TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 11. Session Hijacking

Módulo 12. Evading IDS, Firewalls, and Honeypots

Módulo 13. Hacking Web Servers

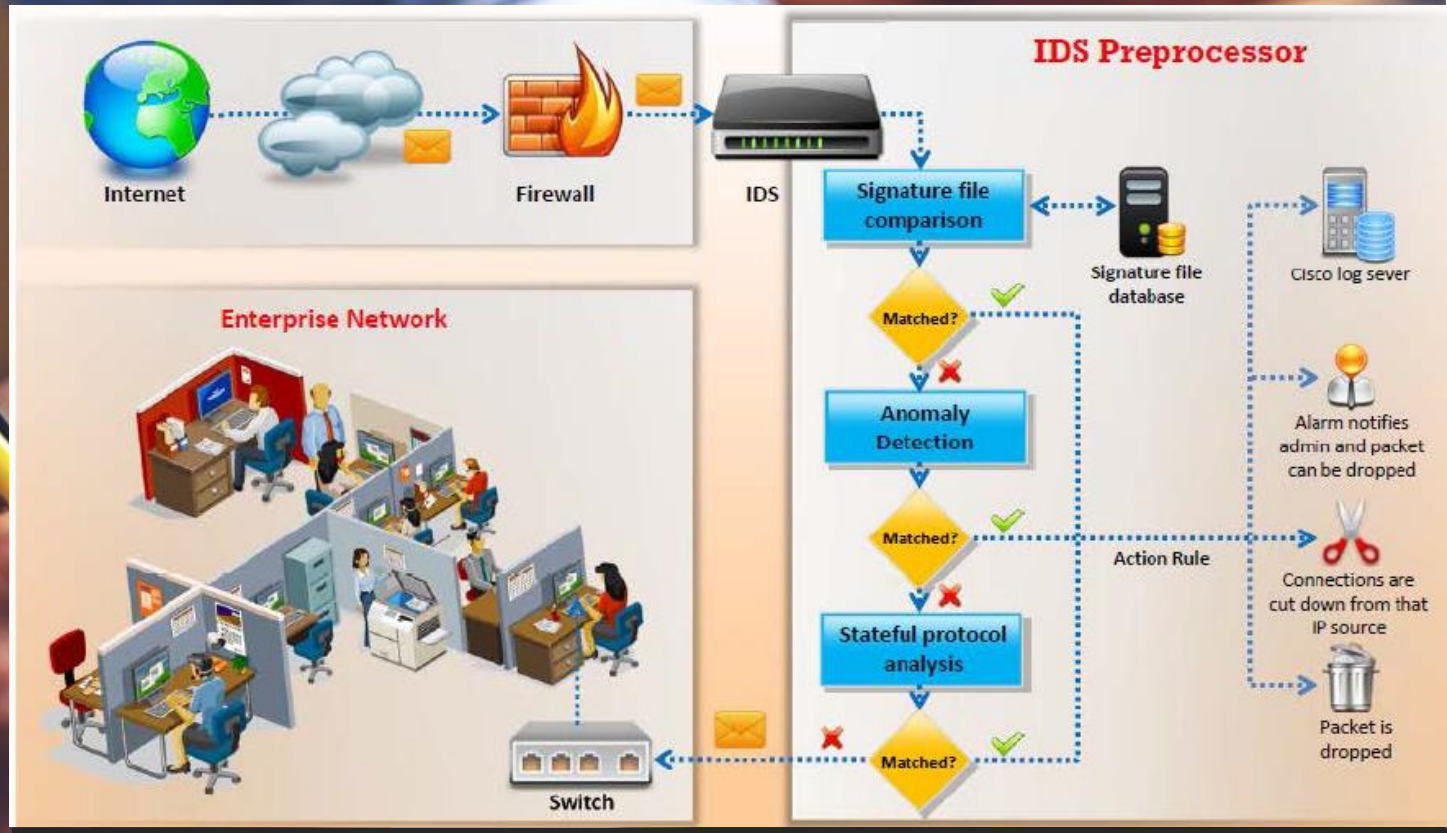
Módulo 14. Hacking Web Applications

Módulo 15. SQL Injection

Conceitos de IDS:

Um sistema de detecção de intrusão é utilizado para monitorar e proteger redes ou sistemas contra atividades maliciosas. Para alertar a equipe de segurança sobre intrusões, sistemas de detecção de intrusão são muito úteis. Ideias são utilizadas para monitorar o tráfego de rede. Um IDS verifica atividades suspeitas e notifica o administrador sobre intrusões imediatamente.

Um sistema de detecção de intrusão (IDS) reúne e analisa as informações a partir de um computador ou uma rede, para identificar as possíveis violações da política de segurança, incluindo o acesso não autorizado, bem como uso indevido de recursos. Um IDS também é referido como "packet-sniffer", que intercepta pacotes que passam por vários meios de comunicação e protocolos.

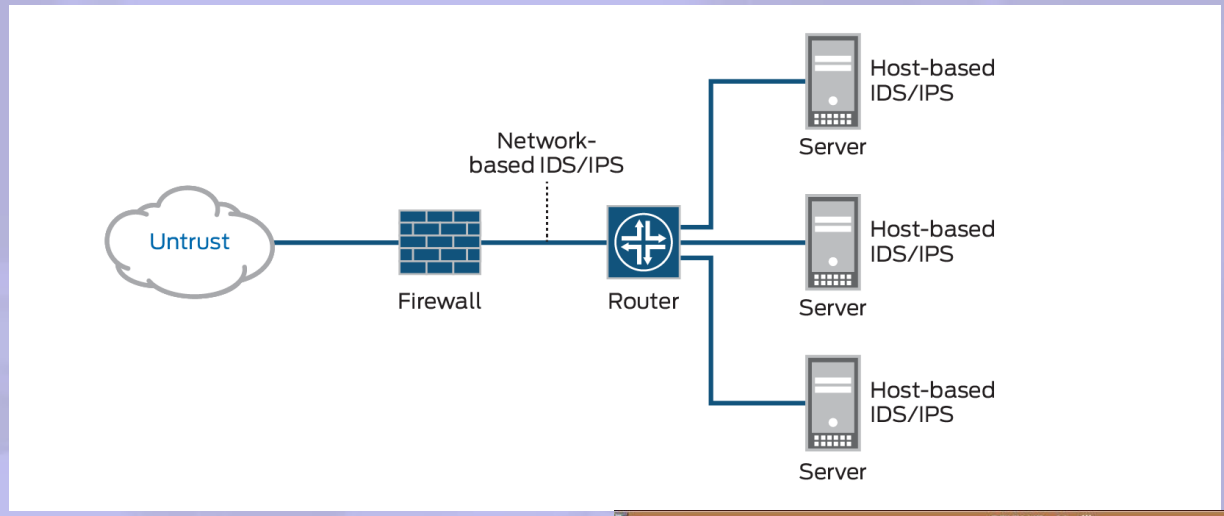


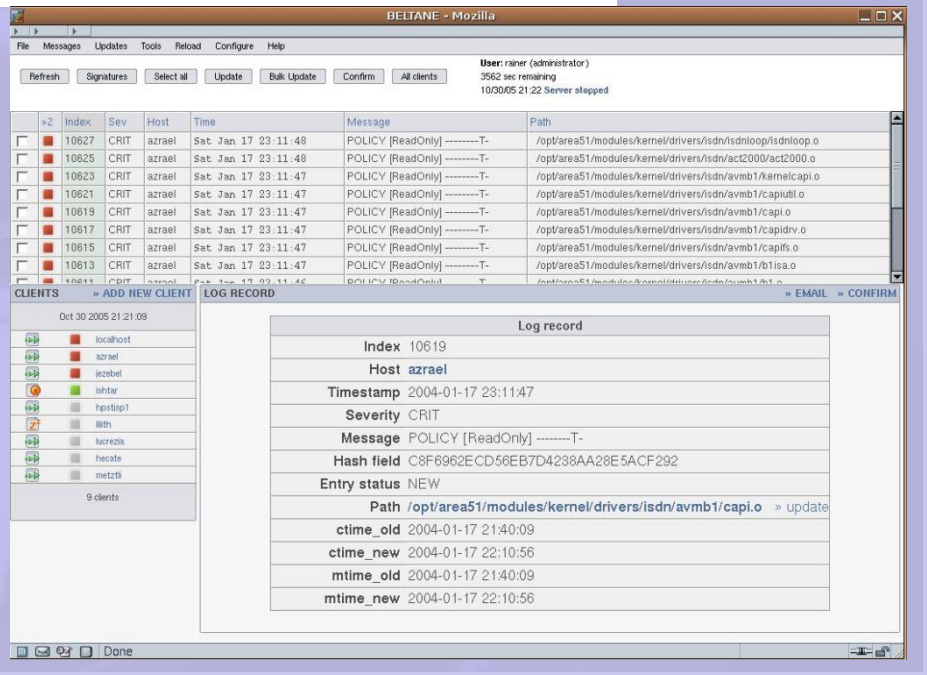
CEHv12 (ANSI)

12.Evading IDS, Firewalls, and Honeypots

Tipos de IDS

- Detecção de Intrusão baseado em rede
- Detecção de Intrusão baseado em Host
- Log Monitoring File
- Verificação de integridade de arquivos





Maneiras de detecção

- **Reconhecimento de assinatura**

É conhecido como detecção de uso indevido. o reconhecimento de assinatura tenta identificar eventos que indicam uso indevido de um recurso do sistema

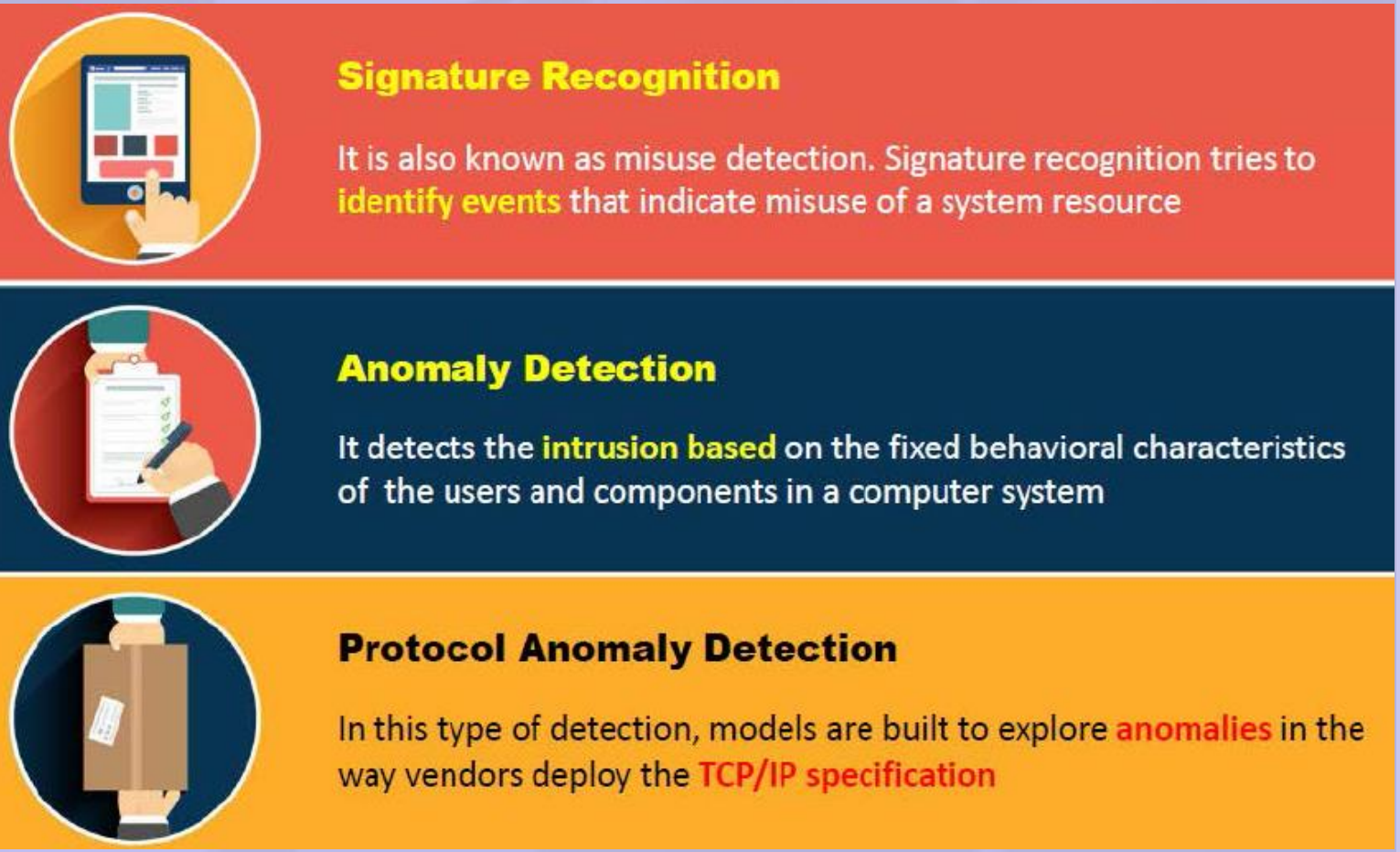
- **Detecção de anomalia**

Ele detecta a intrusão com base nas características comportamentais fixas dos usuários e componentes em um sistema de computador

- **Detecção de anomalia de protocolo**

Neste tipo de detecção, os modelos são construídos para explorar anomalias na forma como os fornecedores implementam a especificação TCP/IP

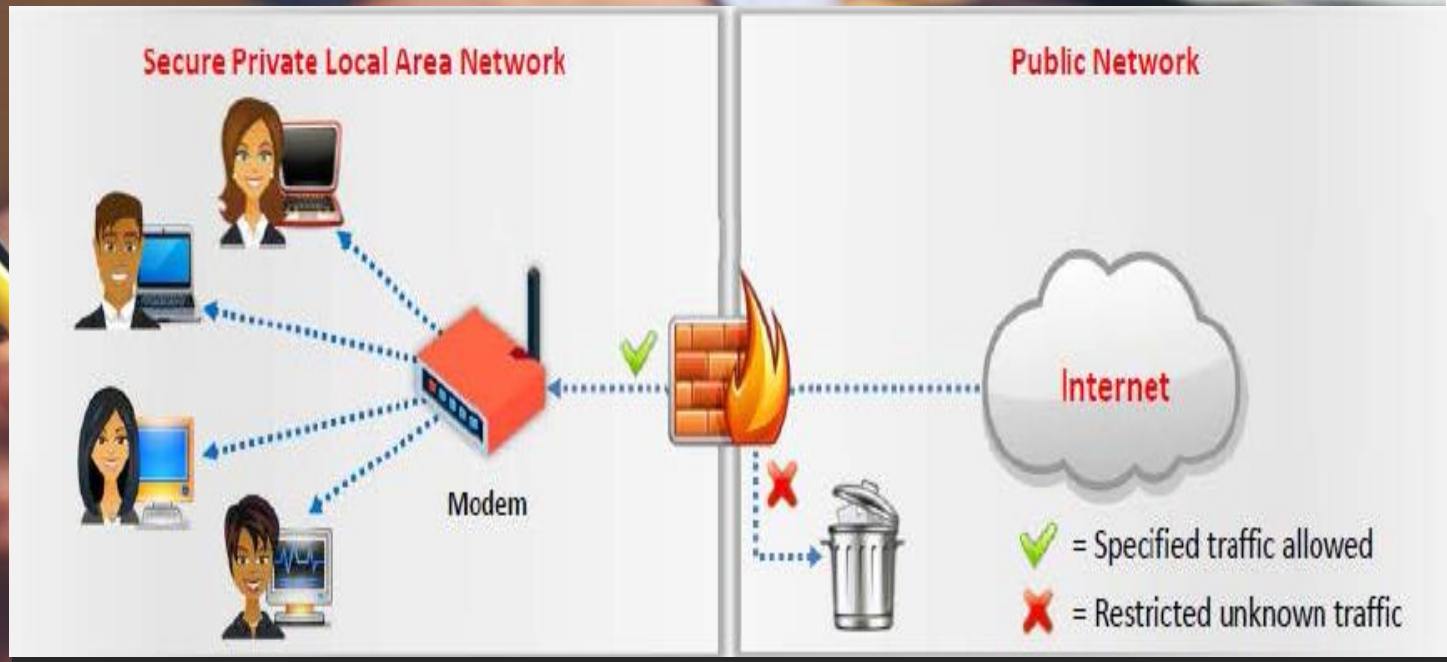
Maneiras de detecção



Conceitos de Firewall:

Um firewall refere-se a um dispositivo de hardware ou um programa de software utilizado em um sistema para evitar que informações maliciosas passem, permitindo apenas a informação aprovada. Firewalls são principalmente classificados em quatro tipos:

- Packet filters
- Circuit-level gateways
- Application-level gateways
- Stateful multilayer inspection firewalls

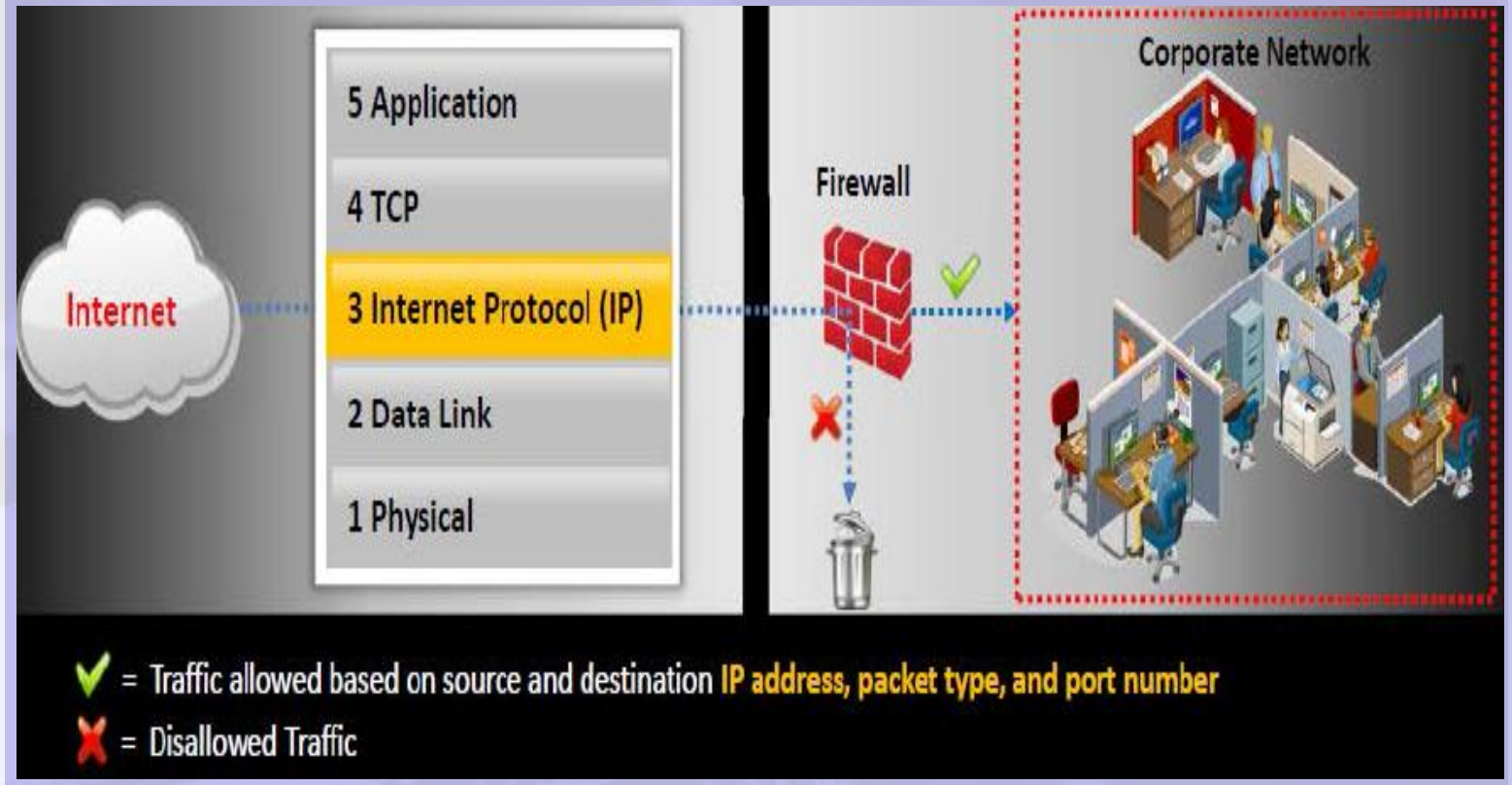


CEHv12 (ANSI)

Conceitos de Firewall

Packet Filter

- Endereço IP da origem;
- Endereço IP do destino;
- O protocolo (se o pacote é um pacote TCP, UDP ou ICMP);
- A porta TCP ou UDP de origem;
- A porta TCP ou UDP de destino.



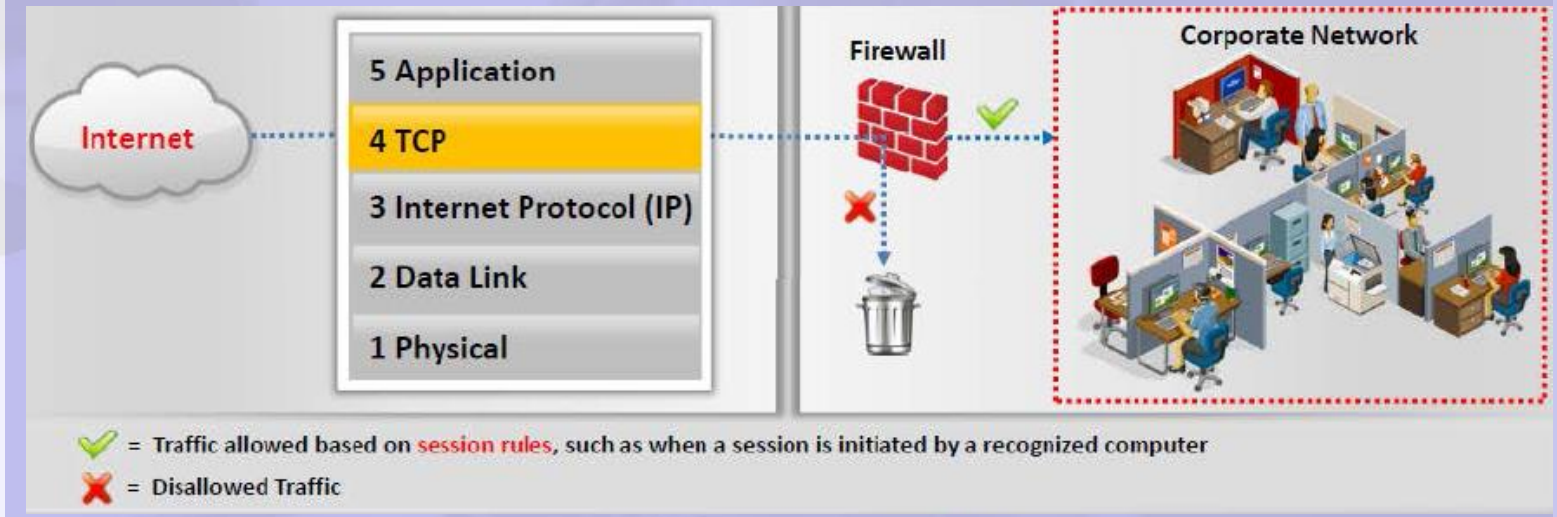

```
[root@localhost ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:23
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]# _
```

Circuit-level Gateway

- Para detectar se uma sessão solicitada é válida ou não, ele verifica o handshaking TCP entre os pacotes. Gateways no nível do circuito não filtram pacotes individuais. Gateways no nível do circuito são relativamente baratos e ocultam as informações sobre a rede privada que eles protegem.

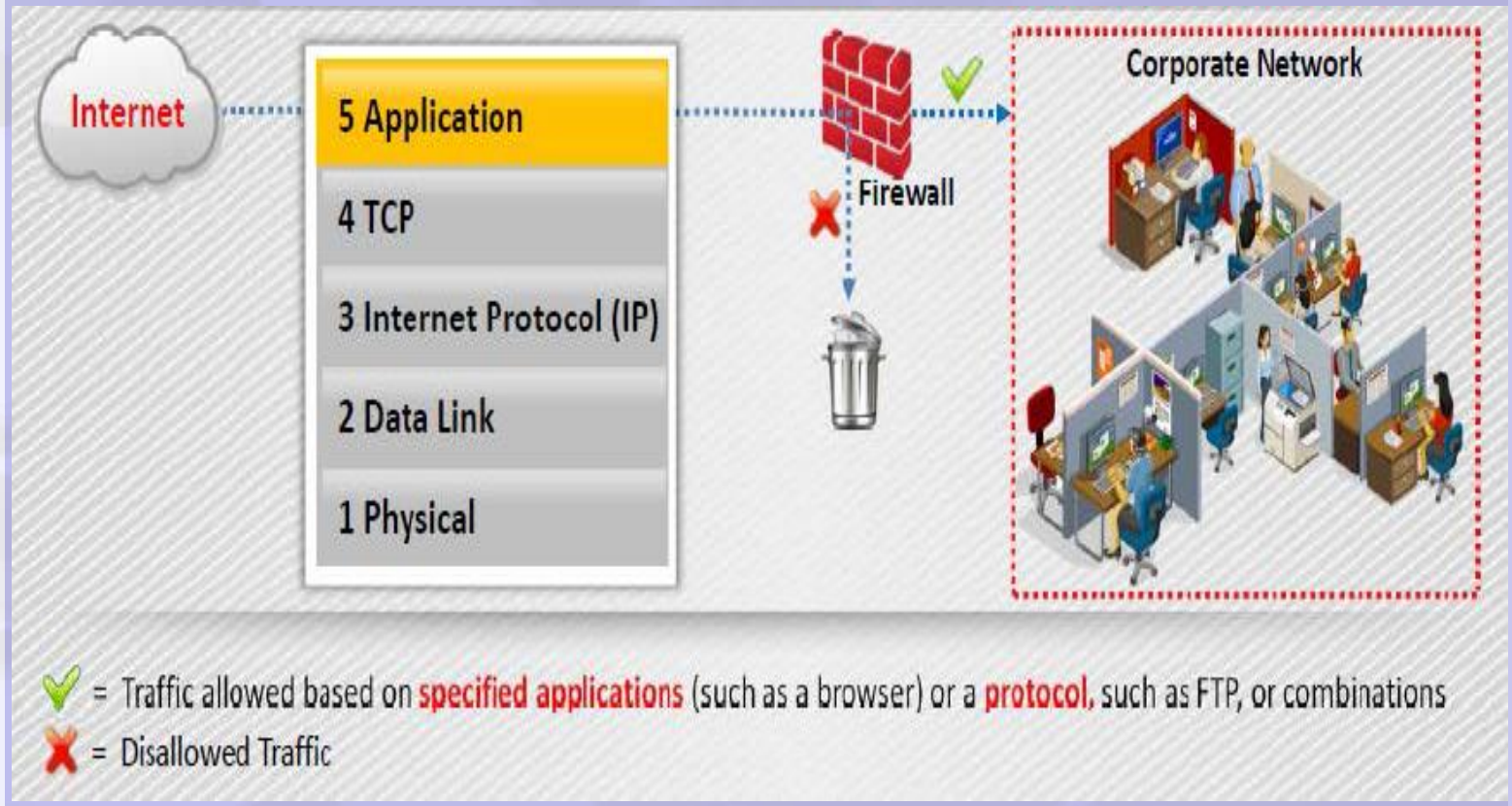


Application-level

- Um firewall de aplicação é utilizado principalmente como um aprimoramento do programa de firewall padrão, fornecendo serviços de firewall até a camada de aplicação. Alguns dos serviços executados por um firewall de aplicação incluem controlar a execução de aplicativos, manipulação de dados, bloquear a execução de códigos maliciosos e muito mais.

Existem dois tipos de firewalls de aplicação:

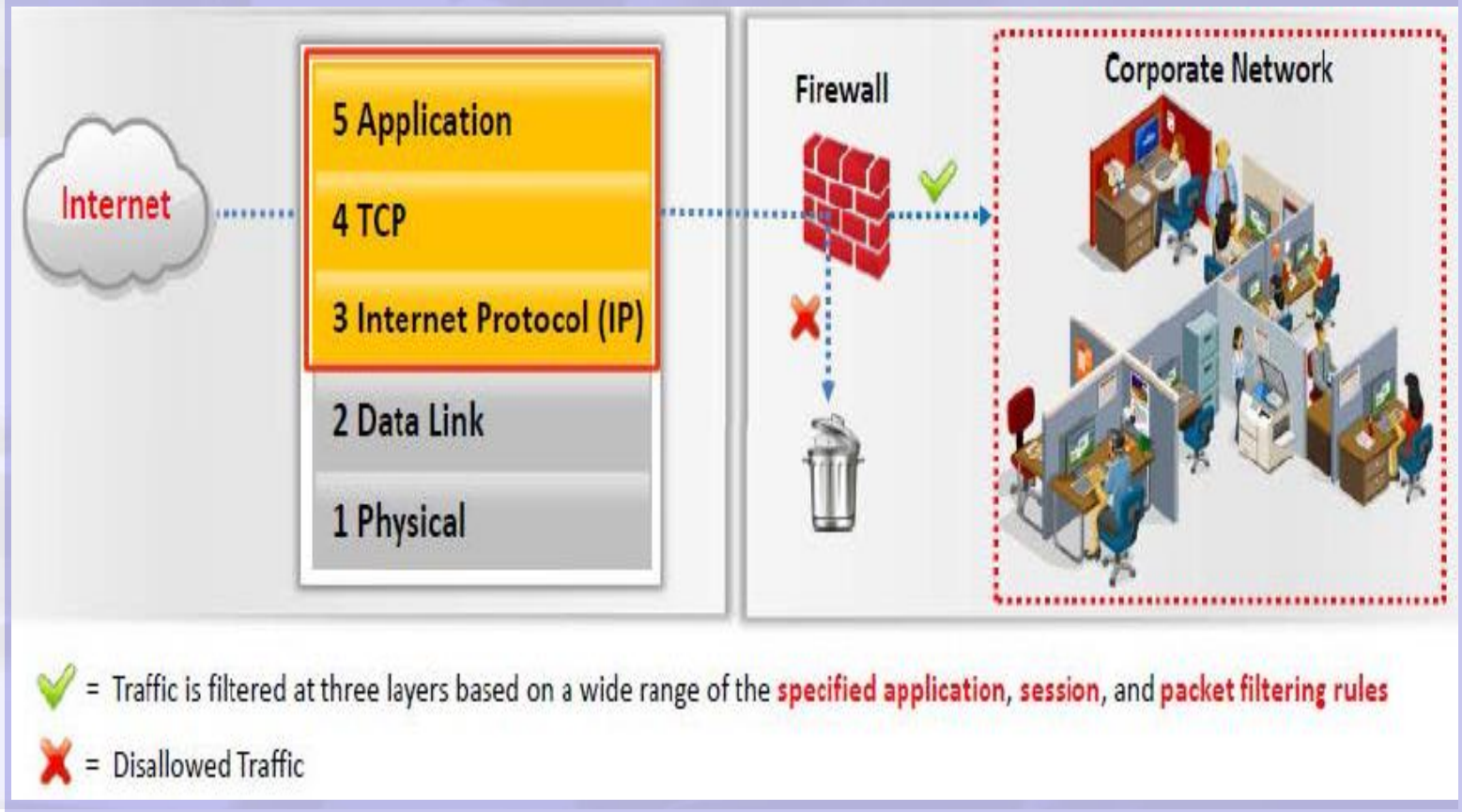
- Firewalls de aplicação baseados em rede: verifica e monitora o tráfego baseado em rede destinado à camada de aplicação.
- Firewalls de aplicação baseados em host: Monitora todo o tráfego de entrada e saída iniciado por um aplicativo ou serviço em um computador, sistema ou host local.



Stateful Inspection

- Um firewall stateful coleta dados sobre cada conexão feita por ele. Todos esses pontos de dados formam perfis de conexões “seguras”. Quando uma conexão subsequente é tentada, ela é verificada na lista de atributos coletados pelo firewall stateful. Se tiver as qualidades de uma conexão segura, pode ocorrer. Caso contrário, os pacotes de dados são descartados. Os pacotes de dados contêm informações sobre os dados contidos neles. Um firewall stateful realiza a inspeção de pacotes, que verifica o conteúdo dos pacotes para ver se eles representam ameaças.

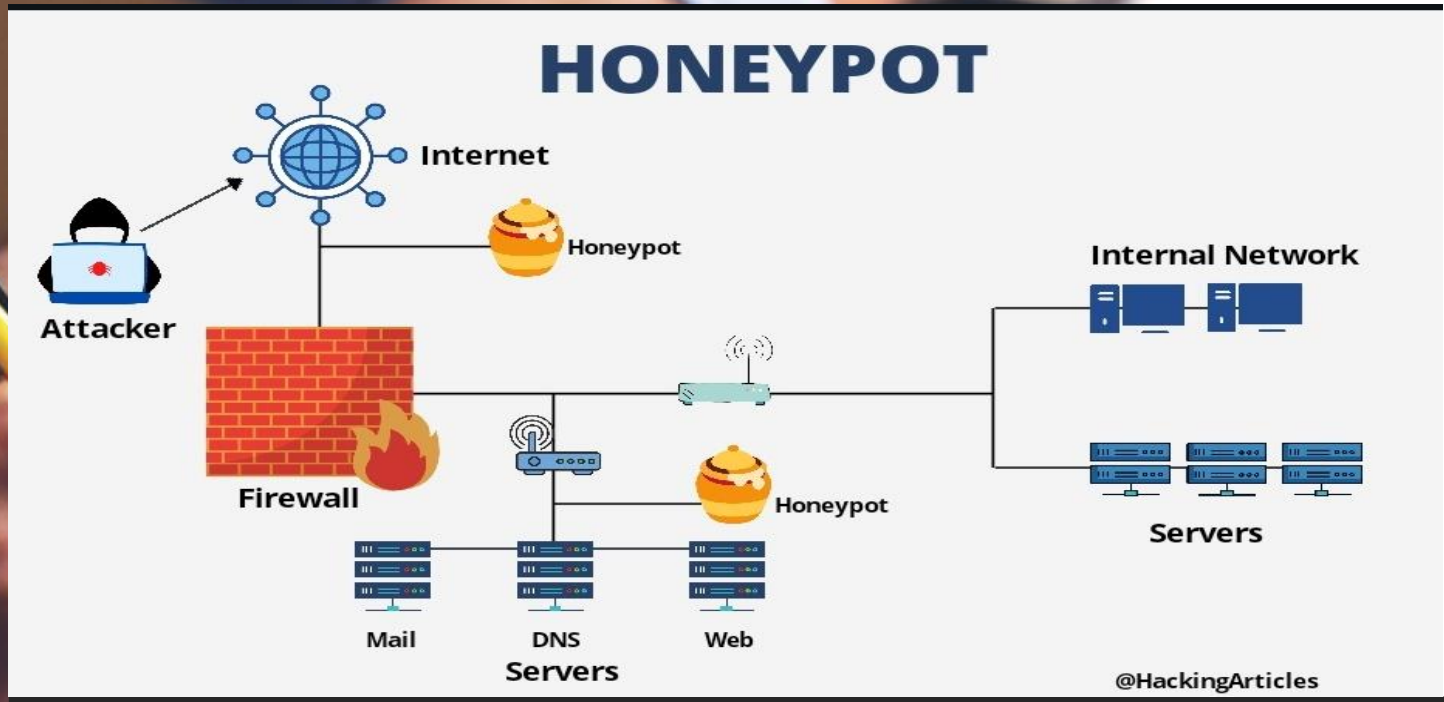
O estado é o status mais recente ou imediato de um processo ou aplicativo. Em um firewall, o estado das conexões é armazenado, fornecendo uma lista de conexões com a qual comparar a conexão que um usuário está tentando fazer. Os dispositivos que rastreiam o estado determinam quais estados são seguros e quais representam ameaças.



Conceitos de Honeypot:

Um honeypot é um sistema que se destina a atrair e prender as pessoas que tentam a utilização não autorizada ou ilícita do sistema. Sempre que houver qualquer interação com um honeypot, é mais provável que seja uma atividade maliciosa. Honeypots são únicos, eles não resolvem um problema específico.

Em vez disso, eles são uma ferramenta altamente flexível com muitas aplicações de segurança diferentes. Alguns honeypots podem ser utilizados para ajudar a prevenir os ataques, outros podem ser utilizados para detectar os ataques enquanto alguns honeypots podem ser utilizados para recolher informações e pesquisa.

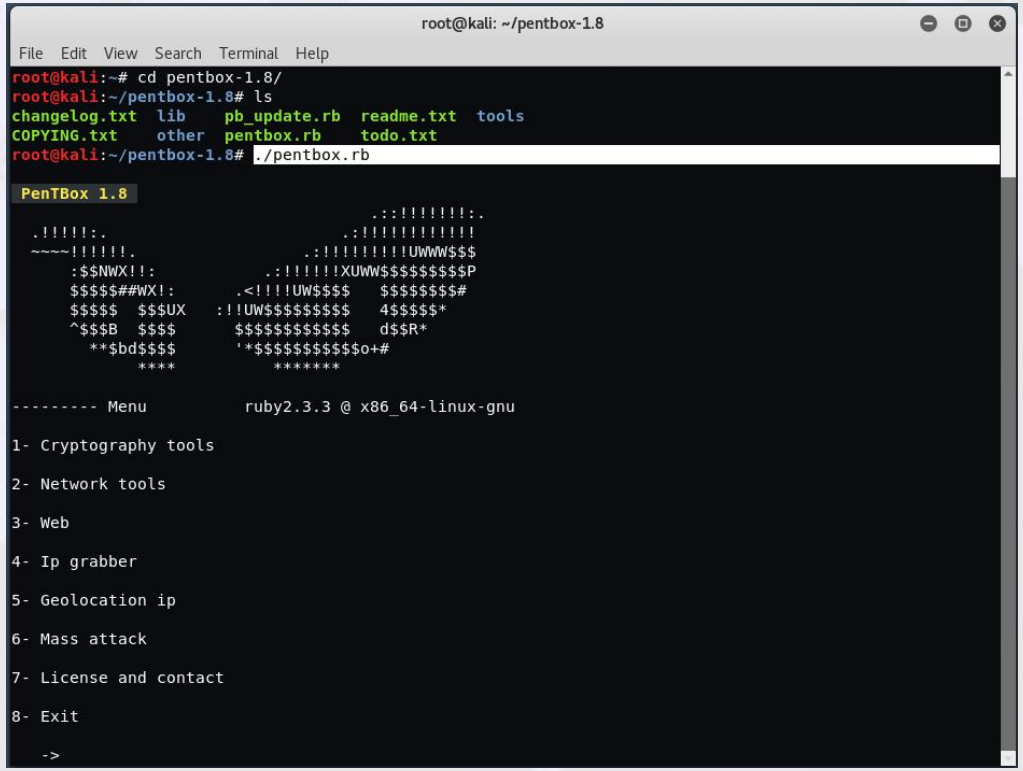


CEHv12 (ANSI)

12.Evading IDS, Firewalls, and Honeypots

Honeypot

O honeypot é um sistema conectado à rede e configurado como chamariz para atrair os ataques cibernéticos detectando, desviando e estudando as tentativas dos hackers em obter acesso não autorizado aos sistemas de informação.



Técnicas de bypass de IDS

Ataques de evasão são devastadores para a precisão do IDS. Um ataque de evasão na camada IP permite que um atacante tente ataques arbitrários contra os hosts em uma rede, sem o IDS nunca perceber. O atacante envia partes do pedido em pacotes que o IDS erroneamente rejeita, permitindo a remoção de partes do fluxo de vista do sistema de identificação. Por exemplo, se a sequência maliciosa é enviado byte-por-byte, e um byte é rejeitada pelo IDS, o IDS não consegue detectar o ataque.

Técnicas de bypass de IDS

Ofuscação

Significa tornar o código mais difícil de entender ou ler, geralmente para fins de segurança ou privacidade. Uma ferramenta chamada ofuscador às vezes é utilizada para converter um programa simples em um que funciona da mesma maneira, mas é muito mais difícil de entender.

Geração de falso positivo

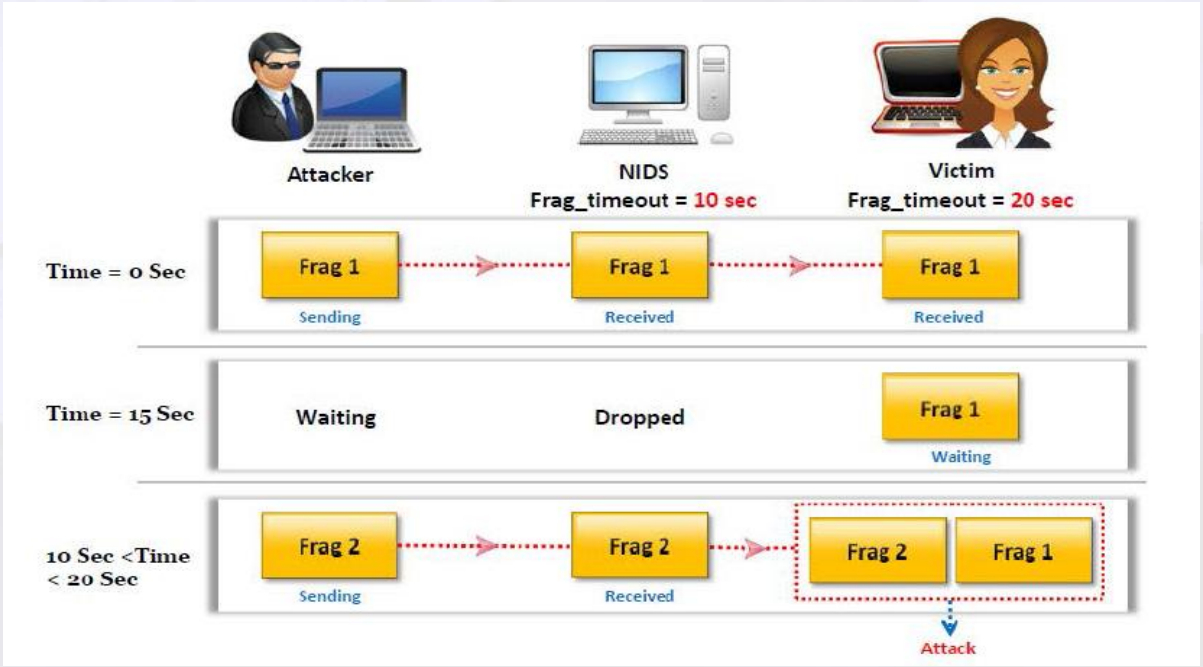
Este modo não ataca o alvo, mas em vez disso, ele faz algo relativamente normal. Neste modo, é gerado um alarme quando nenhuma condição está presente para justificar. Outro ataque é gerar uma grande quantidade de dados de alerta que tem que ser registado.

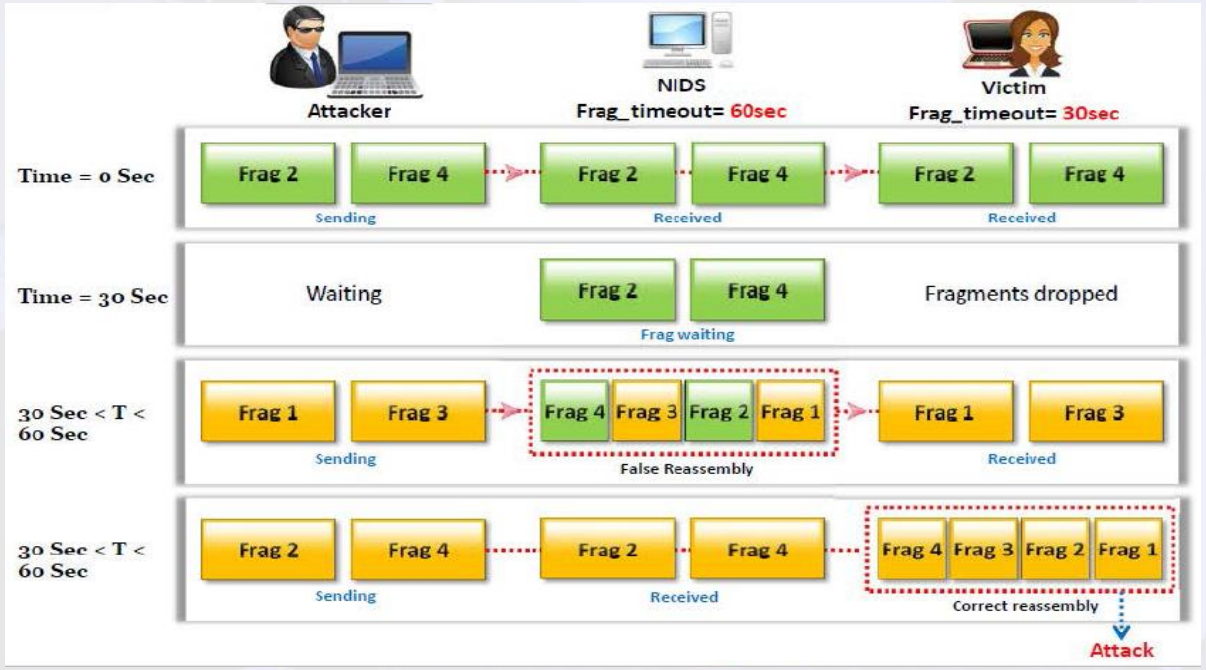
Os atacantes geram pacotes conhecidos para acionar alertas dentro dos IDS, forçando-o a gerar um grande número de falsos positivos. Este tipo de ataque é projetado para criar uma grande quantidade de log "ruído" em uma tentativa de misturar ataques reais com falsos.

Técnicas de bypass de IDS

Fragmentação

As atacantes quebram o datagrama IP em vários pacotes de menor tamanho. O timeout de remontagem de fragmentação do IDS é inferior ao time-out de remontagem da vítima.





Técnicas de bypass de Firewall

Firewalls são os mecanismos de segurança implementados em uma rede ou um sistema para se proteger contra ataques. Atacantes tentam contornar firewalls de modo que eles possam burlar os mecanismos de segurança e obter acesso ao sistema ou rede.

Técnicas de bypass de Firewall

IP Spoofing

A falsificação de endereço IP é uma das maneiras que um invasor tenta utilizar para fugir das restrições do firewall. IP spoofing é uma técnica onde o atacante cria pacotes do protocolo de internet usando um endereço IP e ganha acesso forjado ao longo do sistema ou rede sem autorização.

Tunelamento HTTP

Este método pode ser implementado se a empresa-alvo tiver um servidor web público com a porta 80 utilizada para o tráfego HTTP, que não é filtrada em seu firewall. Muitos firewalls não examinam a carga útil de um pacote HTTP para confirmar se ele é um tráfego HTTP legítimo, assim é possível tunelar o tráfego na porta TCP 80.

Tiny Fragments

O atacante utiliza a técnica de fragmentação IP para criar fragmentos extremamente pequenos e forçar as informações de cabeçalho TCP para o próximo fragmento. Isto pode resultar em um caso em que o campo de flag TCP é forçado para o segundo fragmento, e o filtro não será capaz de verificar estas flags no primeiro octeto, assim, ignorando os fragmentos subsequentes.

Tiny Fragments ocorre quando um pequeno fragmento de pacote entra no servidor. Isso acontece quando um dos fragmentos é tão pequeno que nem cabe no próprio cabeçalho. Parte do cabeçalho desse pacote é enviada como um novo fragmento. Isso pode causar problemas de remontagem e desligar um servidor.

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.