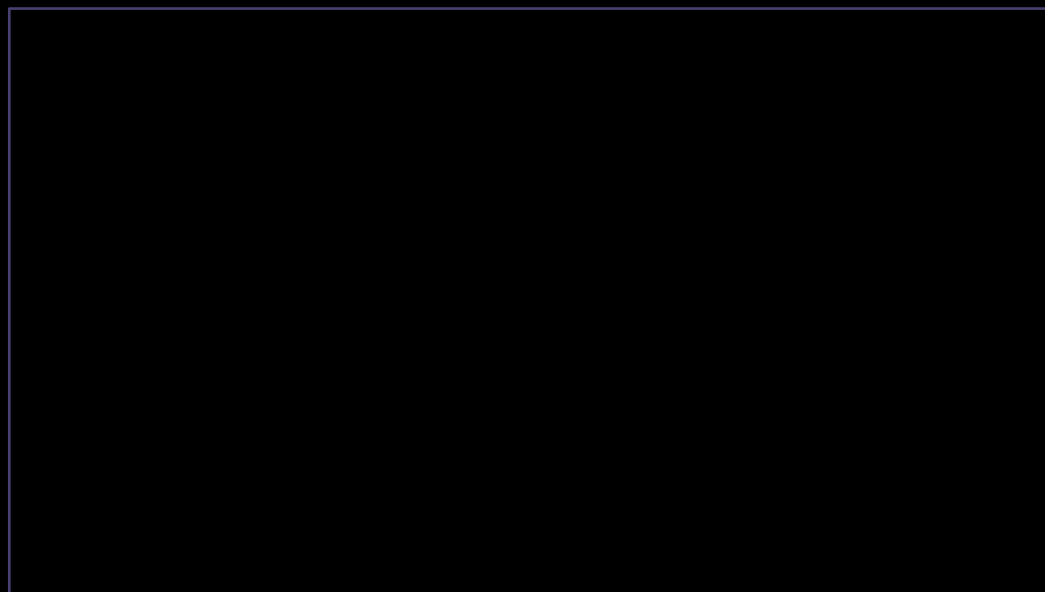




# Prime

**CCS-A**

Threat Hunting e Varreduras de  
Vulnerabilidade



# Threat Hunting

- ▶ Prática de procurar ameaças cibernéticas ainda não detectadas.

- ▶ Utiliza TTPs:



Ferramentas;



Técnicas;



Procedimentos.

- ▶ Os invasores podem usar recursos para se manterem presentes:



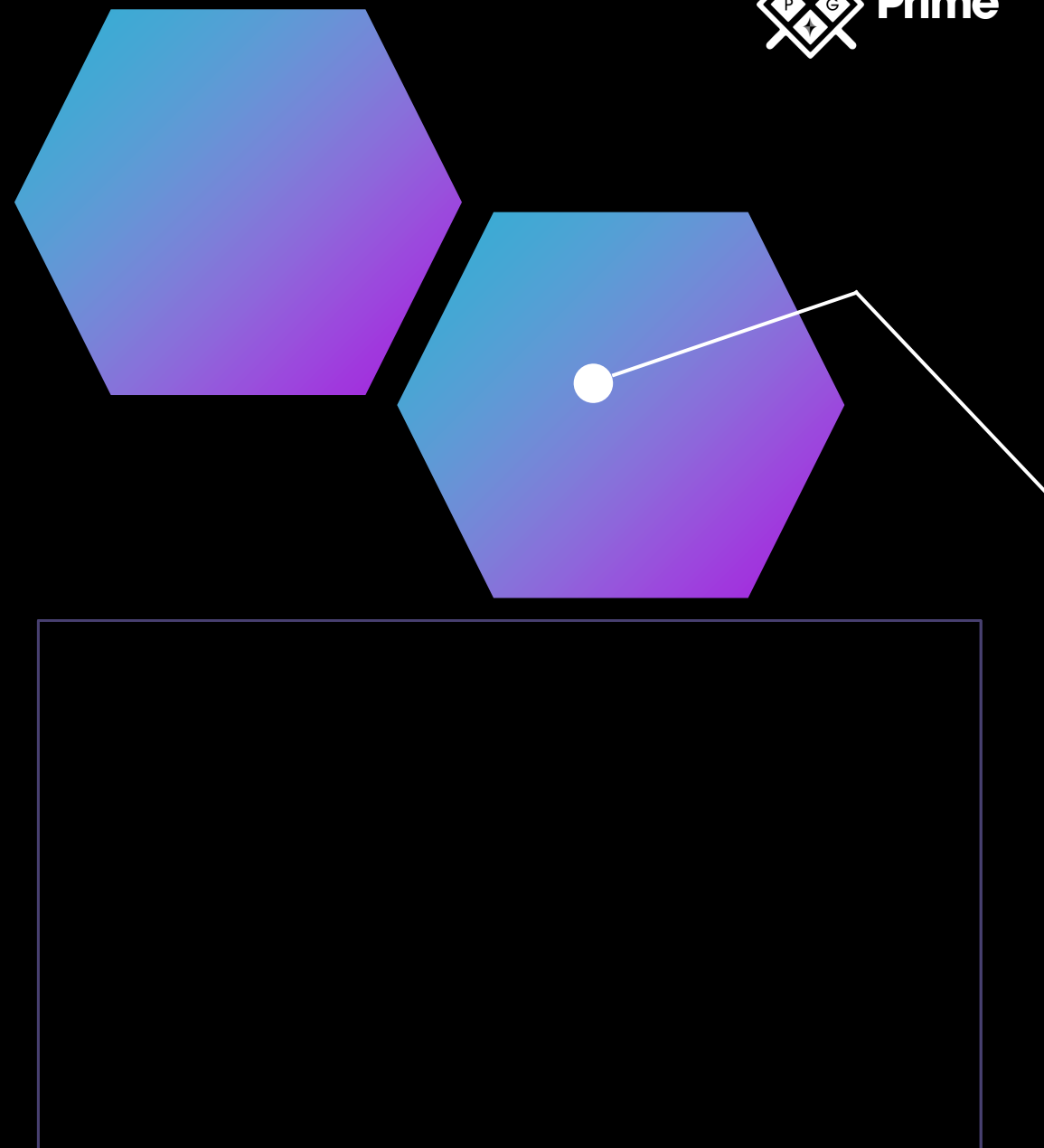
Living off the land.

- ▶ Algumas ferramentas:

- ▶ Fontes de dados de inteligência;
- ▶ Feeds de ameaças;
- ▶ Indicadores de ataque (IOAs);
- ▶ Indicadores de comprometimento (IOCs).

# Fusão de Inteligência

- ▶ Combinação de dados coletados da “inteligência” para obter uma imagem completa da situação atual
- ▶ Conhecimento por trás de:
  -  Recursos;
  -  Infraestrutura;
  -  Motivos;
  -  Objetivos;
  -  Recursos de uma ameaça.
- ▶ Permite:
  - ▶ Identificação;
  - ▶ Contextualização.
- ▶ Envolve ameaças internas e externas.



# Feeds de Ameaças

- ▶ Publicação e distribuição de dados sobre ameaças.
- ▶ Contém listas de indicadores de uma ameaça.
- ▶ Pode conter informações como endereços IP ou remetentes de e-mail maliciosos.
- ▶ Podem vir de fontes:



Internas;



Externas (assinantes do feed).

- ▶ Fontes externas precisam de uma maior curadoria no formato:
  - ▶ Exemplo: Structured Threat Information eXpression (STIX).

# Avisos e Boletins

- ▶ Conjuntos de informações de parceiros, como:



Fornecedores de segurança;



Grupos do setor;



Governo;

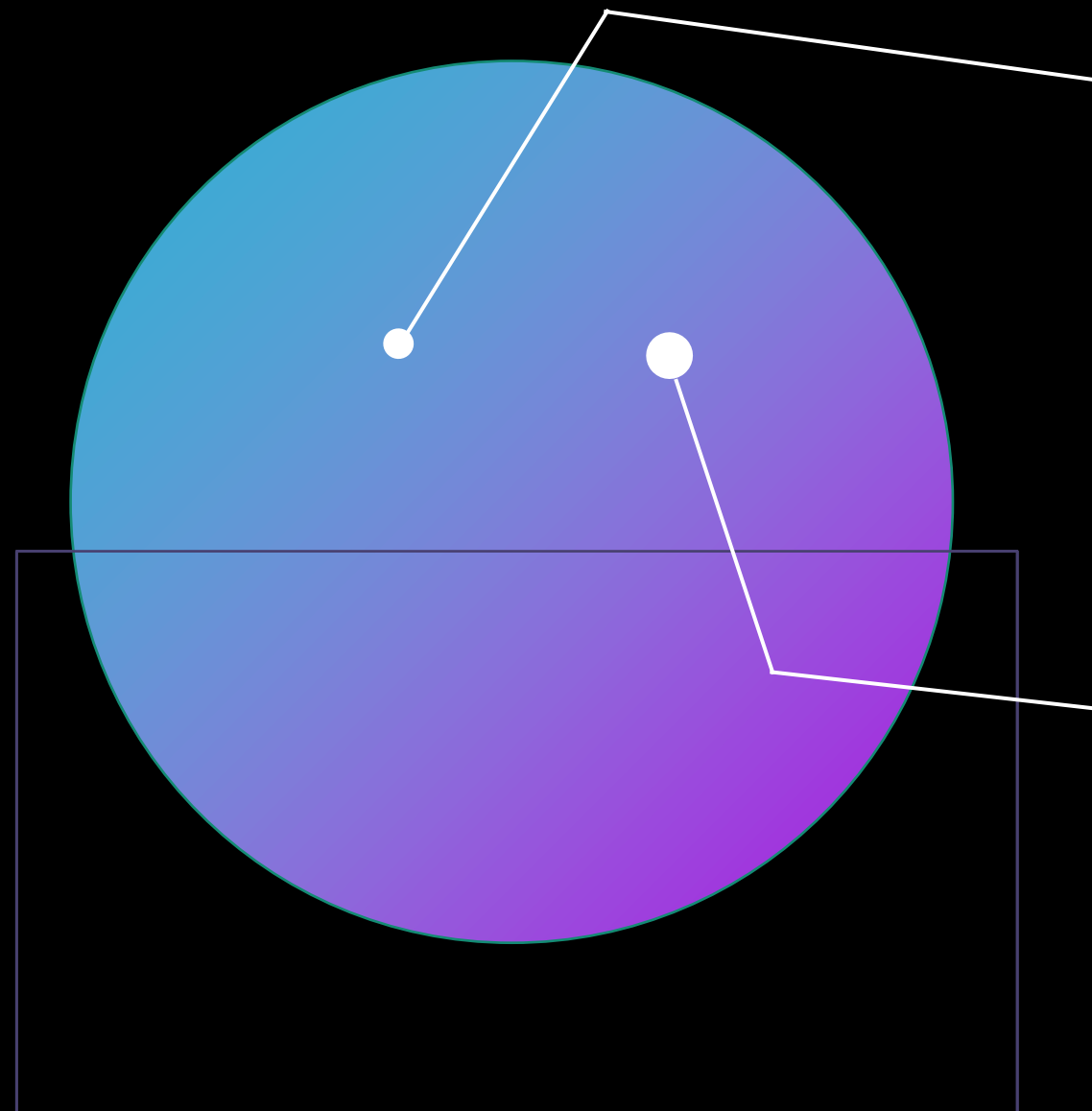


Grupos de compartilhamento de informações;

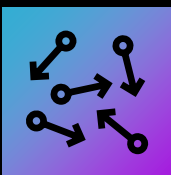


Fontes confiáveis.

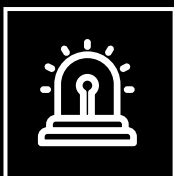
- ▶ São fontes externas de feeds de ameaças e precisam ser processadas para determinar aplicabilidade.



# Manobra



Capacidade de se mover-se estrategicamente para obter uma vantagem competitiva.



Maneiras de combater a manobra:

- ▶ Observação do tráfego;
- ▶ Análise da infraestrutura de rede da empresa.



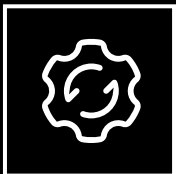
- ▶ Pode ser uma tática defensiva usada por profissionais de segurança.
- ▶ Colocar *honeypots* em áreas específicas da rede para detectar ameaças.

# Varreduras de Vulnerabilidade



Processo de examinar serviços em sistemas de computador para achar vulnerabilidades.

- ▶ Pode ser de forma automatizada.



Processo que determina a versão de um software e busca por vulnerabilidades conhecidas.



Repositório CVE: Vulnerabilidades e Exposições Comuns.

- ▶ Mais de 145.000 vulnerabilidades específicas.

# Falsos Positivos

- ▶ Quando um comportamento é identificado como malicioso de forma errada.
- ▶ Qualquer sistema que utiliza medição está sujeita a erros.
- ▶ Fatores externos também podem introduzir erros.
- ▶ Influência na medição na tomada de decisão.
- ▶ Avaliação de falsos positivos dependem dos:



Resultados dos testes;



E do resultado verdadeiro.

# Falsos Negativos

- ▶ Oposto dos falsos positivos.
- ▶ São vistos como piores do que os falsos positivos.
- ▶ Quando testamos algo que deu negativo, mas na realidade é positivo.



Exemplo: Sistema de detecção de intrusão (IDS) que não gera um alerta de um ataque de malware.

- ▶ Avaliações de falsos negativos dependem de:



Resultados dos testes;



E do resultado verdadeiro.

# Revisões de Logs

- ▶ Escanear vulnerabilidades em logs de eventos em busca de algo suspeitos.
- ▶ A chave é uma configuração adequada, sem dados estranhos.
- ▶ Sistema de log fornece informações úteis para quem ataca.

- ▶ Informações sobre:



Sistemas;



Nomes de contas;



O que contribuiu (ou não) com o acesso.



Um bom log dará a visão do que aconteceu em um sistema.

# Credenciadas Vs. Não-Credenciadas

- ▶ Verificações de vulnerabilidade podem ser executadas com e sem credenciais.



Verificação sem credenciais = Fornece informações sobre o estado de um serviço;



Verificação com credenciais (profunda) = Complexas, pois exigem etapas extras.

- ▶ Varreduras credenciadas revelam informações adicionais em relação às não-credenciadas.

# Intrusivas Vs. Não-Intrusivas

- ▶ Você está realmente tentando invadir o sistema ou explorá-lo?
- ▶ É um *pentest*? (teste de intrusão que tenta explorar o sistema).



## Verificação intrusiva

Verificação que pode ocasionar travamentos e danos;



## Verificação não-intrusiva

Verificação simples de portas e serviços abertos.

# Varredura em Aplicativos

- ▶ Varreduras de vulnerabilidade em aplicativos para procurar falhas no design do aplicativo.
  - ▶ Alvos comuns dos invasores.
- ▶ Varreduras de vulnerabilidade:
  - ▶ Avaliam a força de um aplicativo implantado em relação ao desempenho.
- ▶ Vulnerabilidades de aplicativo representam alguns dos problemas mais arriscados na empresa.

# Varredura em Aplicativos Web



Aplicativos acessíveis pela Web (site).



Método de acessibilidade com maior exposição a atividades não autorizadas.

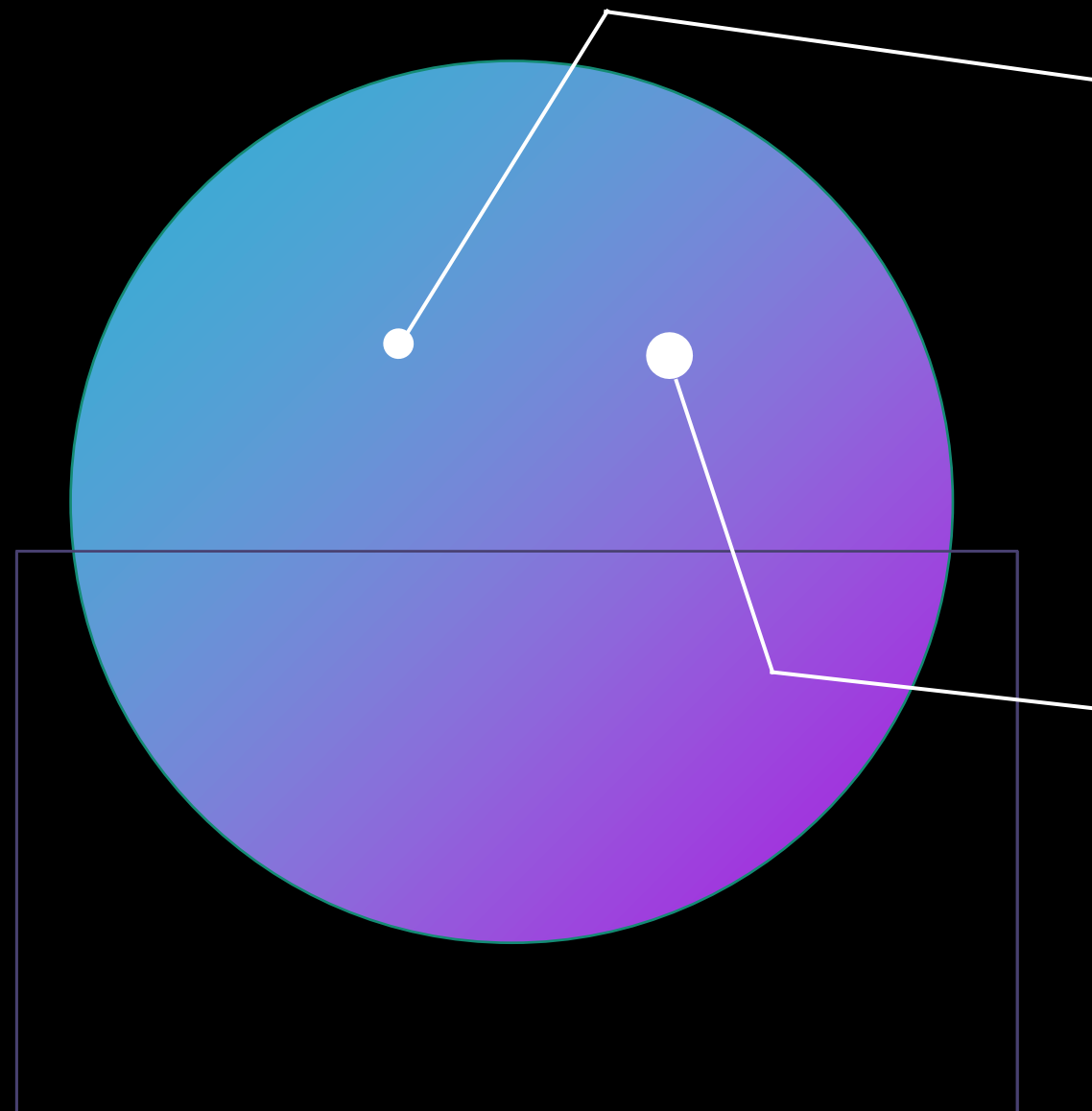


Varredura de vulnerabilidade com Nikto:

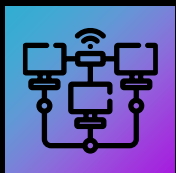
- ▶ Scanners específicos para aplicativos da Web.



Aplicativos da Web criados internamente sofrem mais riscos.



# Varredura na Rede



Dispositivos de rede, como switches, roteadores e impressoras.



Pode haver vulnerabilidades no transporte de dados entre sistemas e usuários.

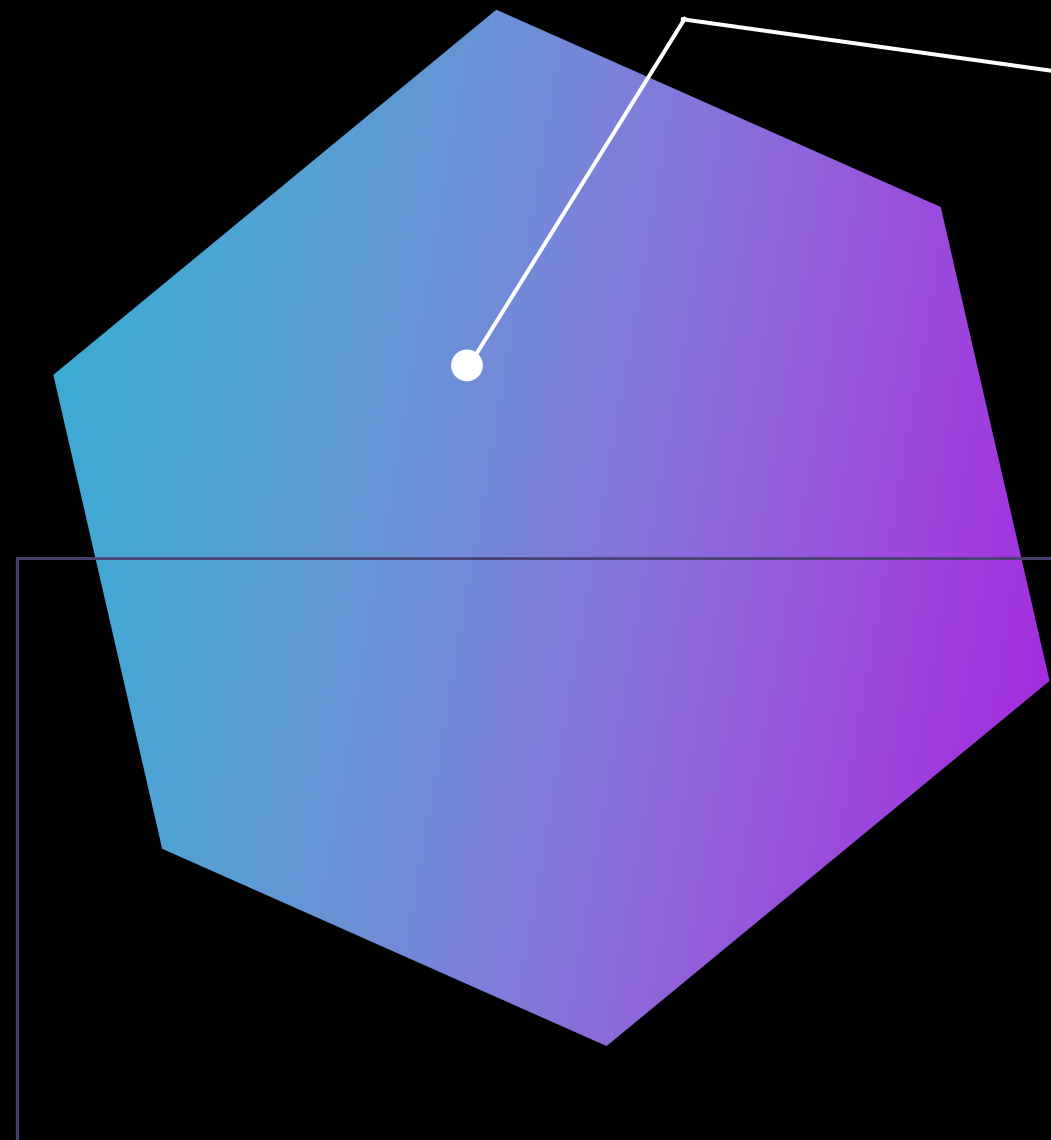


Usada para verificar vulnerabilidades na movimentação, uso de credenciais e operações potencialmente críticas.



Varreduras de vulnerabilidade:

- ▶ Executadas em toda a rede. Todos os sistemas são varridos, mapeados e enumerados.



# Varredura na Configuração

- ▶ informar quaisquer configurações vulneráveis que devam ser alteradas.
  - ▶ Configurações incorretas deixam um sistema mais vulnerável.
  - ▶ Verificar as configurações (periodicamente) é essencial.
- ▶ Protocolos e padrões para validar as configurações (NVD):
  - ▶ Common Configuration Enumeration (CCE): <https://ncp.nist.gov/cce/index>
  - ▶ Common Platform Enumeration (CPE): <https://nvd.nist.gov/products/cpe>

# Vulnerabilidades e Exposições Comuns (CVE)/ Sistema de Pontuação de Vulnerabilidade Comum (CVSS)

## ▶ Common Vulnerabilities and Exposures (CVE)

- ▶ Lista de vulnerabilidades conhecidas em um software.

## ▶ Cada vulnerabilidade tem:



Identificação;



Descrição;



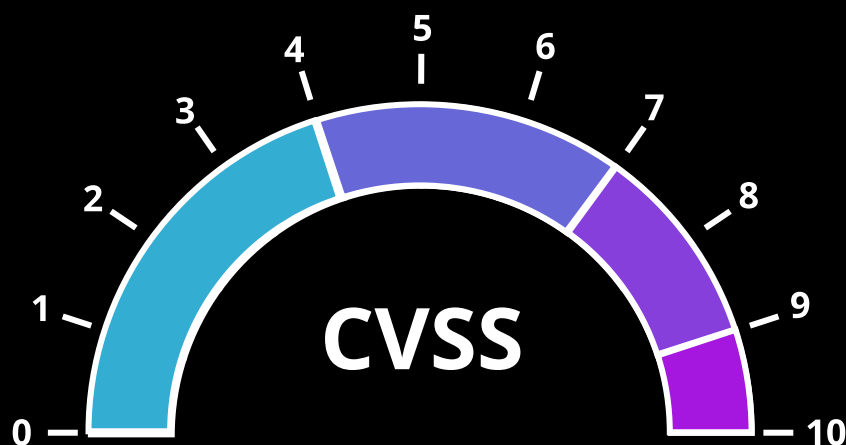
Referência.

## ▶ Gerenciada pelo MITRE: <https://cve.mitre.org/cve>

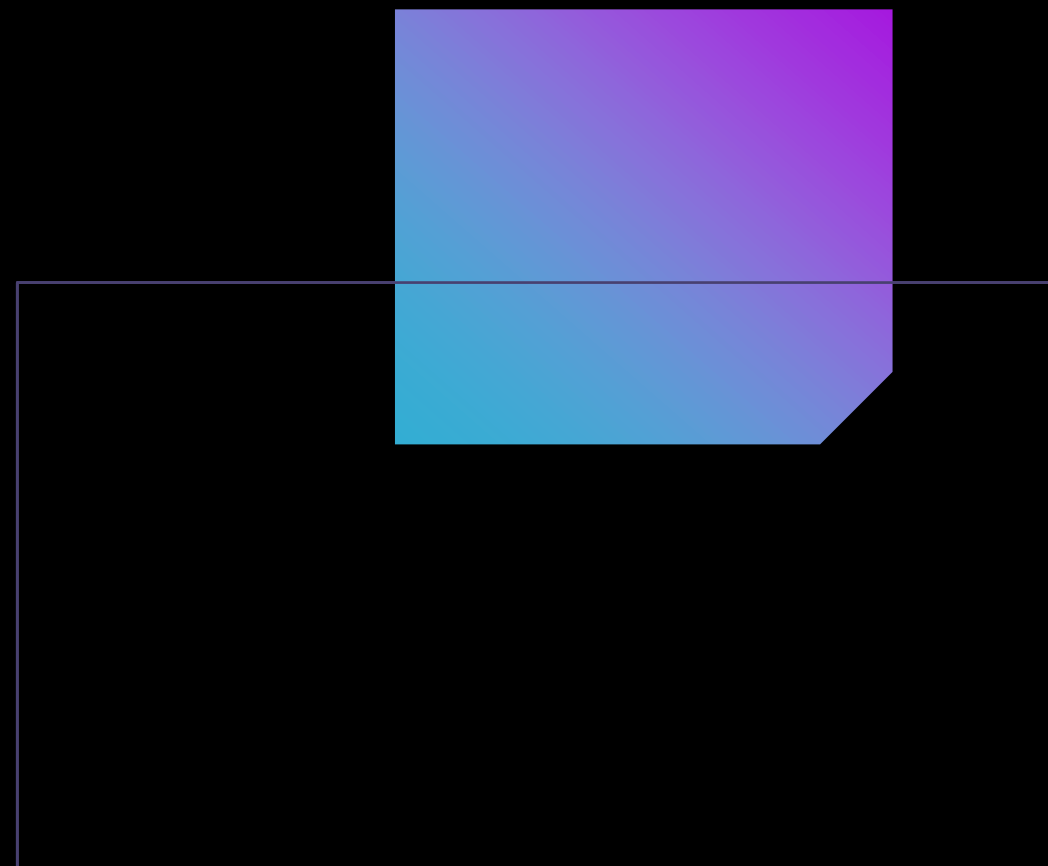
# Vulnerabilidades e Exposições Comuns (CVE)/ Sistema de Pontuação de Vulnerabilidade Comum (CVSS)

## ► Common Vulnerability Scoring System (CVSS)

► Sistema de pontuação.



- Baixa - 0.1 - 3.9
- Média - 4.0 - 6.9
- Alta - 7.0 - 8.9
- Crítica - 9.0 - 10





Prime

# OBRIGADO!

AVALIAÇÕES DE SEGURANÇA -  
THREAT HUNTING E VARREDURAS  
DE VULNERABILIDADE