Instituto Infnet

Segurança Da Informação

FABIANO GISBERT

Segurança em Sistemas Operacionais

Windows

Trace Route

TRACERT (Trace Route) é um utilitário de linha de comando que pode ser usado para rastrear o caminho que um pacote IP (Internet Protocol) faz até o seu destino.

```
C:\Users>tracert lms.infnet.edu.br

Rastreando a rota para lms.infnet.edu.br [64.37.61.82]
com no máximo 30 saltos:

  1     2 ms     2 ms     3 ms  192.168.1.254
  2     4 ms     4 ms     4 ms  10.255.255.3
  3     4 ms     4 ms     5 ms  [redacted].0.37
  4    10 ms    44 ms     9 ms  8.243.35.81
  5   215 ms   113 ms   183 ms  ae1.6.bar3.Orlando1.level3.net [4.69.219.118]
  6   114 ms   112 ms   111 ms  HOSTDIME.bar3.Orlando1.Level3.net [63.209.125.22]
  7   121 ms   117 ms   212 ms  198-49-72-69.static.hostdime.com [198.49.72.69]
  8   122 ms   191 ms   199 ms  host107.nucleoead.net [64.37.61.82]

Rastreamento concluído.
```

O utilitário de diagnóstico TRACERT determina a rota para um destino enviando pacotes eco ICMP (Internet Control Message Protocol) para o destino.

Nesses pacotes, o TRACERT usa vários valores de tempo de vida útil (TTL) de IP.

Objetivo: Encontrar desvios de rota, MitM

Windows

Instituto Infnet

Netstat

Exibe conexões TCP ativas, portas nas quais o computador está em escuta, estatísticas de Ethernet, tabela de roteamento de IP, estatísticas de IPv4 (para os protocolos IP, ICMP, TCP e UDP) e estatísticas de IPv6 (para os protocolos IPv6, ICMPv6, TCP sobre IPv6 e UDP sobre IPv6). Usado sem parâmetros, esse comando exibe conexões TCP ativas.

-a Exibe todas as conexões TCP ativas e as portas TCP e UDP nas quais o computador está em escuta.
-b Exibe o executável envolvido na criação de cada conexão ou porta de escuta.
-E Exibe estatísticas de Ethernet, como o número de bytes e pacotes enviados e recebidos. Esse parâmetro pode ser combinado com -s.
-n Exibe conexões TCP ativas, no entanto, endereços e números de porta são expressos numericamente e nenhuma tentativa é feita para determinar nomes.
-o Exibe conexões TCP ativas e inclui a ID do processo (PID) para cada conexão. Você pode encontrar o aplicativo com base no PID na guia Processos no Gerenciador de Tarefas do Windows. Esse parâmetro pode ser combinado com -a, -n e -b

Windows

Instituto Infnet

Netstat

```
C:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1128
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       348
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       896
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       448
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       680
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1128
  TCP    [::]:49152             [::]:0                 LISTENING       348
  TCP    [::]:49153             [::]:0                 LISTENING       772
  TCP    [::]:49154             [::]:0                 LISTENING       896
  TCP    [::]:49155             [::]:0                 LISTENING       432
  TCP    [::]:49156             [::]:0                 LISTENING       448
  UDP    0.0.0.0:5355           *:*                                    1128
```

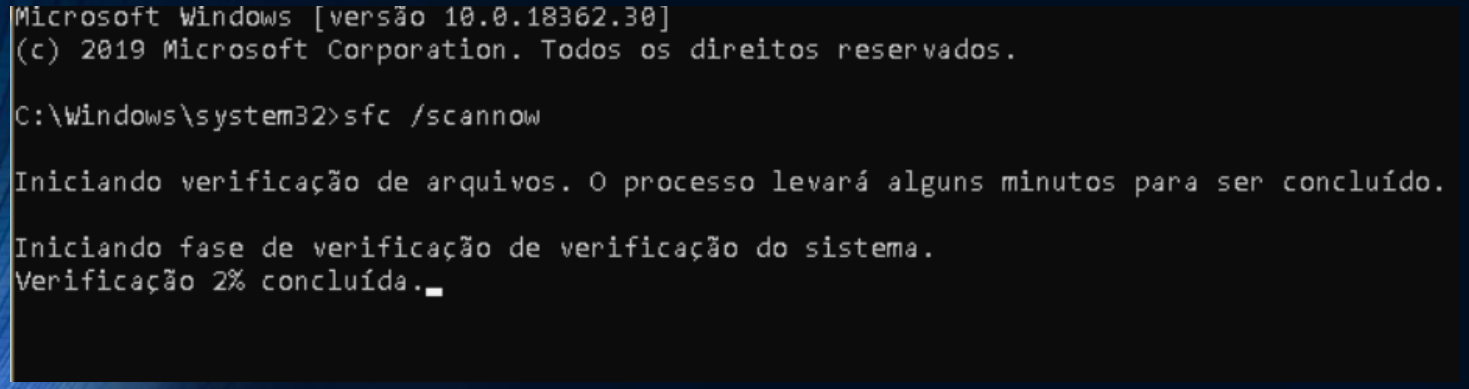
Objetivo: Encontrar backdoors e Worms

Windows

Instituto Infnet

Verificador de Arquivos de Sistema - SFC

O comando sfc /scannow verificará todos os arquivos protegidos do sistema, substituindo os arquivos corrompidos por uma cópia em cache que está localizada em uma pasta compactada em %WinDir%\System32\dllcache.
O espaço reservado %WinDir% representa a pasta do sistema operacional Windows. Por exemplo, C:\Windows.



Objetivo: restaurar arquivos de sistemas modificados ou danificados por vírus

https://support.microsoft.com/pt-br/topic/use-a-ferramenta-verificador-de-arquivos-do-sistema-para-reparar-arquivos-de-sistema-ausentes-ou-corrompidos-79aa86cb-ca52-166a-92a3-966e85d4094e

Windows

Tasklist

Exibe uma lista de processos em execução atualmente no computador local ou em um computador remoto. O comando tasklist /svc mostra a lista de serviços ativos e suas dependências. O comando tasklist /m mostra os serviços que são ativados na inicialização do Windows.

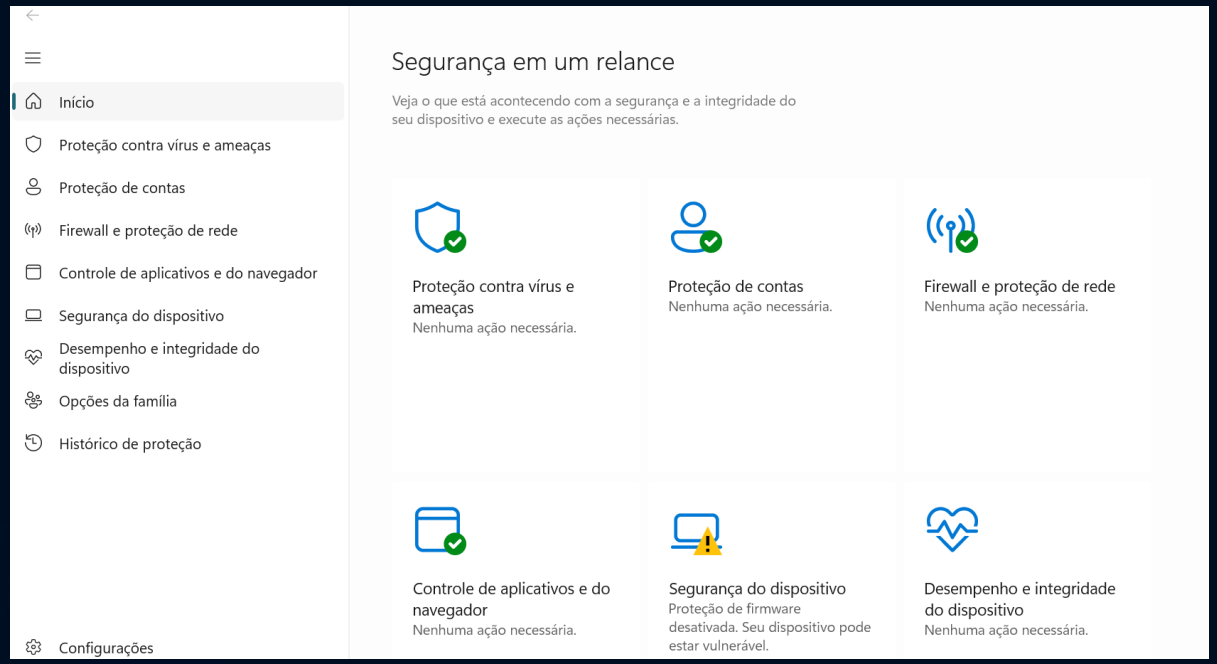
```
C:\Users>tasklist /svc

Nome da imagem            Identifi Serviços
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Secure System                  108 N/A
Registry                       144 N/A
smss.exe                       624 N/A
csrss.exe                     1000 N/A
wininit.exe                      8 N/A
csrss.exe                     1032 N/A
services.exe                  1084 N/A
LsaIso.exe                    1104 N/A
lsass.exe                     1116 EFS, KeyIso, Netlogon, SamSs, VaultSvc
winlogon.exe                  1184 N/A
svchost.exe                   1312 BrokerInfrastructure, DcomLaunch, PlugPlay,
                                   Power, SystemEventsBroker
WUDFHost.exe                  1344 N/A
fontdrvhost.exe               1388 N/A
fontdrvhost.exe               1396 N/A
svchost.exe                   1492 RpcEptMapper, RpcSs
svchost.exe                   1552 LSM
svchost.exe                   1684 TermService
svchost.exe                   1704 HvHost
svchost.exe                   1712 BDESVC
```

Objetivo: Verificar se algum bot está ativando serviços zumbis no sistema.

Windows

Microsoft Defender

Microsoft Defender é um aplicativo que ajuda a manter a segurança do sistema operacional para que ele permaneça online com proteção contra malware, proteção da Web, notificações de segurança em tempo real e dicas de segurança.



Inclui diversos serviços de proteção, entre eles:

Microsoft Defender Antivírus: Uma solução de proteção de última geração que vem com o Windows 11, o Microsoft Defender Antivírus é uma proteção antivírus sempre ativa em tempo real.

Microsoft Defender SmartScreen: Se um site, aplicativo ou download for potencialmente mal-intencionado e puder danificar o computador, o SmartScreen avisará você.

Windows

Instituto Infnet

Microsoft Defender

Firewall Windows: O Firewall do Windows pode ajudar a impedir que um hacker ou software mal-intencionado obtenha acesso ao PC por meio da Internet ou de uma rede.

Regras de firewall
As regras de firewall identificam o tráfego de rede permitido ou bloqueado e as condições para que isso aconteça. As regras oferecem uma ampla seleção de condições para identificar o tráfego, incluindo:

- Nome do aplicativo, do serviço ou do programa
- Endereços IP de origem e de destino
- Pode fazer uso de valores dinâmicos, como gateway padrão, servidores DHCP, servidores DNS e sub-redes locais
- Nome ou tipo de protocolo. Para protocolos de camada de transporte, TCP e UDP, você pode especificar portas ou intervalos de porta. Para protocolos personalizados, você pode usar um número entre o e 255 representando o protocolo IP
- Tipo de interface
- Tipo e código de tráfego ICMP/ICMPv6

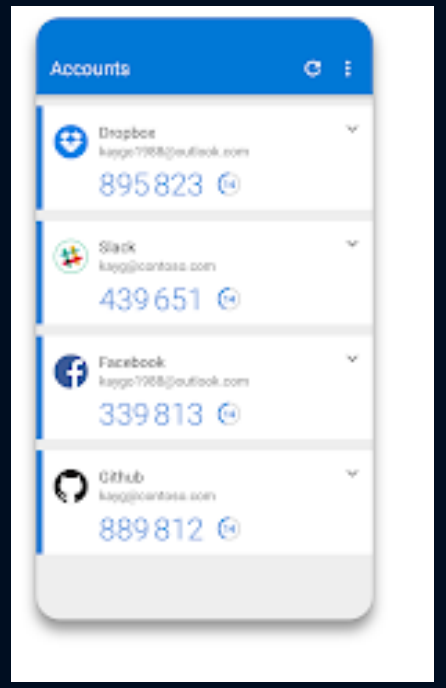
Windows

Microsoft Defender

Proteção Bluetooth: Verifica se os dispositivos conectados via bluetooth estão se conectando com os requisitos mínimos de segurança.

VPN (redes virtuais privadas): Uma VPN, ou rede virtual privada, é um túnel seguro que conecta seu PC e a Internet. Uma variedade de aplicativos VPN estão disponíveis na Microsoft Store.

Windows Hello: O Windows Hello permite autenticação multifator ao logar no Windows.



https://www.microsoft.com/pt-br/security/mobile-authenticator-app

Aplicativo Microsoft Authenticator
O aplicativo Microsoft Authenticator fornece logons fáceis e seguros para todas as suas contas online usando autenticação multifator, logon de telefone sem senha ou preenchimento automático de senha

Windows

AppLocker

O AppLocker foi introduzido com o Windows 7 e permite que as organizações controlem quais aplicativos podem ser executados em seus clientes Windows. O AppLocker ajuda a impedir que os usuários finais executem software não aprovado em seus computadores, ou que não atende aos critérios de manutenção para ser um recurso de segurança.

As políticas do AppLocker podem ser aplicadas a todos os usuários em um computador ou a usuários e grupos individuais. As regras do AppLocker podem ser definidas com base em:

- Atributos dos certificados de codificação usados para assinar um aplicativo e seus binários.
- Atributos dos binários do aplicativo provenientes dos metadados assinados para os arquivos, como Nome de Arquivo Original e versão, ou o hash do arquivo.
- O caminho do qual o aplicativo ou o arquivo é iniciado.

Windows

Instituto Infnet

Controle de Aplicativos – WDAC

O WDAC permite que as organizações controlem quais drivers e aplicativos podem ser executados em seus clientes Windows (a partir do Windows 11)

As políticas WDAC se aplicam ao computador gerenciado como um todo e afetam todos os usuários do dispositivo. As regras do WDAC podem ser definidas com base em:

- Atributos dos certificados de codificação usados para assinar um aplicativo e seus binários
- Atributos dos binários do aplicativo provenientes dos metadados assinados para os arquivos, como Nome de Arquivo Original e versão, ou o hash do arquivo
- A reputação do aplicativo conforme determinado pelo Grafo de Segurança Inteligente da Microsoft
- A identidade do processo que iniciou a instalação do aplicativo e seus binários (instalador gerenciado)
- O caminho do qual o aplicativo ou arquivo é iniciado (começando com Windows 10 versão 1903)
- O processo que iniciou o aplicativo ou binário

Windows

Controle de Aplicativos – WDAC

As configurações do WDAC são implementadas pelo Powershell

Definindo política:

```
## Update the path to your WDAC policy XML
$WDACPolicyXMLFile = $env:USERPROFILE + "\Desktop\MyWDACPolicy.xml"
[xml]$WDACPolicy = Get-Content -Path $WDACPolicyXMLFile
if (($WDACPolicy.SiPolicy.PolicyID) -ne $null) ## Multiple policy format (For Windows builds 1903+ only, including Server 2022)
{
    $PolicyID = $WDACPolicy.SiPolicy.PolicyID
    $PolicyBinary = $PolicyID+".cip"
}
else ## Single policy format (Windows Server 2016 and 2019, and Windows 10 1809 LTSC)
{
    $PolicyBinary = "SiPolicy.p7b"
}

## Binary file will be written to your desktop
ConvertFrom-CIPolicy -XmlFilePath $WDACPolicyXMLFile -BinaryFilePath $env:USERPROFILE\Desktop\$PolicyBinary
```

https://learn.microsoft.com/pt-br/windows/security/application-security/application-control/windows-defender-application-control/deployment/deploy-wdac-policies-with-script

Windows

Outras ferramentas de Segurança

Bitlocker: Ferramenta de criptografia de disco completo para proteger dados contra acessos não autorizados.
Caminho: Painel de Controle > Sistema e Segurança > Criptografia de Unidade de Disco BitLocke

Exploit Protection: Descrição: Configurações avançadas para proteger o sistema contra vulnerabilidades e exploits.
Caminho: Configurações > Atualização e Segurança > Segurança do Windows > Controle de Aplicativos e Navegadores > Configurações de Exploit Protection

Credenciais Protegidas (Windows Credential Manager): Gerenciamento de credenciais para facilitar o login em sites e aplicativos.
Caminho: Painel de Controle > Contas de Usuário > Gerenciador de Credenciais

Windows Sandbox: Ambiente isolado que permite executar aplicativos em um ambiente seguro sem afetar o sistema principal.
Caminho: Ativar através de "Ativar ou desativar recursos do Windows" > Selecionar "Windows Sandbox"
Nota: Disponível apenas nas edições Pro e Enterprise.

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Security-Enhanced Linux (SELinux) é uma arquitetura de segurança para sistemas Linux® que permite que administradores tenham mais controle sobre quem pode acessar o sistema. Ele foi originalmente desenvolvido pela Agência de Segurança Nacional (NSA) dos Estados Unidos como uma série de patches para o kernel do Linux usando módulos de segurança do Linux (LSM).


```
sudo apt-get install selinux-utils selinux-basics
```

Prevenção: O SELinux define controles de acesso para as aplicações, processos e arquivos de um sistema. Ele usa políticas de segurança, um conjunto de regras que dizem ao SELinux o que pode ou não ser acessado, para impor o acesso permitido por uma determinada política.

Se o SELinux não conseguir tomar uma decisão sobre o acesso baseado nas permissões armazenadas em cache, ele enviará uma solicitação para o servidor de segurança. Esse servidor verifica o contexto de segurança da entidade e o arquivo. O contexto é aplicado do banco de dados de políticas do SELinux. Em seguida, a permissão é concedida ou negada.

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Funcionalidades do SELinux.

- Restringe o acesso de usuários e processos a arquivos e recursos do sistema.
- Baseado em **políticas de segurança** predefinidas.

Controle de Acesso Mandatório (MAC)

Diferente do controle de acesso onde os proprietários dos recursos definem as permissões, o MAC permite que as políticas de segurança sejam definidas de maneira centralizada e obrigatória.

O SELinux já implementa o Controle de Acesso Mandatório (MAC) por padrão. Para garantir que ele esteja ativo:

sestatus

Editar o arquivo /etc/selinux/config

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Modos de Operação

- Enforcing: Políticas ativas e aplicadas, bloqueando acessos não permitidos.
- Permissive: Apenas registra eventos de violação (logs), sem bloquear acessos.
- Disabled: SELinux desativado.

Verificar status: sestatus
Alterar modo: setenforce
Configuração em /etc/selinux/config.

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Outras Funcionalidades do SELinux.

Políticas de Segurança Granulares: As políticas SELinux definem regras precisas sobre como processos e usuários podem interagir com arquivos, dispositivos e outros processos. Isso é feito através de contextos de segurança atribuídos a cada entidade no sistema.

Confinamento de Processos: O SELinux pode limitar o impacto de uma exploração comprometida ao confinar processos a conjuntos específicos de permissões.

Proteção de Sistema de Arquivos: Pode proteger arquivos críticos do sistema, garantindo que apenas processos autorizados possam acessá-los.

Logs e Auditoria: Registra todas as ações que são negadas pelo SELinux, permitindo que os administradores monitorem e auditem eventos de segurança.

Linux

SELinux (Security-Enhanced Linux)

Confinamento de Processos no SELinux

O SELinux funciona aplicando um **contexto de segurança** a todos os processos e objetos no sistema. Esse contexto define explicitamente o que cada processo pode ou não fazer, limitando o impacto de atividades maliciosas ou erros de configuração. Aqui estão os conceitos principais:

Contextos de Segurança:

Cada processo, arquivo, dispositivo e recurso no sistema é etiquetado com um contexto de segurança, que contém os seguintes componentes:

- Usuário (user): Representa o tipo de entidade executando o processo (ex.: system_u, unconfined_u).
- Papel (role): Define o que aquele processo pode fazer no sistema (ex.: object_r, system_r).
- Tipo (type): É o mais relevante. Especifica as permissões do processo ou recurso. Processos interagem apenas com tipos que possuem permissões explícitas.

Ex: -rw-r--r--. 1 root root system_u:object_r:httpd_sys_content_t:so index.html

- system_u: Usuário do sistema.object_r: Papel associado ao objeto.
- httpd_sys_content_t: Tipo específico que indica que o arquivo pertence ao serviço HTTPD (servidor web).

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Confinamento de Processos no SELinux

Permissões Baseadas em Tipos

O SELinux usa políticas de segurança para restringir o que cada tipo pode acessar.

Exemplo: O processo httpd_t (tipo associado ao Apache) pode: Ler arquivos com o tipo httpd_sys_content_t. não pode acessar arquivos com o tipo shadow_t (usado para armazenar senhas).Isso evita que um atacante use o Apache para comprometer partes críticas do sistema, como o arquivo /etc/shadow

Princípio do Menor Privilégio

Com o SELinux, processos só têm as permissões estritamente necessárias para executar suas funções.Exemplo Prático:Se um atacante explorar uma vulnerabilidade no Apache, o processo ainda estará restrito às permissões associadas ao contexto httpd_t.O atacante não poderá, por exemplo, acessar diretórios do sistema como /root ou /home.

Linux

Instituto Infnet

SELinux (Security-Enhanced Linux)

Comando chcon

O comando chcon é utilizado para alterar temporariamente o contexto de segurança de um arquivo ou diretório no SELinux (Security-Enhanced Linux). O contexto de segurança determina como processos e usuários podem interagir com aquele recurso, de acordo com as políticas definidas.

Sintaxe do Comando:

CONTEXTO: Define o novo contexto de segurança no formato:usuário:papel:tipo:nível
Obs: O mais importante na prática é o tipo, que define as permissões para processos específicos.

ARQUIVO/DIRETÓRIO: Caminho para o arquivo ou diretório cujo contexto será alterado.

Linux

Instituto Infnet

Aplicação prática

Configurar o SELinux para um Servidor Web

Cenário: O Apache HTTP Server está instalado e o site está armazenado em /var/www/html/index.html.

Verifique o contexto de segurança do arquivo:

```
ls -Z /var/www/html/index.html
```

Caso o contexto esteja incorreto (ex.: unconfined_u:object_r:default_t:so), ajuste para o tipo correto:

```
sudo chcon -t httpd_sys_content_t /var/www/html/index.html
```

Linux

Instituto Infnet

Iptables

iptables é uma ferramenta de filtragem de pacotes que permite a administração das tabelas fornecidas pelo firewall do kernel do Linux.

```
sudo apt-get install iptables   # para distribuições baseadas no Debian
sudo yum install iptables       # para distribuições baseadas no Red Hat
```

Prevenção: Ajuda a prevenir ataques de rede, como ataques de negação de serviço (DoS), spoofing de IP, e acesso não autorizado.

Caso de Uso: Configurar iptables para bloquear todo o tráfego de entrada na porta 22 (SSH) de endereços IP suspeitos após várias tentativas de login falhadas:

```
sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set
sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60
```

Linux

Instituto Infnet

AppArmor

AppArmor é uma infraestrutura de controle de acesso baseado em política de segurança que permite que programas sejam limitados a um conjunto específico de recursos. Ele utiliza um sistema de Controle de Acesso Mandatório (MAC - Mandatory Access Control) construído sobre a interface LSM (Linux Security Modules) do Linux. Na prática, o kernel consulta o AppArmor antes de cada chamada do sistema para saber se o processo está autorizado a fazer a operação dada.

```
sudo apt-get install apparmor apparmor-profiles apparmor-utils
```

Prevenção: Ajuda a prevenir a execução de código não autorizado e limita os danos que podem ser causados por programas comprometidos.

Caso de Uso: Usar AppArmor para criar um perfil de segurança que restringe um processo de banco de dados MySQL para que ele só possa ler e escrever em diretórios específicos, prevenindo acesso não autorizado a outras partes do sistema.

Linux

Instituto Infnet

ClamAV

ClamAV é um software antivírus de código aberto para detectar trojans, vírus, malware e outras ameaças maliciosas.

```
sudo apt-get install clamav clamav-daemon  # para distribuições baseadas no Debian
sudo yum install clamav                    # para distribuições baseadas no Red Hat
```

Prevenção: Ajuda a detectar e remover malware, vírus, trojans e outras ameaças.

Caso de Uso: Agendar verificações diárias do sistema de arquivos com ClamAV para detectar e remover arquivos infectados:

```
clamscan -r /home
```

Linux

Instituto Infnet

Fail2ban

Fail2ban é uma ferramenta que escaneia arquivos de log e bane endereços IP que mostram sinais maliciosos, como muitas falhas de autenticação.

```
sudo apt-get install fail2ban
```

Prevenção: Ajuda a prevenir ataques de força bruta, especialmente em serviços como SSH, reduzindo a chance de acesso não autorizado.

Caso de Uso: Configurar Fail2ban para monitorar tentativas de login SSH e banir IPs que falham na autenticação mais de 3 vezes em 10 minutos:

```
sudo nano /etc/fail2ban/jail.local
```

→

```
[sshd]
enabled = true
maxretry = 3
findtime = 600
bantime = 3600
```

Linux

Instituto Infnet

Auditd

Auditd é um daemon para o subsistema de auditoria do Linux. Ele registra uma variedade de eventos do sistema, permitindo o rastreamento detalhado de atividades no sistema.

```
sudo apt-get install auditd
```

Prevenção: Ajuda a detectar atividades suspeitas, fornecendo uma trilha de auditoria detalhada que pode ser usada para investigar possíveis incidentes de segurança.

Caso de Uso: Configurar auditd para monitorar alterações no diretório /etc::

```
sudo auditctl -w /etc -p wa -k etc_changes
```

Linux

Instituto Infnet

Chkrootkit

Chkrootkit é uma ferramenta que verifica a presença de rootkits no sistema.

```
sudo apt-get install chkrootkit
```

Prevenção: Ajuda a detectar e remover rootkits, prevenindo acesso não autorizado e comprometimento do sistema.

Caso de Uso: Executar chkrootkit para verificar a presença de rootkits no sistema:

```
sudo chkrootkit
```

Linux

Instituto Infnet

Snort

Snort é uma ferramenta de segurança de rede open-source (código aberto) usada como um IDS/IPS (Sistema de Detecção e Prevenção de Intrusos). Foi desenvolvida inicialmente por Martin Roesch e atualmente é mantida pela Cisco Systems.

Funcionalidades:

- Detecção de Intrusos (IDS):Monitora o tráfego de rede em tempo real.Identifica atividades suspeitas, como tentativas de exploração, varreduras de porta e ataques conhecidos.
- Prevenção de Intrusos (IPS):Pode ser configurado para bloquear pacotes maliciosos automaticamente antes de chegarem ao destino.
- Análise de Protocolos:Examina o comportamento dos protocolos de rede para identificar anomalias.
- Registro de Eventos:Gera logs detalhados sobre atividades e ataques detectados.
- Detecção Baseada em Assinaturas:Usa regras específicas para identificar ameaças conhecidas (como malware, explorações e worms).

Linux

Instituto Infnet

Snort

Exemplo de Aplicação

Instalação (em sistemas baseados em Debian):

```
sudo apt update
sudo apt install snort
```

Testar o Modo IDS: Configure o arquivo de regras /etc/snort/snort.conf para incluir assinaturas de ataques.

Rodar o Snort:

```
snort -c /etc/snort/snort.conf -A console
```

Linux

Instituto Infnet

Kali Linux – Ferramenta de Pen test Linux

https://www.kali.org/get-kali/#kali-virtual-machines

FIM