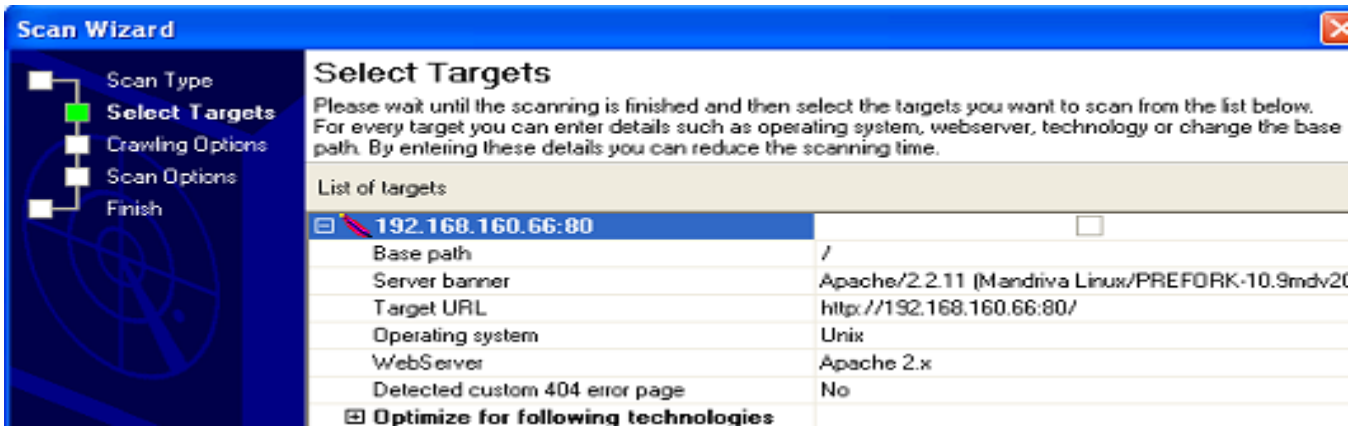
- Falso Negativo → Um ataque ocorre mas o IDS não detectou. Isso acontece muito nos NIDS por causa da criptografia. Afinal, as regras são baseadas em texto.

O Snort é um dos IDS's mais populares. É classificado por método de detecção, Análise de assinaturas, e o alvo: rede. Possui também uma grande base com 200 assinaturas. Os alertas do Snort são criados a partir dos atributos de regras citados antes. Veja um exemplo:

```
alert icmp $HOME_NET any -> $HOME_NET any (msg:"Qualquer tipo de trafego ICMP foi gerado.");

alert tcp $HOME_NET 146 -> $HOME_NET 1024 (msg:"Backdoor Activity"; content:"WHATISIT"; reference:cve,CAN-2002-0013; sid:1415; rev:2; classtype:backdoor;);
```



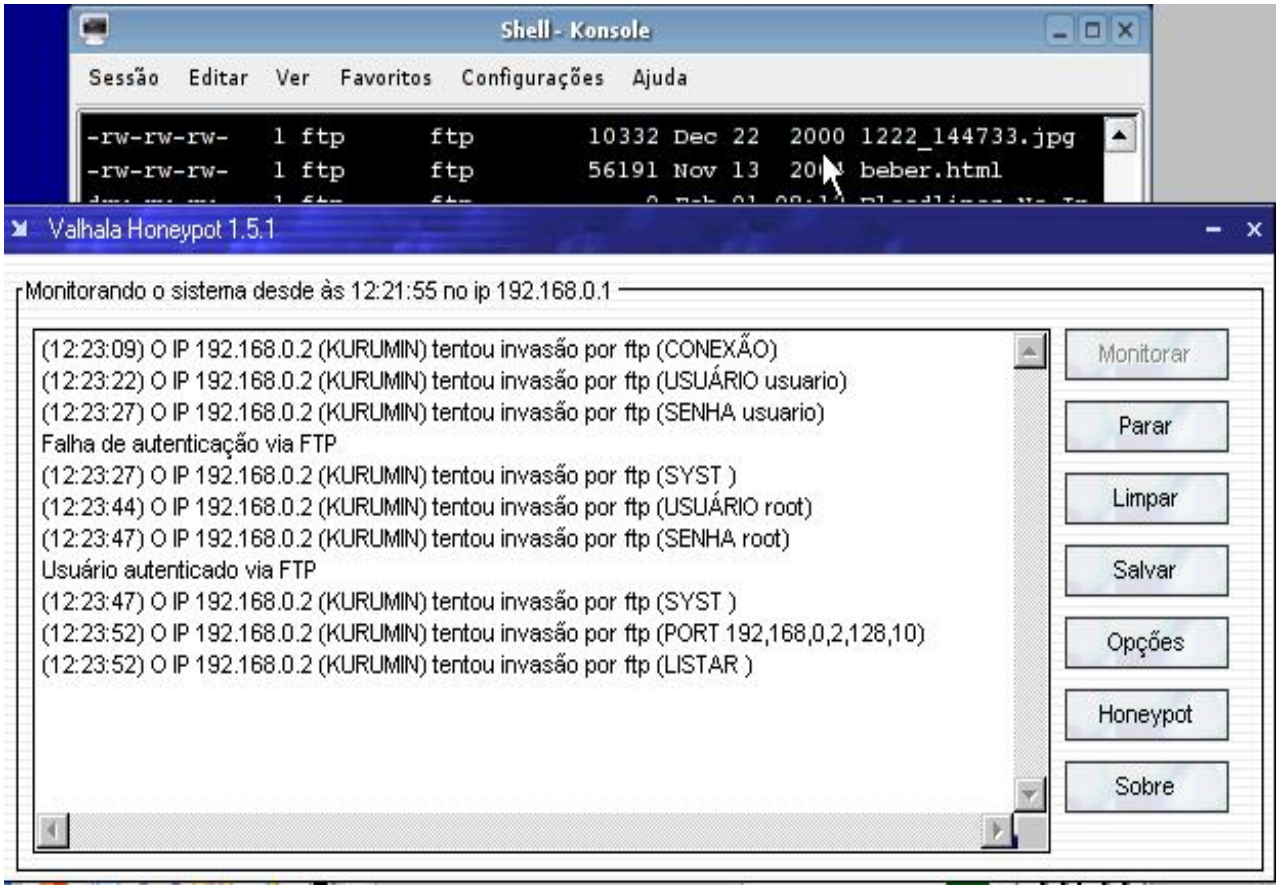
VERIFICANDO VULNERABILIDADES ATRAVÉS DE UM SCANNER (ACUNETIX)



DETECÇÃO DO IP 192.168.160.126 PELO SNORT

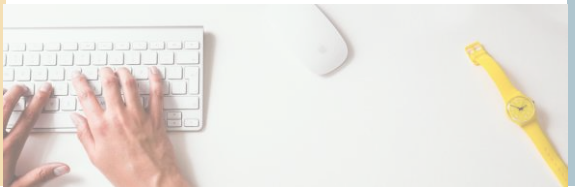
```
***AP*** Seq: 0xA946CB3E  Ack: 0xABD3DDA9  Win: 0xFE0C  TcpLen: 20
TCP TTL:128 TOS:0x0 ID:11830 IpLen:20 DgmLen:126 DF
05/20-09:48:06.300326 192.168.160.126:2674 -> 192.168.160.247:139
[Classification: Generic Protocol Command Decode] [Priority: 3]
[**] [1:538:15] NETBIOS SMB IPC$ unicode share access [**]

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref => http://cve.mitre.org/cgi
in/cvename.cgi?name=2002-0012][Xref => http://www.securityfocus.com/bid/4132][Xref => http://www.s
urityfocus.com/bid/4089][Xref => http://www.securityfocus.com/bid/4088]
TCP Options (4) => MSS: 1460 NOP NOP SackOK
*******S* Seq: 0xD9A7366A  Ack: 0x0  Win: 0xFFFF  TcpLen: 28
TCP TTL:128 TOS:0x0 ID:11568 IpLen:20 DgmLen:48 DF
05/20-09:47:48.234105 192.168.160.126:2444 -> 192.168.160.66:705
[Classification: Attempted Information Leak] [Priority: 2]
[**] [1:1421:11] SNMP AgentX/tcp request [**]
```

6.5 HoneyPots



São IDS's do tipo rede ou host que tentam enganar o usuário fazendo-o pensar que invadiu o sistema. Veja os seguintes tipos:

- **HoneyPot por software** → É utilizado um programa específico para a criação do HoneyPot. Esse programa normalmente usa serviços simulados de baixa interatividade e controla os logs por conta própria.



- **HoneyNet** → **“**Rede” real ou virtual criada para ser atacada. Composta de no mínimo duas máquinas, usa sistemas e serviços reais (alta interação). Necessita do Snort ou outro IDS para analisar o tráfego dos ataques.

- **HoneyToken** → Arquivo ou informação que desperte a curiosidade de um suporto invasor. Ex: senha.txt

  A utilização de arquivo deve ser monitorada.

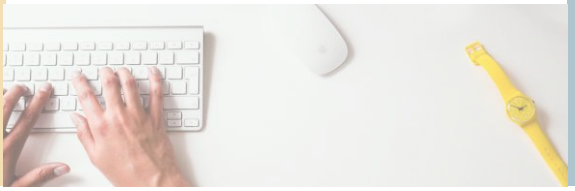
6.5.1 Tipos de Interação

- *Baixa Interação*

Os serviços do HoneyPot são simulados (Ex: Telnet, FTP, http, etc.). Portanto, não oferecem risco ao sistema. O único problema é ser de fácil descoberta pelo invasor.

- *Alta Interação*

Usa sistemas operacionais e serviços reais. Difícil de ser descoberto e permite recolher mais informações. A única limitação é que pode ser comprometido e utilizado como ponte para atacar outras máquinas.

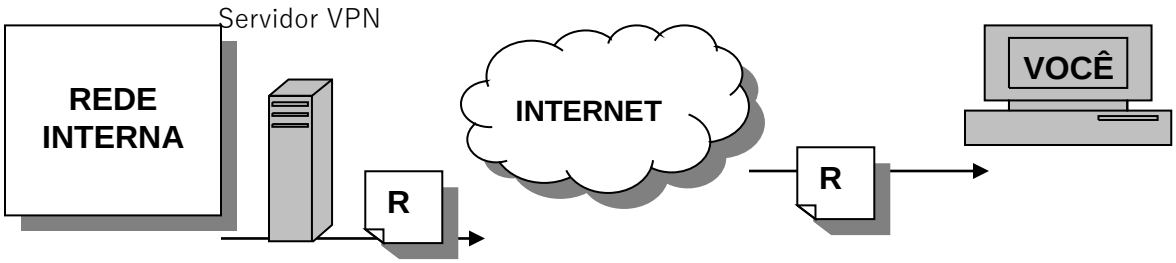


7. VPN (Virtual Private Network)

Uma VPN é uma forma segura de acessar uma rede interna através da internet.

Utilizando-se do conjunto de protocolos **IPSEC** para criptografia, a VPN torna-se também uma opção segura, além de muito prática.

Exemplo de Situação:



Na situação acima, imagine que você viajando e soube que o servidor DNS caiu. Você terá de ir até o escritório ou acessará a rede interna remotamente.

O servidor VPN permite "conceder" um IP privado para um PC remoto (público), através da internet. Ex: