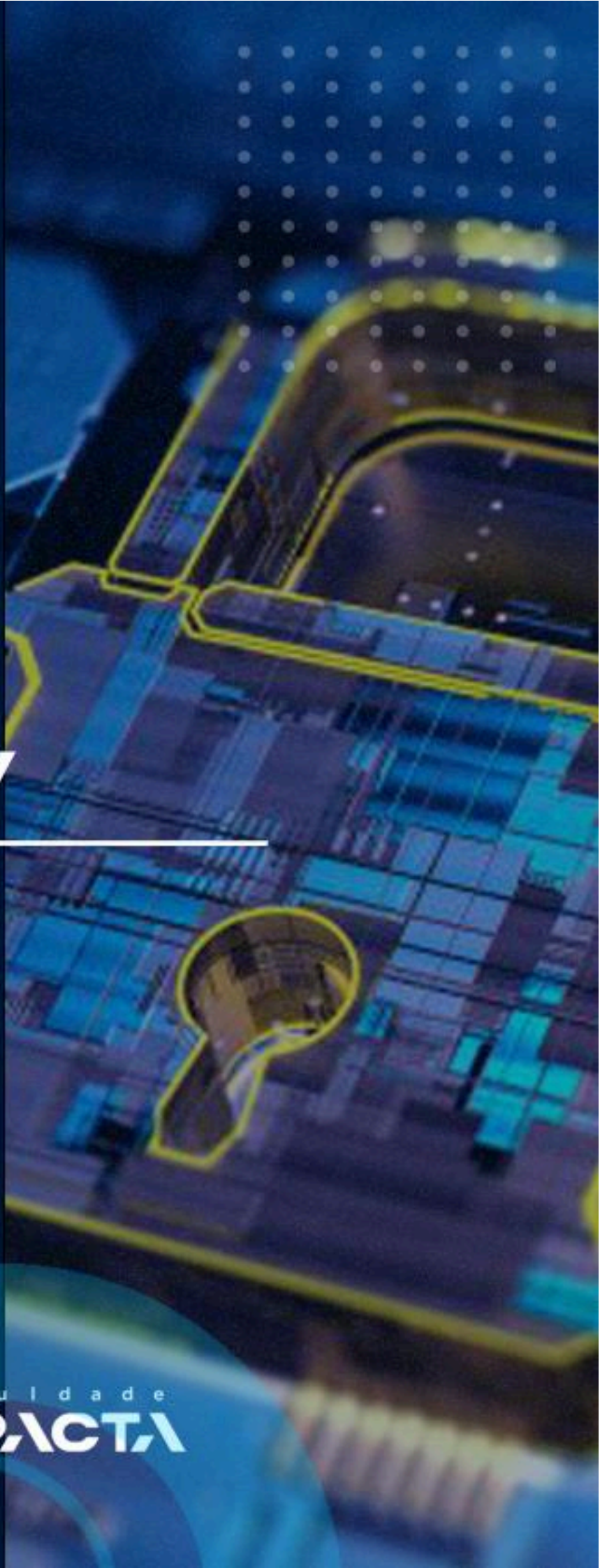
NEaD
Núcleo de Educação a Distância

CYBER SECURITY



Faculdade IMPACTA

10

Proteção de Endpoint

Alex Sandro da Silva Feitosa

Resumo

Nessa aula, abordaremos o processo pelo qual um site de análise de malware gera um relatório detalhado sobre arquivos suspeitos. Será apresentado um panorama geral das etapas envolvidas, desde o envio do arquivo até a geração do relatório final. O objetivo é entender como essas plataformas identificam comportamentos maliciosos e organizam as informações de forma clara para análise. Essa visão introdutória ajudará a compreender a utilidade desses relatórios em contextos de segurança da informação.

1.1. Proteção antimalware

1.1.1 Ameaças de endpoints

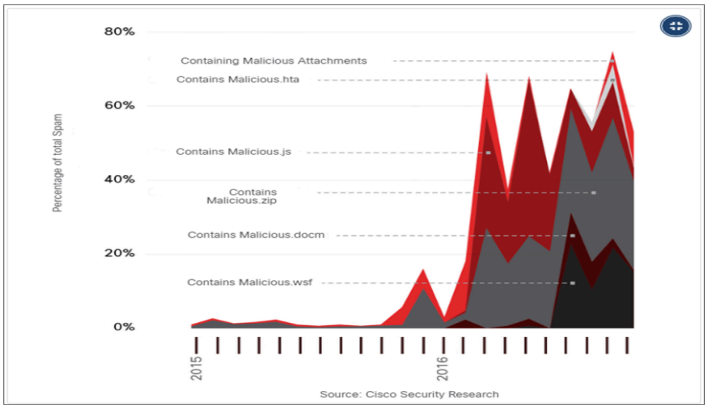
Os pontos de extremidade podem ser definidos como hosts na rede que podem acessar ou ser acessados por outros hosts na rede.

Cada ponto de extremidade é potencialmente uma forma de software malicioso obter acesso a uma rede.

Dispositivos que acessam redes remotamente através de VPNs também são pontos finais que podem injetar malware na rede VPN a partir da rede pública.

Vários tipos comuns de malware foram encontrados para alterar significativamente os recursos em menos de 24 horas, a fim de evitar a detecção.

Figura 1.1 Porcentagem de SPAM



Fonte:CCNA Cyber OPS Associate v1, 2020.

Como muitos ataques se originam de dentro da rede, proteger uma LAN interna é quase tão importante quanto proteger o perímetro externo da rede.

Depois que um host interno é infiltrado, ele pode se tornar um ponto de partida para um invasor obter acesso a dispositivos críticos do sistema, como servidores e informações confidenciais.

Há dois elementos LAN internos para proteger:

- Endpoints - Os hosts são suscetíveis a ataques relacionados a malware.
- Infraestrutura de rede - Pontos de extremidade de interconexão de dispositivos de infraestrutura LAN

Proteção de Endpoint contra malware baseada em host:

- Software antimalware/antivírus baseado em host e firewalls baseados em host são usados para proteger dispositivos móveis usando VPN.

Software antivírus / antimalware:

- É um software instalado em um host para detectar e mitigar vírus e malware. Por exemplo, proteção contra vírus e ameaças do Windows Defender, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro e outros.

Programas antimalware podem detectar vírus usando três abordagens diferentes:

- Baseado em assinatura:reconhece várias características de arquivos de malware conhecidos
- Baseado em heurística: reconhece recursos gerais compartilhados por vários tipos de malware
- Baseado em comportamento: emprega análise de comportamento suspeito
- A proteção antivírus baseada em host, também conhecida como baseada em agentes, é executada em todas as máquinas protegidas.

Firewall de host:

- Este software está instalado em um host.

- Restringe conexões de entrada e saída a conexões iniciadas somente por esse host.

Alguns softwares de firewall podem impedir que um host se infecte e impedir que hosts infectados espalhem malware para outros hosts. Esta função está incluída em alguns sistemas operacionais.

Por exemplo, o Windows inclui o Firewall do Windows Defender com Segurança Avançada.

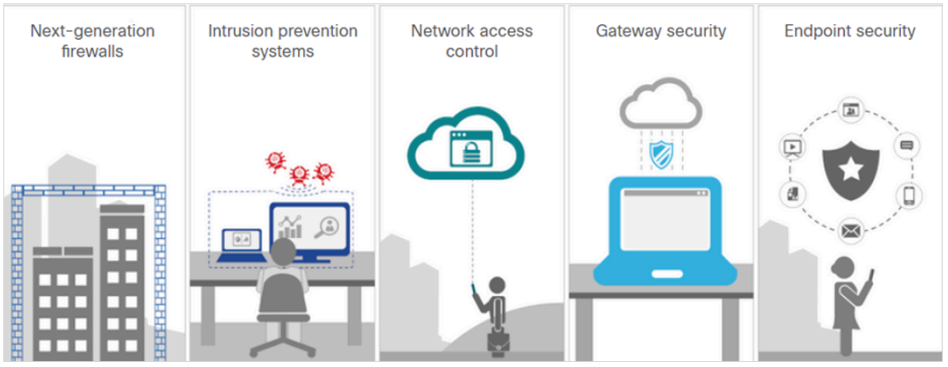
Suites de segurança baseadas em host:

- Recomenda-se instalar um conjunto de produtos de segurança baseado em host em redes domésticas e empresariais para fornecer uma defesa em camadas que proteja contra as ameaças mais comuns.
- Estes incluem antivírus, anti-phishing, navegação segura, sistema de prevenção de intrusões baseado em host e recursos de firewall.
- Os produtos de segurança baseados em host também fornecem função de telemetria.
- A maioria dos softwares de segurança baseados em host inclui uma funcionalidade robusta de registro que é essencial para operações de segurança cibernética.
- O laboratório de testes independente AV-TEST fornece análises de alta qualidade de proteções baseadas em host, bem como informações sobre muitos outros produtos de segurança.

Proteção de ponto de extremidade contra malware baseada em rede:

- Os dispositivos de prevenção de malware baseados em rede são capazes de compartilhar informações entre si para tomar decisões melhor informadas.
- A proteção de endpoints em uma rede sem fronteiras pode ser realizada usando técnicas baseadas em rede, bem como baseadas em host.

Figura 1.2 Proteção avançada contra malwares

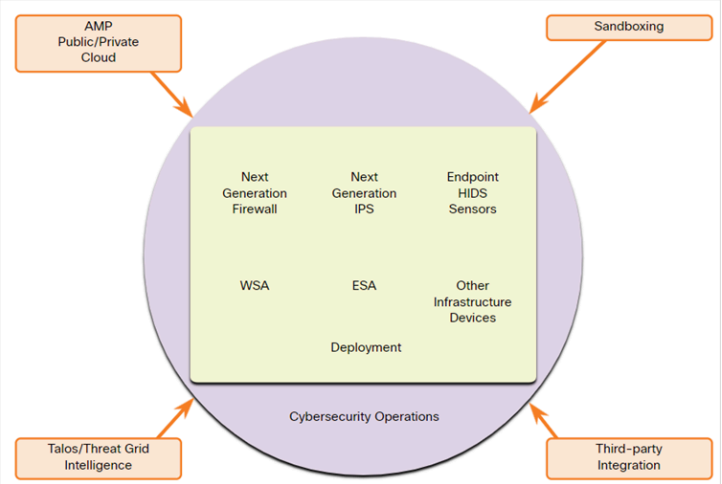


Fonte: CCNA Cyber OPS Associate v1, 2020.

Alguns exemplos de dispositivos e técnicas que implementam proteções de host no nível da rede:

- Proteção avançada contra malware (AMP) - Fornece proteção de terminais contra vírus e malware.
- Email Security Appliance (ESA) - Fornece filtragem de SPAM e e-mails potencialmente maliciosos antes que eles cheguem ao endpoint.
- Web Security Appliance (WSA) - Fornece filtragem de sites e lista negra
- Controle de Admissão de Rede (NAC) - Permite que somente sistemas autorizados e compatíveis se conectem à rede.

Figura 1.3 Proteções



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.1.2 Proteção contra intrusão baseada em host

Superfície de ataque de segurança

Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que é acessível a um invasor.

Ele pode consistir em portas abertas em servidores ou hosts, software executado em servidores voltados para a Internet, protocolos de rede sem fio e usuários.

Componentes da superfície de ataque:

- Superfície de ataque de rede: explora vulnerabilidades em redes.
- Superfície de ataque de software: fornecido por meio da exploração de vulnerabilidades em aplicativos de software baseados na Web, na nuvem ou em host.
- Superfície de ataque humano: explora fraquezas no comportamento do usuário.

Limitar o acesso a ameaças potenciais criando listas de aplicativos proibidos é conhecido como lista negra.

As listas negras de aplicativos podem ditar quais aplicativos de usuário não têm permissão para serem executados em um computador.

As listas brancas especificam quais programas podem ser executados.

Dessa forma, aplicativos vulneráveis conhecidos podem ser impedidos de criar vulnerabilidades em hosts de rede.

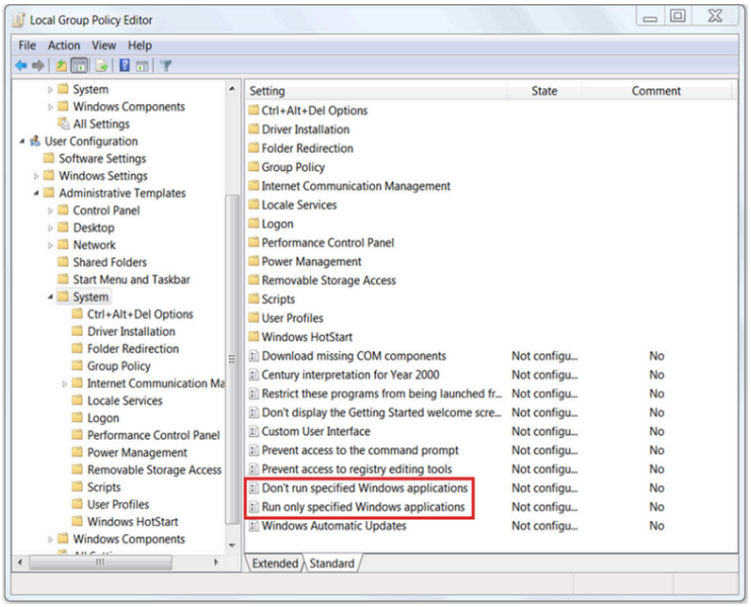
Os sites também podem ser incluídos na lista branca e na lista negra.

Essas listas negras podem ser criadas manualmente ou podem ser obtidas de vários serviços de segurança.

As listas negras podem ser continuamente atualizadas pelos serviços de segurança e distribuídas para firewalls e outros sistemas de segurança que as utilizam.

O sistema de gerenciamento de segurança Firepower da Cisco é um exemplo de um sistema que pode acessar o serviço de inteligência de segurança Cisco Talos para obter listas negras.

Figura 1.4 Local Group Policy



Fonte: CCNA Cyber OPS Associate v1, 2020.

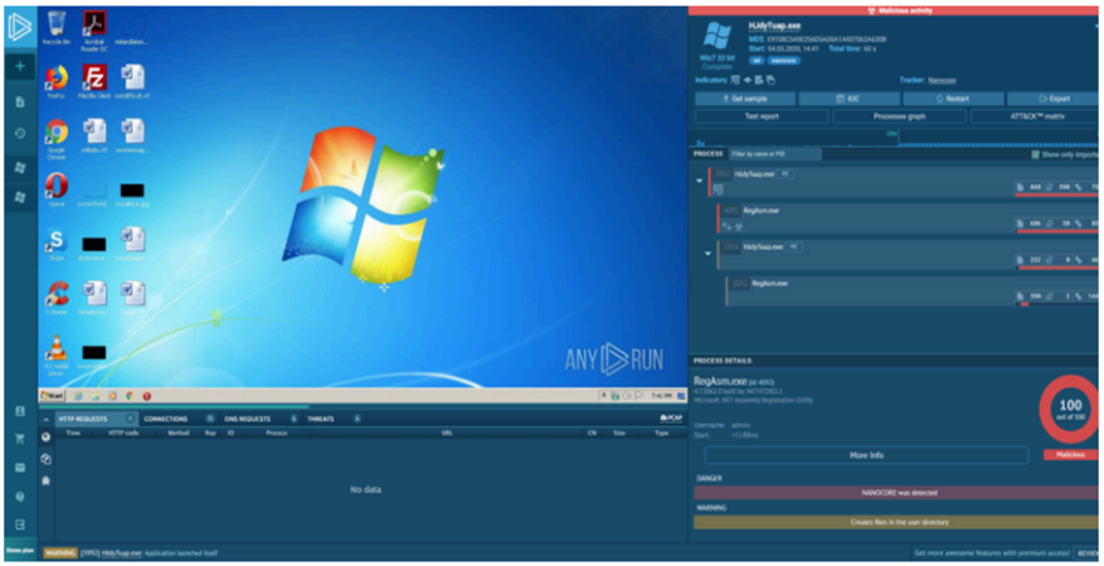
Sandboxing Baseado em sistema de segurança de aplicativos:

- Sandboxing é uma técnica que permite que arquivos suspeitos sejam executados e analisados em um ambiente seguro.

Cuckoo Sandbox é um sandbox popular sistema de análise de malware livre. Ele pode ser executado localmente e ter amostras de malware enviadas a ele para análise.

ANY.RUN é uma ferramenta online que oferece a capacidade de carregar uma amostra de malware para análise como qualquer sandbox online.

Figura 1.5 SandBox



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.2. Common Vulnerability Scoring System (CVSS)

1.2.1 Sistema de pontuação de vulnerabilidade comum (CVSS)

O Common Vulnerability Scoring System (CVSS) é uma ferramenta de avaliação de risco projetada para transmitir os atributos comuns e a gravidade das vulnerabilidades em sistemas de hardware e software de computador.

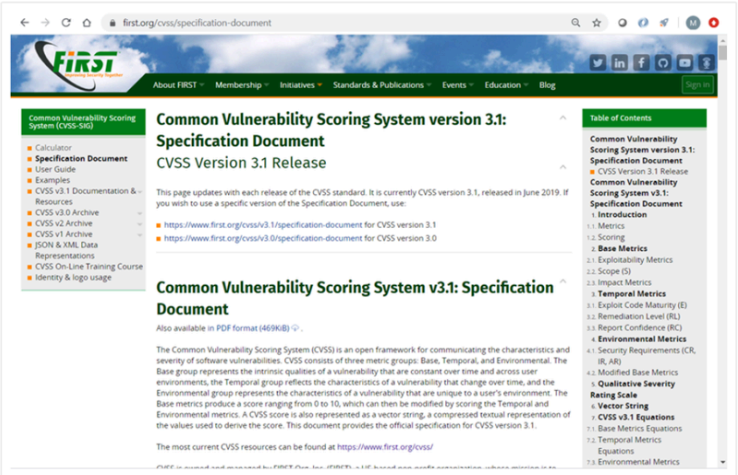
O CVSS fornece pontuações padronizadas de vulnerabilidade.

Ele fornece uma estrutura aberta com métricas para todos os usuários.

O CVSS ajuda a priorizar o risco.

O Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) foi designado como guardião do CVSS para promover sua adoção globalmente.

Figura 1.6 CVSS



Fonte: CCNA Cyber OPS Associate v1, 2020.

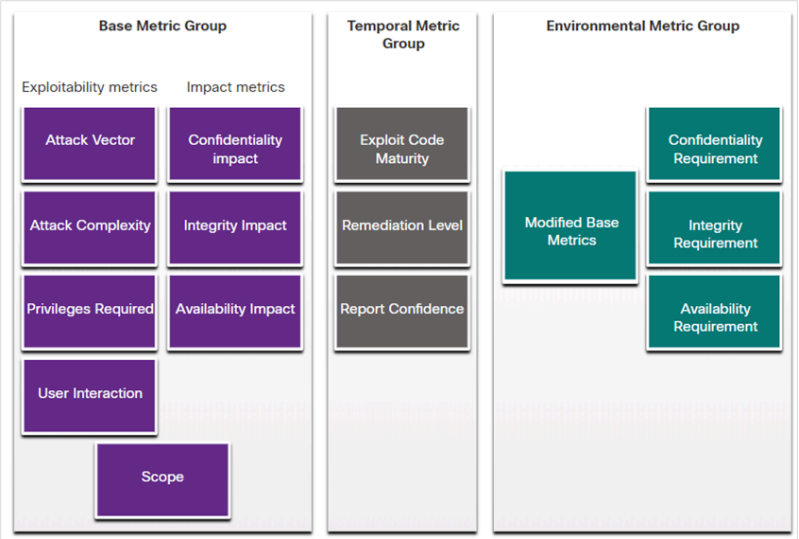
O CVSS utiliza três grupos de métricas para avaliar a vulnerabilidade.

Grupo de Métricas Base: Representa as características de uma vulnerabilidade que são constantes ao longo do tempo e em contextos.

Grupo de métricas temporais: mede as características de uma vulnerabilidade que pode mudar ao longo do tempo, mas não em ambientes de usuário.

Grupo de métricas ambientais: mede os aspectos de uma vulnerabilidade que estão enraizados no ambiente de uma organização específica.

Figura 1.7 Grupo de Métricas Base



Fonte: CCNA Cyber OPS Associate v1, 2020.

Grupo Métrico Base CVSS:

As métricas de Exploração do Grupo de Métricas Base incluem os seguintes critérios:

- Vetor de ataque
- A complexidade do ataque
- Privilégios necessários
- Interação do usuário
- Examinar

Os componentes de métricas de Impacto do Grupo Métrico Base incluem os seguintes critérios:

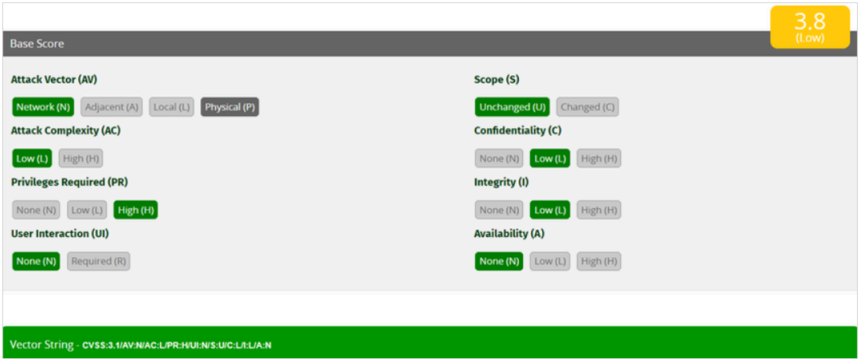
- Impacto de Confidencialidade
- Impacto da integridade
- Impacto da disponibilidade

O processo CVSS usa uma ferramenta chamada Calculadora CVSS v3.1.

A calculadora é como um questionário no qual são feitas as escolhas que descrevem a vulnerabilidade para cada grupo de métricas.

Posteriormente, uma pontuação é gerada e a classificação de gravidade numérica é exibida.

Figura 1.8 Calculadora



Fonte: CCNA Cyber OPS Associate v1, 2020.

Após a conclusão do grupo Métrica Base, os valores de métrica Temporal e Ambiental modificam os resultados da Métrica Base para fornecer uma pontuação geral.

Quanto maior a classificação de gravidade, maior o impacto potencial de uma exploração e maior a urgência em abordar a vulnerabilidade.

Qualquer vulnerabilidade que exceda 3.9 deve ser resolvida.

Tabela 1.1. Intervalos de escores e significado qualitativo correspondente.

Classificação	**Pontuação CVSS**
Nenhum	0
Baixa	0.1 – 3.9
Médio	4.0 – 6.9
Alto	7.0 – 8.9
Críticos	9.0 – 10.0

Fonte: do autor, 2022.

1.2.2 Outras fontes de informações sobre vulnerabilidades

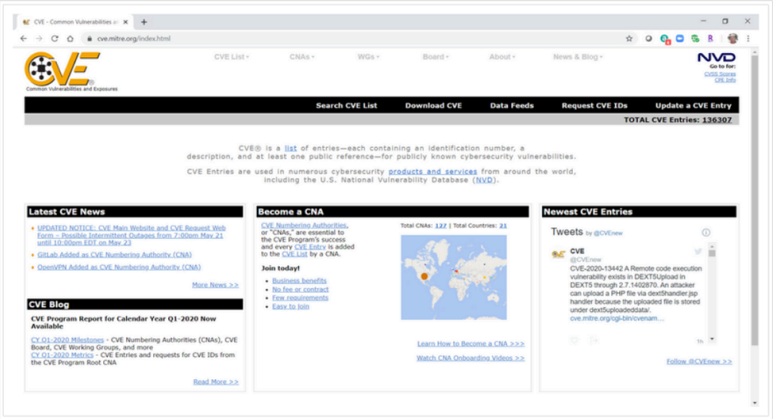
Common Vulnerabilities and Exposures (CVE):

O identificador CVE fornece uma maneira padrão de pesquisar uma referência a vulnerabilidades.

Os serviços de inteligência contra ameaças usam identificadores CVE e aparecem em vários logs do sistema de segurança.

O site CVE Details fornece uma ligação entre as pontuações do CVSS e as informações do CVE.

Figura 1.9 CVE Details



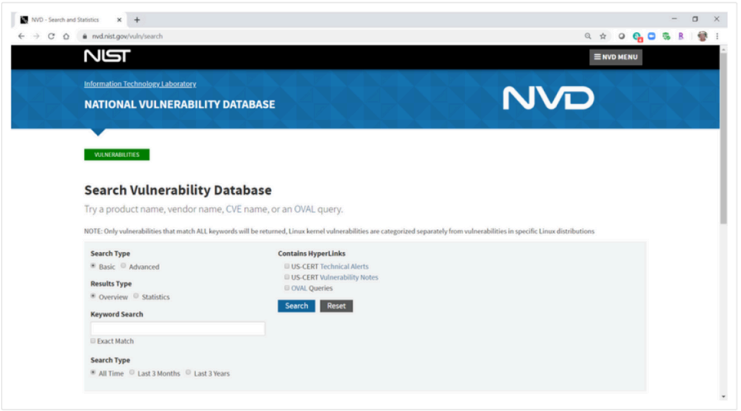
Fonte: CCNA Cyber OPS Associate v1, 2020.

National Vulnerability Database (NVD):

Isso utiliza identificadores CVE e fornece informações adicionais sobre vulnerabilidades, como pontuações de ameaças CVSS, detalhes técnicos, entidades afetadas e recursos para investigação adicional.

O banco de dados foi criado e é mantido pela agência do National Institute of Standards and Technology (NIST) do governo dos EUA.

Figura 1.10 Calculadora NIST



Fonte: CCNA Cyber OPS Associate v1, 2020.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes:** primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security:** applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002**:Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes:** projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.