



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -
SECURITY IMPLEMENTATION

Progresso do curso

Módulo 1. Introdução ao Hacking Ético

Módulo 2. Footprinting e Reconhecimento

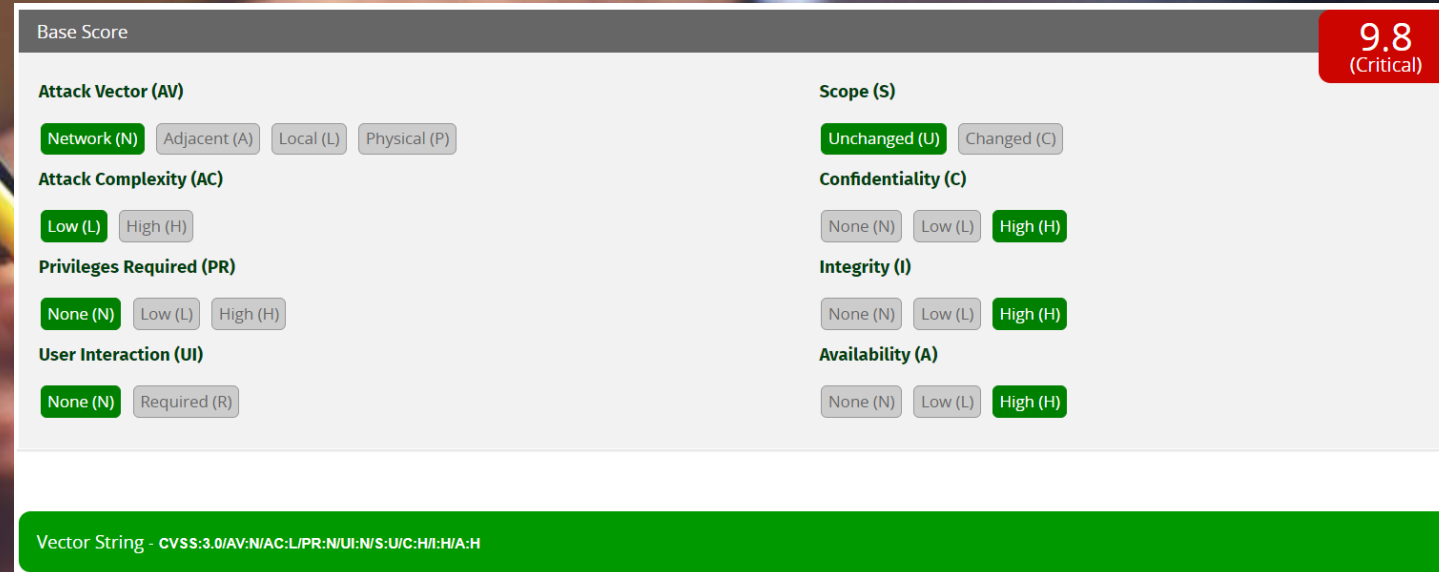
Módulo 3. Scanning de Redes

Módulo 4. Enumeração

Módulo 5. Análise de Vulnerabilidade

Conceitos de Análise de Vulnerabilidades:

No mundo de hoje, as organizações dependem muito da tecnologia da informação para proteger informações vitais. Estas informações estão associadas às áreas de finanças, pesquisa e desenvolvimento, pessoal, direito e segurança. As avaliações de vulnerabilidade examinam as redes e sistemas em busca de pontos fracos de segurança conhecidos. Os invasores realizam análises de vulnerabilidade para identificar brechas de segurança na rede da organização de destino, infraestrutura de banco de dados, aplicações e sistemas operacionais. As vulnerabilidades identificadas são usadas por invasores para explorar ainda mais esta rede alvo.



Base Score

9.8 (Critical)

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Vector String - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CEHv12 (ANSI)

05.Vulnerability Analysis

Objetivos deste Módulo

- Visão geral da pesquisa de vulnerabilidade, avaliação de vulnerabilidade e sistemas de pontuação de vulnerabilidade
- Visão geral do ciclo de vida do gerenciamento de vulnerabilidade (fases de avaliação de vulnerabilidade)
- Compreendendo vários tipos de vulnerabilidades e técnicas de avaliação de vulnerabilidades
- Compreendendo diferentes abordagens de soluções de avaliação de vulnerabilidade
- Compreendendo os diferentes tipos de ferramentas de avaliação de vulnerabilidade e critérios para escolhê-los
- Ferramentas de avaliação de vulnerabilidade
- Gerando e analisando relatórios de avaliação de vulnerabilidade

Objetivos deste Módulo

A avaliação da vulnerabilidade desempenha um papel importante no fornecimento de segurança aos recursos e infraestrutura de qualquer organização contra várias ameaças internas e externas. Para proteger uma rede, um administrador precisa realizar o gerenciamento de patches, instalar um software antivírus adequado, verificar as configurações, resolver problemas conhecidos em aplicativos de terceiros e solucionar problemas de hardware com configurações padrão. Todas essas atividades juntas constituem uma avaliação de vulnerabilidade.

Objetivos deste Módulo

Este módulo começa com uma introdução aos conceitos de avaliação de vulnerabilidade. Ele também discute os vários sistemas de pontuação de vulnerabilidade, bancos de dados de vulnerabilidade, ciclo de vida no gerenciamento de vulnerabilidade e várias abordagens e ferramentas utilizadas para realizar avaliações de vulnerabilidade. Este módulo fornecerá conhecimento sobre as ferramentas e técnicas utilizadas por invasores para realizar uma análise de vulnerabilidade de qualidade. Ele conclui com uma análise dos relatórios de avaliação de vulnerabilidade que ajudam um hacker ético a consertar as vulnerabilidades identificadas.

Conceitos de avaliação de vulnerabilidade

Geralmente, há duas causas principais para sistemas vulneráveis em uma rede: configuração incorreta de software ou hardware e práticas de programação inadequadas. Os invasores exploram essas vulnerabilidades para realizar vários tipos de ataques aos recursos organizacionais. Esta seção fornece uma visão geral da avaliação de vulnerabilidade, sistemas de pontuação de vulnerabilidade, bancos de dados de vulnerabilidade e o ciclo de vida da avaliação de vulnerabilidade.

Pesquisa de Vulnerabilidade

- Pesquisa de vulnerabilidade é o processo de análise de protocolos, serviços e configurações para descobrir as vulnerabilidades e falhas de design que irão expor um sistema operacional e seus aplicativos à exploração, ataque ou uso indevido.

```
root@kali:~# nmap --script vuln -p139,445 192.168.0.18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-25 20:58 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.18
Host is up (0.0017s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_
Nmap done: 1 IP address (1 host up) scanned in 39.49 seconds
root@kali:~#
```


Um administrador precisa de Análise de Vulnerabilidades

- Para coletar informações sobre tendências de segurança, ameaças recém-descobertas, superfícies de ataque, vetores e técnicas de ataque;
- Para encontrar pontos fracos no sistema operacional e nos aplicativos e alertar o administrador da rede antes de um ataque à rede;
- Para entender as informações que ajudam a prevenir problemas de segurança;
- Para saber como se recuperar de um ataque à rede.

Um administrador precisa de Análise de Vulnerabilidades

Um hacker ético precisa acompanhar as vulnerabilidades descobertas mais recentemente e exploits para ficar um passo à frente dos invasores por meio da pesquisa de vulnerabilidade, que inclui:

- Descobrir as falhas e fraquezas do projeto do sistema que podem permitir que os invasores comprometam um sistema
- Manter-se atualizado sobre novos produtos e tecnologias e ler notícias relacionadas a exploits atuais
- Verificar sites de hackers clandestinos (sites Deep e Dark) para as vulnerabilidades e explorações recém descobertas.
- Verificar alertas recém-lançados sobre inovações relevantes e melhorias de produto para sistemas de segurança.

Um administrador precisa de Análise de Vulnerabilidades

Especialistas em segurança e pesquisadores de vulnerabilidades classificam as vulnerabilidades por:

- Nível de gravidade (baixo, médio ou alto)
- Faixa de exploração (local ou remota)

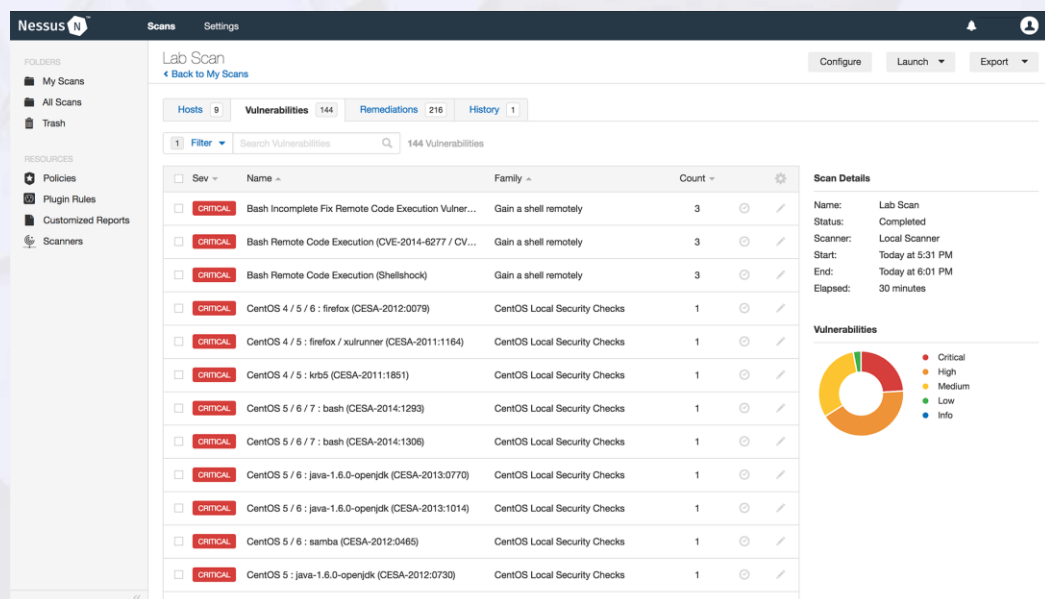
Os hackers éticos precisam conduzir pesquisas intensas com a ajuda das informações adquiridas nas fases de fingerprint e varredura para encontrar vulnerabilidades.

A seguir estão alguns dos sites online usados para realizar pesquisas de vulnerabilidade:

- Microsoft Vulnerability Research (MSVR) (<https://www.microsoft.com>)
- Dark Reading (<https://www.darkreading.com>)
- Security Tracker (<https://securitytracker.com>)
- Trend Micro (<https://www.trendmicro.com>)
- Security Magazine (<https://www.securitymagazine.com>)
- PenTest Magazine (<https://pentestmag.com>)
- SC Magazine (<https://www.scmagazine.com>)
- Exploit Database (<https://www.exploit-db.com>)
- SecurityFocus (<https://www.securityfocus.com>)
- Computerworld (<https://www.computerworld.com>)
- WindowsSecurity (<http://www.windowsecurity.com>)
- D'Crypt (<https://www.d-crypt.com>)

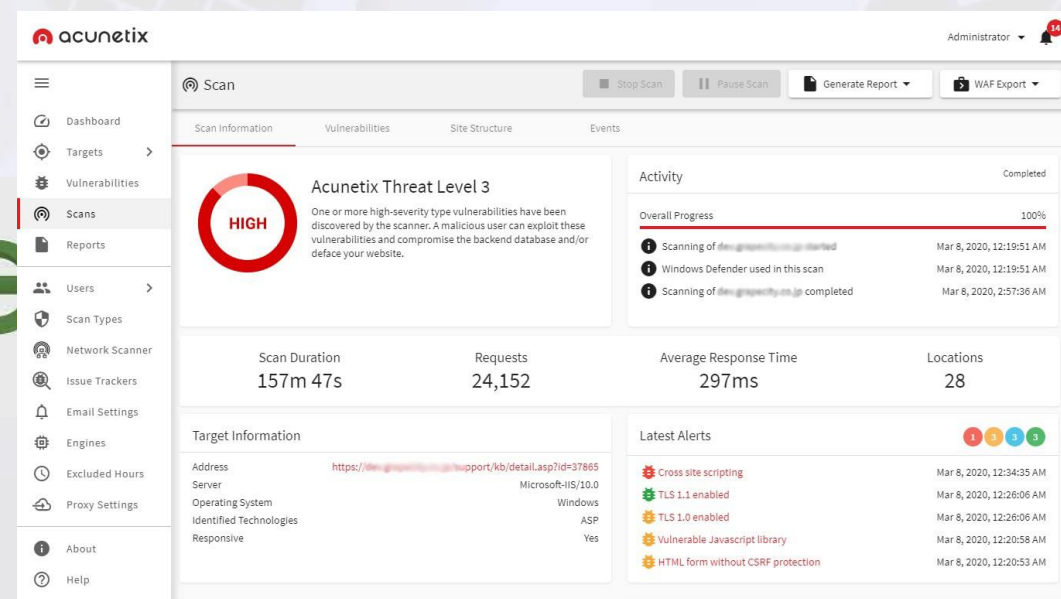
O que é avaliação de vulnerabilidade?

A avaliação de vulnerabilidade é um exame aprofundado da capacidade de um sistema ou aplicativo, incluindo os procedimentos e controles de segurança atuais, de resistir à exploração. Ele reconhece, mede e classifica as vulnerabilidades de segurança em um sistema de computador, rede e canais de comunicação.



The screenshot shows the Nessus web interface. On the left is a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Customized Reports', and 'Scanners'. The main area displays a table of vulnerabilities for a 'Lab Scan'. The table has columns for severity, name, family, and count. Several critical vulnerabilities are listed, including 'Bash Incomplete Fix Remote Code Execution Vulnerability' and 'CentOS 4 / 5 / 6 : firefox (CESA-2012-0079)'. A 'Scan Details' panel on the right shows the scan name, status (Completed), scanner (Local Scanner), start/end times, and elapsed time (30 minutes). Below this is a 'Vulnerabilities' donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012-0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1



The screenshot shows the Acunetix web interface. The top navigation bar includes 'Dashboard', 'Targets', 'Vulnerabilities', 'Scans', 'Reports', 'Users', 'Scan Types', 'Network Scanner', 'Issue Trackers', 'Email Settings', 'Engines', 'Excluded Hours', 'Proxy Settings', 'About', and 'Help'. The main area displays the 'Scan' results for a specific scan. A large red circle indicates a 'HIGH' threat level. The 'Scan Information' tab is active, showing 'Scan Duration: 157m 47s', 'Requests: 24,152', 'Average Response Time: 297ms', and 'Locations: 28'. The 'Vulnerabilities' tab shows a list of vulnerabilities, including 'Cross site scripting', 'TLS 1.1 enabled', 'TLS 1.0 enabled', 'Vulnerable Javascript library', and 'HTML form without CSRF protection'. The 'Activity' tab shows a list of events, including 'Scanning of https://www.grapacity.co.jp started', 'Windows Defender used in this scan', and 'Scanning of https://www.grapacity.co.jp completed'.

Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012-0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1

Identificação de vulnerabilidades

Os scanners de vulnerabilidades são capazes de identificar as seguintes informações:

- A versão do sistema operacional em execução em computadores ou dispositivos
- Portas de IP e protocolo de controle de transmissão / protocolo de datagrama de usuário (TCP / UDP) que estão ouvindo
- Aplicativos instalados
- Contas com senhas fracas
- Arquivos e pastas com permissões fracas
- Serviços e aplicativos padrão que podem ter que ser desinstalados
- Erros na configuração de segurança de aplicativos comuns
- Computadores expostos a vulnerabilidades conhecidas ou relatadas publicamente
- Informações de software
- Patches e hotfixes ausentes
- Configurações de rede fracas e portas mal configuradas ou vulneráveis
- Ajuda para verificar o inventário de todos os dispositivos na rede

Avaliação Ativa/Passiva

Existem duas abordagens para a verificação de vulnerabilidade de rede:

1 - **Verificação ativa:** o invasor interage diretamente com a rede de destino para encontrar vulnerabilidades. A varredura ativa ajuda a simular um ataque na rede alvo para descobrir vulnerabilidades que podem ser exploradas pelo invasor.

Exemplo: um invasor envia sondagens e solicitações especialmente criadas ao host de destino na rede para identificar vulnerabilidades.

2 - **Verificação passiva:** o invasor tenta encontrar vulnerabilidades sem interagir diretamente com a rede de destino. O invasor identifica vulnerabilidades por meio de informações expostas pelos sistemas durante as comunicações normais. Essa abordagem fornece informações sobre os pontos fracos, mas não fornece um caminho para o combate direto aos ataques.

Exemplo: um invasor adivinha as informações do sistema operacional, aplicativos e versões de aplicativos e serviços observando a configuração e a desativação da conexão TCP.

Limitações da avaliação de vulnerabilidade

O julgamento humano é necessário para analisar os dados após a digitalização e identificação de falsos positivos e falsos negativos.

A metodologia utilizada pode ter impactos nos resultados do teste. Por exemplo, a varredura de vulnerabilidades do software executado no contexto de segurança e do administrador de domínio produzirá resultados diferentes do software executado no contexto de segurança de um usuário autenticado ou não autenticado. Da mesma forma, diversos pacotes de software de varredura de vulnerabilidade avaliam a segurança de maneira diferente e têm recursos exclusivos. Isso pode influenciar os resultados da avaliação.

Sistemas de pontuação de vulnerabilidade e bancos de dados

Devido à crescente gravidade dos ataques cibernéticos, a pesquisa de vulnerabilidades se tornou prioridade, pois ajuda a reduzir a chance de ataques.

A pesquisa de vulnerabilidade fornece conhecimento de técnicas avançadas para identificar falhas ou brechas no software que podem ser exploradas por invasores.

Os sistemas de pontuação de vulnerabilidade e bancos de dados de vulnerabilidade são utilizados por analistas de segurança para classificar as vulnerabilidades do sistema de informações e fornecer uma pontuação composta da gravidade geral e do risco associado às vulnerabilidades identificadas.

Os bancos de dados de vulnerabilidade coletam e mantêm informações sobre várias vulnerabilidades presentes nos sistemas de informação.

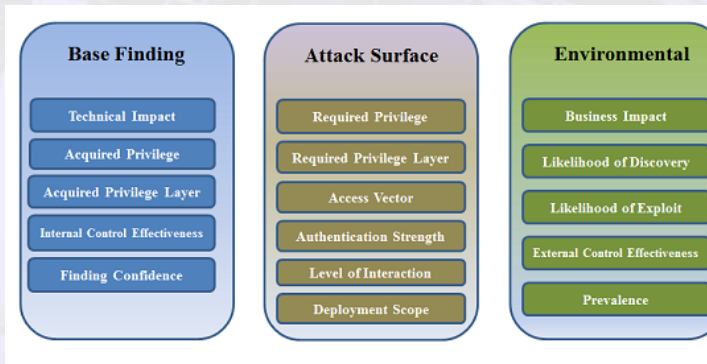
Sistemas de pontuação de vulnerabilidade e bancos de dados

<https://www.first.org/cvss/calculator/3.0>

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

https://cve.mitre.org/cve/search_cve_list.html

https://cwe.mitre.org/cwss/cwss_v1.0.1.html



Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

- CVSS provides an open framework for **communicating the characteristics and impacts** of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the **underlying vulnerability characteristics** used to **generate the scores**

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Common Vulnerability Scoring System Calculator version 1.0 - CVE-2017-0144

Through the calculator, the user can enter the CVSS scores for each of the three metrics (Base, Temporal, and Environmental) and the calculator will generate the overall CVSS score. The calculator also provides a detailed breakdown of the scores and the underlying characteristics used to generate the scores.

Base Score Metrics

Base Score: 7.5 (High)

Attack Vector (AV): Network (N) | Attack Complexity (AC): Low (L) | Authentication (Auth): None (N) | Confidentiality Impact (C): High (H) | Integrity Impact (I): High (H) | Availability Impact (A): High (H)

Base Score: 7.5 (High)

Source: <https://www.first.org>

Vulnerability Scoring Systems and Databases

National Vulnerability Database (NVD)

- A **U.S. government repository** of standards-based vulnerability management data represented using the **Security Content Automation Protocol (SCAP)**
- These data **enable the automation of vulnerability management**, security measurement, and compliance
- The NVD includes **databases of security checklist references**, security-related software flaws, misconfigurations, product names, and impact metrics

NVD

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

CVE-2019-6452 Detail

Current Description
Kycera Command Center (KCC) 1000000000 and 10000000000 allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE
Kycera Command Center (KCC) 1000000000 and 10000000000

Impact

CVSS v3.0 Severity Metrics
Base Score: 7.5 (High)
Attack Vector (AV): Network (N) | Attack Complexity (AC): Low (L) | Authentication (Auth): None (N) | Confidentiality Impact (C): High (H) | Integrity Impact (I): High (H) | Availability Impact (A): High (H)

CVSS v2.0 Severity Metrics
Base Score: 7.5 (High)
Attack Vector (AV): Network (N) | Attack Complexity (AC): Low (L) | Authentication (Auth): None (N) | Confidentiality Impact (C): High (H) | Integrity Impact (I): High (H) | Availability Impact (A): High (H)

QUICK INFO

CVE Dictionary Entry
CVE: CVE-2019-6452
NVD Published Date: 2019-09-10
NVD Last Modified: 2019-09-10

<https://nvd.nist.gov>

Vulnerability Scoring Systems and Databases

Common Weakness Enumeration (CWE)

- A **category system for software vulnerabilities and weaknesses**
- It is sponsored by the **National Cybersecurity FFRDC**, which is owned by **The MITRE Corporation**, with support from **US-CERT** and the **National Cyber Security Division of the U.S. Department of Homeland Security**
- It has over **600 categories** of weaknesses, which enable CWE to be effectively employed by the community as a **baseline for weakness identification, mitigation, and prevention efforts**

CWE Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

View the List of Weaknesses

Search CWE

Clearly find a specific software weakness by performing a search of the CWE List by keyword(s) or by CWE ID Number. To search by multiple keywords, separate each by a space.

Search results: About 10 results (0.17 seconds)

CWE-427: Uncontrolled Search Path Element (C3.2)
This weakness occurs when a program uses a search path element (such as a file name or directory name) that is not controlled by the program. This can allow an attacker to specify a path that is not intended by the program, leading to a security breach.

CWE-428: Improper Handling of Length Parameters (C3.2)
This weakness occurs when a program does not properly validate the length of a parameter (such as a file name or directory name) before using it. This can allow an attacker to specify a path that is not intended by the program, leading to a security breach.

CWE-429: Improper Handling of File Paths (C3.2)
This weakness occurs when a program does not properly validate the format of a file path before using it. This can allow an attacker to specify a path that is not intended by the program, leading to a security breach.

<https://cwe.mitre.org>

Vulnerability Scoring Systems and Databases

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures

CVE List
CNAs About
WGs News & Blog
Board
NVD
CVE Scores
CVE IDs
Advanced Search

Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

HOME > CVE > SEARCH RESULTS

TOTAL CVE Entries: 118125

Search Results

There are 414 CVE entries that match your search.

Name	Description
CVE-2019-9565	Druid Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kycera Command Center (KCC) 1000000000 and 10000000000 allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

<https://cve.mitre.org>

Ciclo de vida de gerenciamento de vulnerabilidade

O ciclo de vida do gerenciamento de vulnerabilidade é um processo importante que ajuda a identificar e corrigir os pontos fracos de segurança antes que possam ser explorados. Isso inclui definir a postura e as políticas de risco para uma organização, criando uma lista completa de ativos de sistemas, varrendo e avaliando o ambiente em busca de vulnerabilidades e exposições e tomando medidas para mitigar as vulnerabilidades que são identificadas.

As organizações devem manter um programa de gerenciamento de vulnerabilidade adequado para garantir a segurança geral das informações.

Fases envolvidas na gestão de vulnerabilidade

1- Identificar ativos e criar um baseline

Esta fase identifica ativos críticos e os prioriza para definir o risco com base na criticidade e valor de cada sistema. Isso cria um bom baseline para o gerenciamento de vulnerabilidade.

Esta fase envolve também a coleta de informações sobre os sistemas identificados para entender as portas funcionais, software, drivers e configuração básica de cada sistema, a fim de desenvolver e manter o baseline do sistema.

2- Verificação de vulnerabilidades

Esta fase é crucial no gerenciamento de vulnerabilidades. Nesta etapa, o analista de segurança executa o scanner de vulnerabilidades na rede para identificar as vulnerabilidades conhecidas na infraestrutura da organização.

Scanners de vulnerabilidades também podem ser realizadas em modelos de conformidade aplicáveis para avaliar os pontos fracos da infraestrutura da organização em relação às respectivas diretrizes de conformidade.

Fases envolvidas na gestão de vulnerabilidade

3- Avaliação de risco

Nesta fase, todas as incertezas graves que estão associadas ao sistema são avaliadas e priorizadas, e a correção é planejada para eliminar permanentemente as falhas do sistema.

A avaliação de risco resume a vulnerabilidade e o nível de risco identificado para cada um dos ativos selecionados. Ele determina se o nível de risco de um determinado ativo é alto, médio ou baixo. A remediação é planejada com base no nível de risco determinado. Por exemplo, as vulnerabilidades classificadas como de alto risco são direcionadas primeiro para diminuir as chances de exploração que afetariam adversamente a organização.

4- Remediação

Remediação é o processo da aplicação de correções em sistemas vulneráveis, a fim de reduzir o impacto e a gravidade das vulnerabilidades.

Esta fase é iniciada após a implementação bem-sucedida das etapas de avaliação, criação do baseline e escaneamento.

Fases envolvidas na gestão de vulnerabilidade

5- Verificação

Nesta fase, a equipe de segurança realiza uma nova varredura dos sistemas para avaliar se a remediação está concluída e se as correções individuais foram aplicadas aos ativos afetados. Esta fase proporciona uma visibilidade clara da empresa e permite que a equipe de segurança verifique se todas as fases anteriores foram perfeitamente empregadas ou não. A verificação pode ser realizada por vários meios, como sistemas de ticket, scanners e relatórios.

Obs: Esta fase também é conhecida como reteste.

6- Monitorar

As organizações precisam realizar monitoramento regular para manter a segurança do sistema. Utilizar ferramentas como IDS/IPS e firewalls. O monitoramento contínuo identifica ameaças potenciais e quaisquer novas vulnerabilidades que tenham evoluído. De acordo com as práticas recomendadas de segurança, todas as fases do gerenciamento de vulnerabilidades devem ser executadas regularmente.

Fase de Pós-Avaliação

Também conhecida como fase de recomendação, é realizada com base na avaliação de risco. A caracterização do risco ajuda a priorizar a lista de recomendações. As tarefas realizadas na fase de pós-avaliação incluem:

- Criação de uma lista de prioridades para recomendações de avaliação com base na análise de impacto
- Desenvolver um plano de ação para implementar a remediação proposta
- Captura de lições aprendidas para melhorar o processo completo no futuro
- Realização de treinamento para funcionários

Avaliação de risco

Na fase de avaliação de risco, os riscos são identificados, caracterizados e classificados junto com as técnicas utilizadas para controlar ou reduzir seu impacto.

É uma etapa importante para identificar os pontos fracos de segurança na arquitetura de TI de uma organização.

As tarefas realizadas na fase de avaliação de risco incluem:

- Realizar a categorização de risco com base na classificação de risco (por exemplo, crítico, alto, médio e baixo)
- Avalie o nível de impacto
- Determine os níveis de ameaça e risco

Remediação

Remediação refere-se às etapas executadas para mitigar as vulnerabilidades identificadas.

Estes incluem etapas como avaliação de vulnerabilidades, localização de riscos e criação de respostas para vulnerabilidades.

É importante que o processo de remediação seja específico, mensurável, atingível, relevante e com prazo determinado.

Remediação

As tarefas realizadas na fase de remediação incluem:

- Priorizar a remediação com base na classificação de risco
- Desenvolver um plano de ação para implementar a recomendação ou remediação
- Realizar uma análise de causa raiz
- Aplicar patches e correções
- Capture as lições aprendidas
- Conduzir treinamento de conscientização
- Realizar tratamento de exceções e aceitação de risco para as vulnerabilidades que não podem ser remediado

Verificação

A fase de verificação ajuda os analistas de segurança a verificar as correções aplicadas examinando novamente os sistemas. Esta fase inclui a verificação das correções utilizadas para corrigir ou mitigar os riscos.

As tarefas realizadas na fase de verificação incluem:

- Verificar novamente os sistemas para identificar se uma correção aplicada foi eficaz na correção da vulnerabilidade
- Execução de análise dinâmica
- Rever a superfície de ataque

Monitoramento

Esta fase realiza o monitoramento de incidentes usando ferramentas como IDS/IPS, SIEM e firewalls. Implementa monitoramento de segurança contínuo para impedir ameaças em constante evolução.

As tarefas realizadas na fase de monitoramento incluem:

- Varredura e avaliação periódica de vulnerabilidade
- Correção oportuna de vulnerabilidades identificadas
- Monitoramento de detecção de intrusão e registros de prevenção de intrusão
- Implementar políticas, procedimentos e controles

Solução de avaliação de vulnerabilidade

As organizações precisam selecionar uma solução de avaliação de vulnerabilidade adequada para detectar, avaliar e proteger seus ativos de TI críticos de várias ameaças internas e externas.

As características de uma boa solução de avaliação de vulnerabilidade são as seguintes:

- Garanta resultados corretos testando a rede, recursos de rede, portas, protocolos, e sistemas operacionais
- Utiliza uma abordagem baseada em referência bem organizada para teste
- Verifica automaticamente seus bancos de dados atualizando-os continuamente
- Cria relatórios breves, acionáveis e personalizáveis, incluindo relatórios de vulnerabilidades por nível de gravidade e análise de tendência
- Suporta várias redes
- Sugere soluções e soluções alternativas adequadas para corrigir vulnerabilidades
- Imita a visão externa dos invasores para atingir seu objetivo

Conceitos de Análise de Vulnerabilidades:

A avaliação da vulnerabilidade desempenha um papel importante no fornecimento de segurança aos recursos e infraestrutura de qualquer organização contra várias ameaças internas e externas. Para proteger uma rede, um administrador precisa realizar o gerenciamento de patches, instalar um software antivírus adequado, verificar as configurações, resolver problemas conhecidos em aplicativos de terceiros e solucionar problemas de hardware com configurações padrão. Todas essas atividades juntas constituem uma avaliação de vulnerabilidade.



TEORIA NA PRÁTICA

CEHv12 (ANSI)

05.Vulnerability Analysis

Nikto - web server scanner

- Acessar sua máquina virtual Kali

1. Abrir o terminal como root
2. Digitar o comando:
3. "nikto -C all --host <Alvo>"
4. "nikto -C all --host <Alvo> --port 443"
5. Analise o resultado

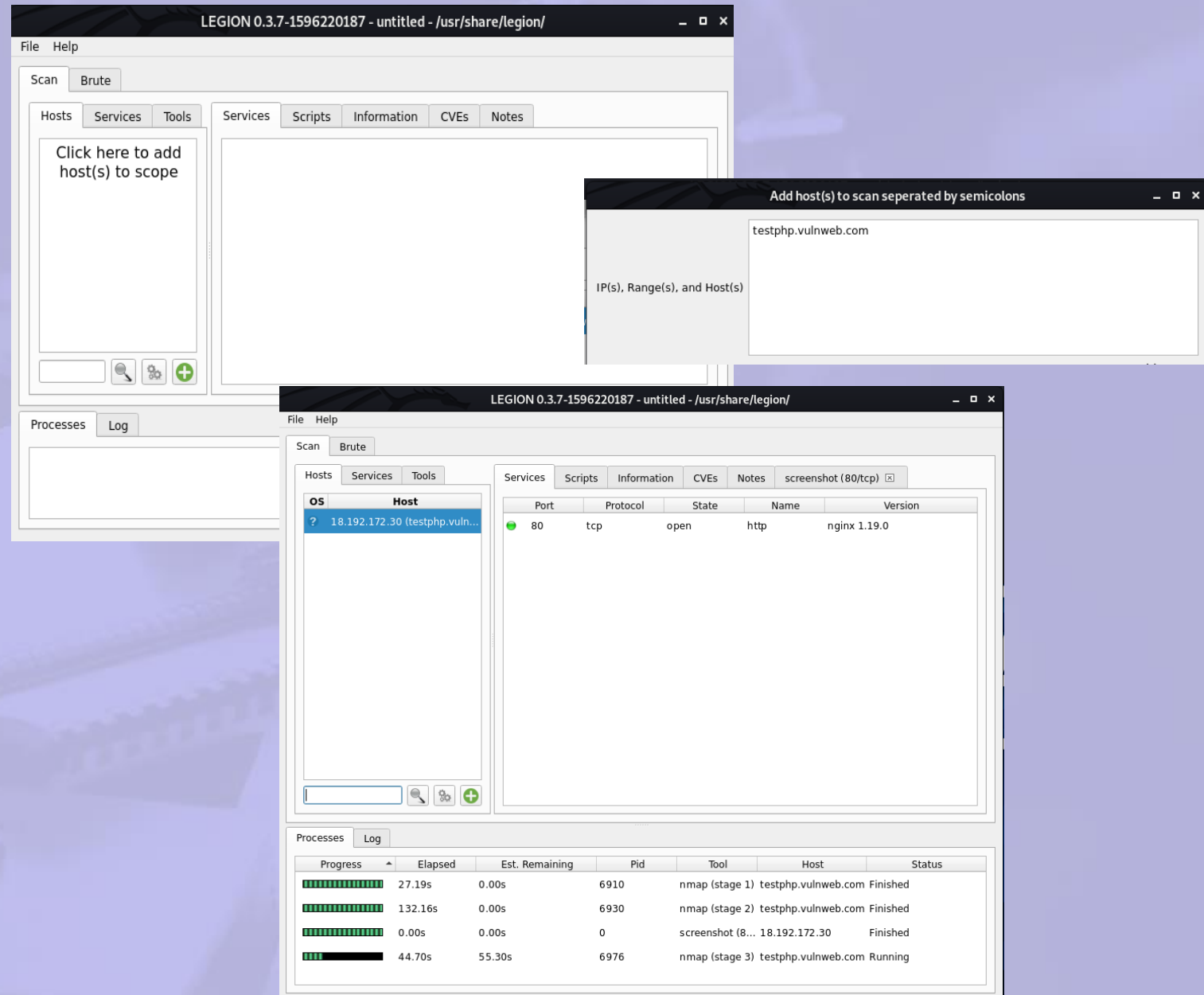
```
(root@kali)-[~]
# nikto --host testphp.vulnweb.com -C all
- Nikto v2.1.6
-----
+ Target IP: 18.192.172.30
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2021-04-03 21:20:46 (GMT-3)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
+ The X-Content-Type-Options header is not set. This could allow the user agent to
  e MIME type
^C
```

```
(root@kali)-[~]
# nikto --host testphp.vulnweb.com -C all --port 443
- Nikto v2.1.6
-----
+ No web server found on testphp.vulnweb.com:443
-----
+ 0 host(s) tested
```

Legion

- Acessar sua máquina virtual Kali

1. Abrir o terminal como root
2. Digitar o comando “#legion”
3. Analise o resultado



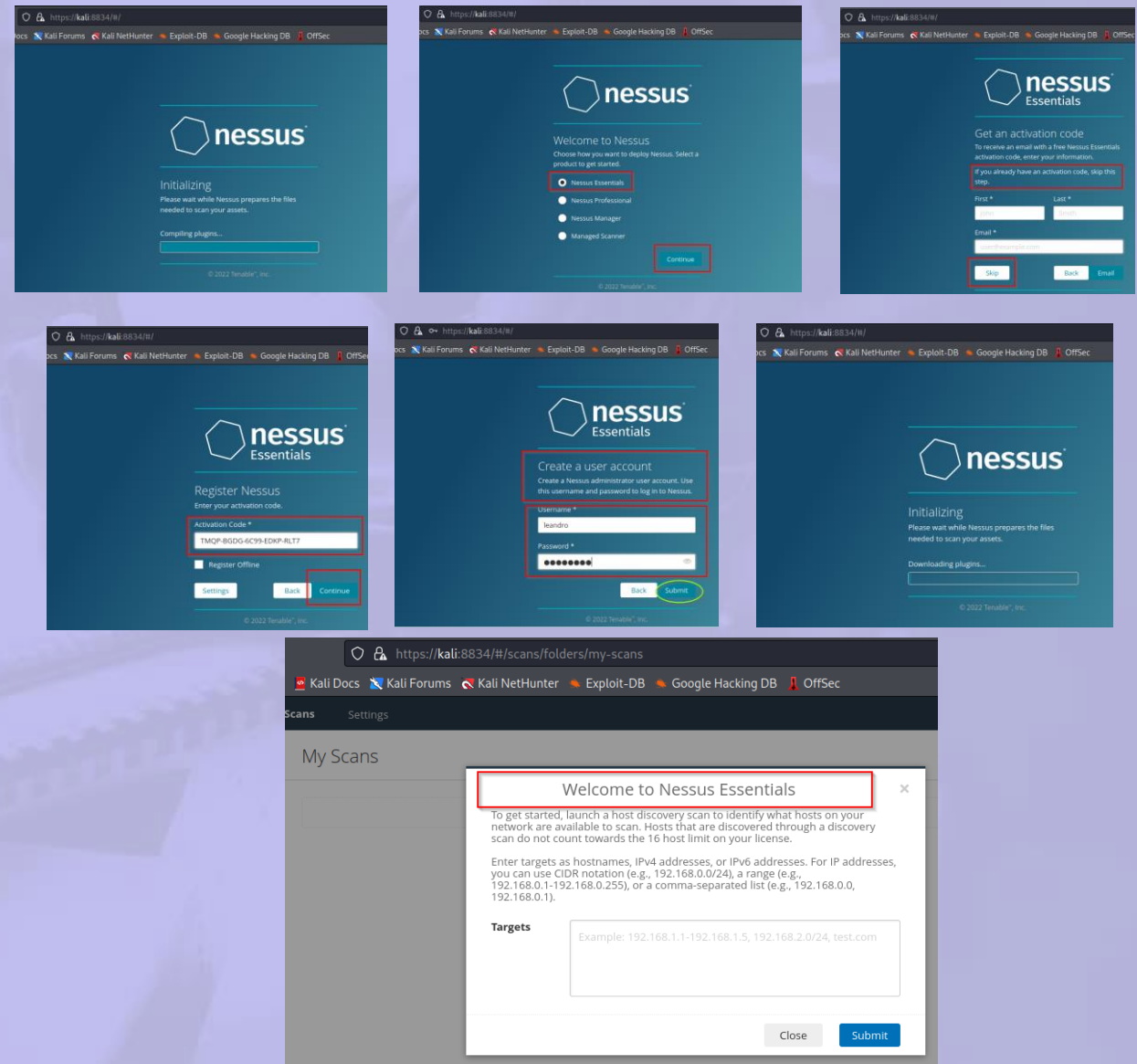
Nessus - Vulnerability Scanner

■ Download Nessus - Vulnerability Scanner

1. <https://www.tenable.com/products/nessus-home>
2. Registre-se para obter a chave home/essentials.
3. Clicar no link de download
4. Escolher a versão para debian 64 bits (Kali Linux)
5. Acessar o diretório onde foi realizado o download do arquivo
6. Execute o comando de instalação: `# dpkg -i nessus-<versão>.deb`
7. Inicie o serviço do nessus conforme instrução, após instalação.

`# /bin/systemctl start nessusd.service`

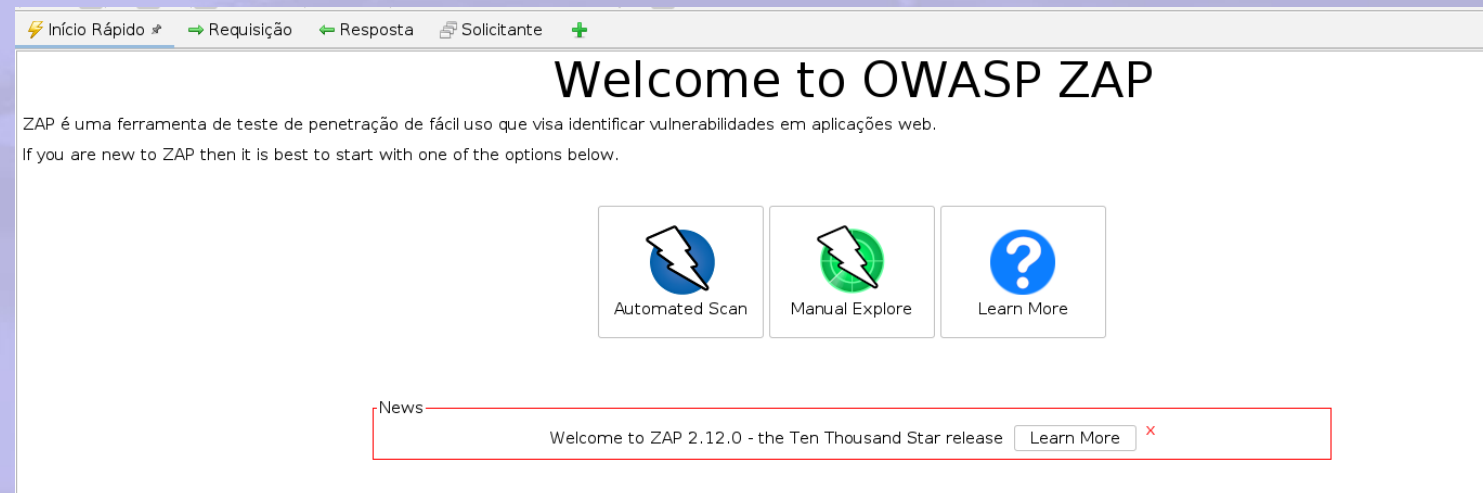
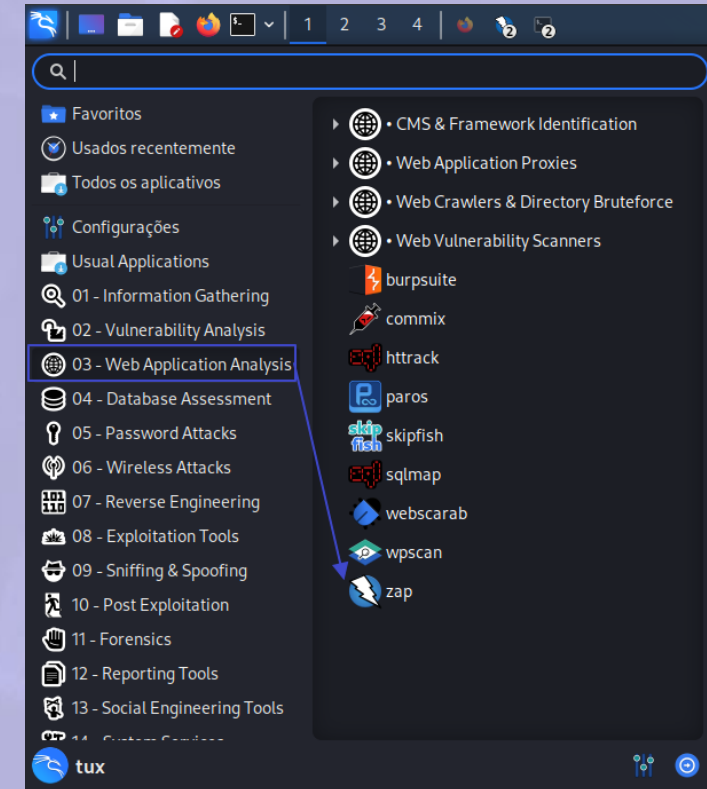
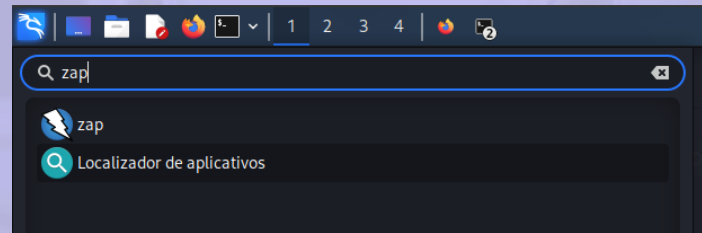
Acesse o navegador em `https://127.0.0.1:8834`



zaproxy - WEB Vulnerability Scanner

- Instalação zaproxy Web Vulnerability Scanner

1. # apt install zaproxy owasp-mantra-ff





Obrigado!

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