

Instalação OpenVAS

Observação: Você deverá “importar a máquina .OVA” disponível no disco D: esse processo leva aproximadamente 15 minutos.

Login: Root Senha: 123@Doc

Atividade 01 – Atualizar Repositório / Instalação do software

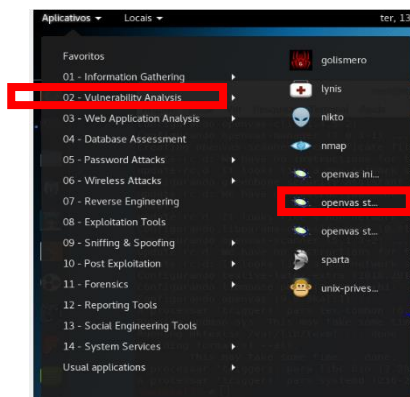
O OpenVas é um suíte de análise de vulnerabilidade, capaz de identificar, classificar e avaliar os riscos em um ambiente corporativos. Como tivemos problemas na instalação do Openvas, criei uma máquina pronta com a ferramenta instalada. Faltando apenas iniciar. Vamos começar?

1. Antes de iniciar crie o usuário suporte, usuário que você realizará autenticação no OpenVas, para criar siga as instruções abaixo:

(Comando create para criação de usuário, role para determinação de Administrador, password para criar senha)

```
root@kali:~# openvasmd --create-user=suporte --role=Admin && openvasmd --user=suporte --new
-password=123@Doc
User created with password '78efc508-459f-4179-82b1-7d63c63e4b30'.
```

2. Clique em “Análise de Vulnerabilidade” e em seguida em “Openvas Start”:



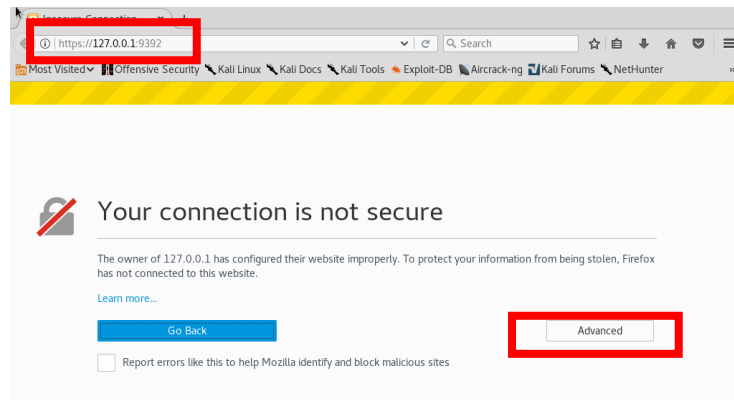
3. Ao dar o start a porta 9392 será aberta e todo o serviço estará ativo:

```
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

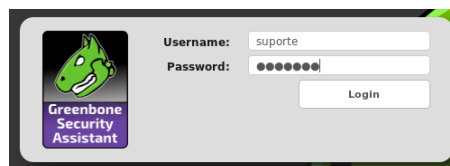
● greenbone-security-assistant.service - Greenbone Security Assistant
   Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2019-02-13 08:43:49 -03; 6s ago
     Docs: man:gsad(8)
           http://www.openvas.org/
    Main PID: 1208 (gsad)
      Tasks: 4 (limit: 4915)
    CGroup: /system.slice/greenbone-security-assistant.service
            └─1208 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --m
listen=127.0.0.1 --mport=9390
                └─1217 /usr/sbin/gsad --foreground --listen=127.0.0.1 --port=9392 --m
listen=127.0.0.1 --mport=9390

fev 13 08:43:49 kali systemd[1]: Started Greenbone Security Assistant.
fev 13 08:43:50 kali gsad[1208]: Warning: MHD_USE_THREAD_PER_CONNECTION must be
used only with MHD_USE_INTERNAL_POLLING_THREAD. Flag MHD_USE_INTERNAL_POLLING_TH
READ was added. Consider setting MHD_USE_INTERNAL_POLLING_THREAD explicitly.
```

4. Abra o navegador Firefox, informe o localhost e a porta 9392, clique em Avançado e Adicione o certificado de segurança:



5. Acesse o painel de controle do greenbone, inserido o login e senha gerados na etapa 01:



6. Explorando a ferramenta. Acesse a guia Administration / users e verifique o usuário suporte tem privilégios de administrador. Para trocar de senha basta clicar no ícone em destaque, nessa guia também podemos criar novos usuários:

Name	Roles	Groups	Host Access	Authentication Type	Actions
suporte	Admin		Allow all and deny:	Local	

7. Ainda na guia Configuration terá vários itens vou listar algumas características:

Target: criar listas diversas para alvos diferentes, podemos criar lista para rede interna, rede externa, além de criar listas para computadores Linux, Windows. Para criar uma nova **target** clique na **estrela**.

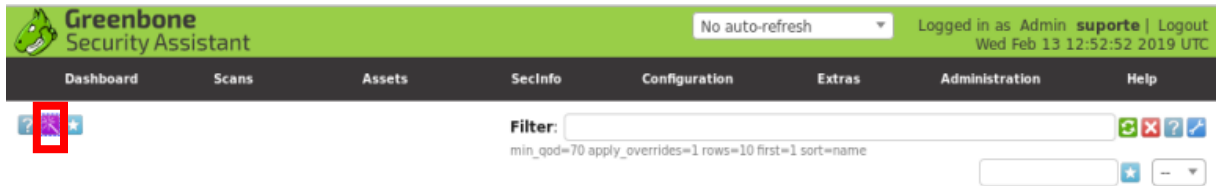
Port List: será exibido uma lista de portas pré configuradas, TCP, UDP. Uma informação importante é que a verificação por portas é um pouco lenta ela prioriza algumas portas, inclusive a do NMAP que é capaz de realizar a varredura de auto nível.

Credentials: Define quais são as credenciais que o Openvas irá utilizar para fazer a análise de vulnerabilidade. Podemos criar uma nova credencial clicando na estrela.

Existem outros tipos de características, já vocês vão explorar para ser apresentado.

Criando um Scan

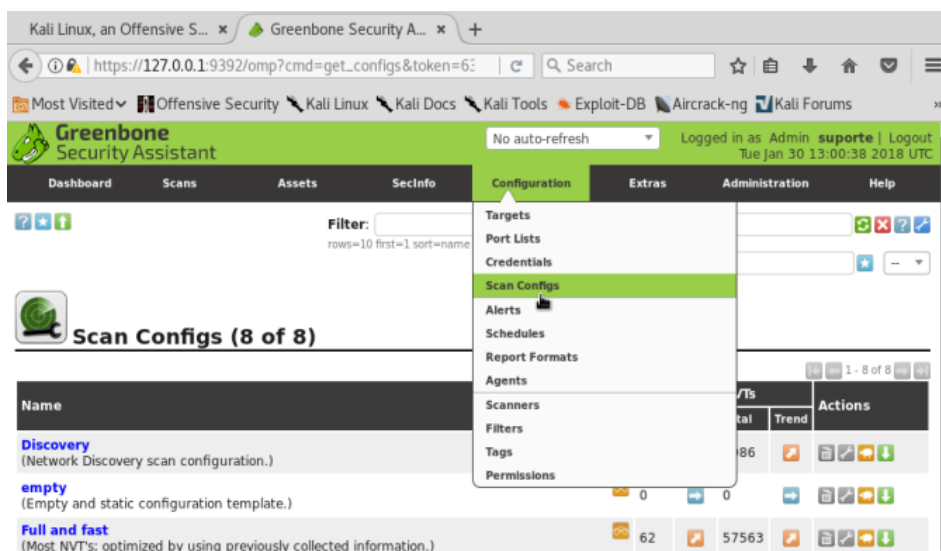
1. Na tela inicial do greenbone, clique na varinha lilás que fica no canto superior esquerdo e em seguida clique em Advanced Task Wizard:



2. Aqui você deverá preencher as informações que vão conter seu novo scan:

Porém nós vamos criar o nosso próprio template! Siga as instruções abaixo:

1. Configurando formas de scan, por padrão o Openvas vem com alguns filtros definidos, porém você pode adicionar novos parâmetros, vá em “Configuração” em seguida “Scan Configs”:



O Openvas é define as vulnerabilidades por NVTs (Teste de Vulnerabilidades de Rede). Cada “Scan Configuration” tem algumas NVTs configuradas.

2. Criando uma nova configuração de Scan: **Clique no ícone da “Estrela”**:



3. Em seguida atribua um nome e em seguida clique em **“create”**:

New Scan Config

Name: Vuln LAN

Comment:

Base: ☒ Empty, static and fast ☐ Full and fast

Create

4. Em seguida edite as configurações, nessa sessão é possível selecionar as **famílias/NVTs**, para essa configuração inicial iremos configurar todos os NVTs: (observação além dos **NVTs**, existem diversas funções que podem ser atribuídas na configuração.)

Edit Scan Config

Name: Vuln LAN

Comment: Empty and static configuration template.

Edit Network Vulnerability Test Families

Family	NVTs selected	Trend	Select all NVTs	Actions
AIX Local Security Checks	0 of 1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
Amazon Linux Local Security Checks	0 of 748	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
Brute force attacks	0 of 9	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
Buffer overflow	0 of 557	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
CISCO	0 of 647	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
CentOS Local Security Checks	0 of 2984	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit
Citrix Xenserver Local Security Checks	0 of 30	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="checkbox"/>	Edit

Save

- Depois de criar um “**Scan Config**” devemos configurar um “**Targets**”, clique na estrelinha e configure o “**Novo Target**” atribua um nome, **deixe padrão Localhost**.

New Target

Name:

Comment:

Hosts: ☒ Manual No file selected.

☐ From file

☐ From host assets (0 hosts)

Exclude Hosts:

Reverse Lookup Only: ☐ Yes ☒ No

Reverse Lookup Unify: ☐ Yes ☒ No

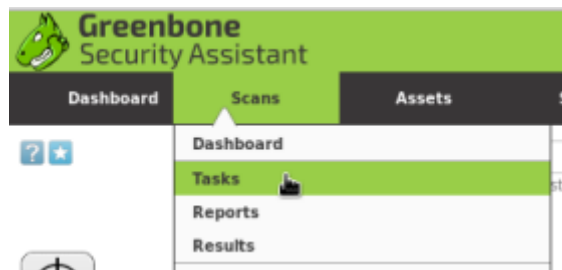
Port List:

Alive Test:

Credentials for authenticated checks:

SSH: on port

- Após criar a **nova targets**, vamos criar uma tarefa de escaneamento, em seguida clique na “**Estrela**”:



- Atribua um nome e clique em “**Create**” na estrela:

New Task

Name:

Comment:

Scan Targets:

Alerts:

Schedule: ☐ Once

Add results to Assets: ☒ yes ☐ no

Apply Overrides: ☒ yes ☐ no

Min QoD: %

Alterable Task: ☐ yes ☒ no

Auto Delete Reports: ☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest reports

Scanner:

Scan Config:

8. Clique na Tarefa e configure para atualizar a cada 30 segundos:

Name	Status	Reports		Severity	Trend
		Total	Last		
Vuln LAN em Kali Linux	New				

9. Após abrir pressione “Play” e defina para atualizar a cada 30 segundos:

The screenshot shows the Greenbone Security Assistant interface. At the top, there is a green header with the logo and navigation tabs: Dashboard, Scans, Assets, SecInfo, Configuration, Extras, Administration, and Help. A dropdown menu is set to 'Refresh every 30 Sec.'. The main content area displays the configuration for a task named 'Teste de Vulnerabilidade Kali Linux'. The task details include:

- Name:** Teste de Vulnerabilidade Kali Linux
- Comment:**
- Target:** kali Linux A
- Alerts:**
- Schedule:** (Next due: over)
- Add to Assets:** yes
- Apply Overrides:** yes
- Min QoD:** 70%
- Alterable Task:** no
- Auto Delete Reports:** Do not automatically delete reports
- Scanner:** OpenVAS Default (Type: OpenVAS Scanner)
- Scan Config:** Full and fast
- Order for target hosts:** Sequential
- Network Source Interface:**
- Maximum concurrently executed NVTs per host:** 4
- Maximum concurrently scanned hosts:** 20
- Status:** Requested
- Duration of last scan:**
- Average scan duration:**

On the right side, there is a sidebar with task metadata:

- ID:** ef273be8-9197-4f38-bd3a-3eb78875ecba
- Created:** Tue Jan 30 14:09:27 2018
- Modified:** Tue Jan 30 14:09:28 2018
- Owner:** suporte

Espere carregar: (esse processo demora uns 10 minutos)

The screenshot shows the Greenbone Security Assistant interface with the task 'Vuln LAN em Kali Linux' in progress. The task details are the same as in the previous screenshot, but the status is now 'Running' and the progress bar shows 22% completion.

- Name:** Vuln LAN em Kali Linux
- Comment:**
- Target:** Kali Linux
- Alerts:**
- Schedule:** (Next due: over)
- Add to Assets:** yes
- Apply Overrides:** yes
- Min QoD:** 70%
- Alterable Task:** no
- Auto Delete Reports:** Do not automatically delete reports
- Scanner:** OpenVAS Default (Type: OpenVAS Scanner)
- Scan Config:** Full and fast
- Order for target hosts:** Sequential
- Network Source Interface:**
- Maximum concurrently executed NVTs per host:** 4
- Maximum concurrently scanned hosts:** 20
- Status:** Running 22%

11. Após conclusão o **Openvas** irá classificar os riscos e informar quais foram as **vulnerabilidades**:

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Tue Jan 30 14:11:16 2018	1 %	Teste de Vulnerabilidade Kali Linux	N/A	0	0	0	0	0	 



12. Quando concluir o **Status**, irá aparecer a informações contendo qual foi o resultado do **Scan**:

Status	Task	Severity	Scan Results				
			High	Medium	Low	Log	False Pos.
Done	Vulnerabilidades em Kali Linux	4.3 (Medium)	0	4	0	19	0


13. Clique sobre a data de execução para exibir as **vulnerabilidades**:

Report: Results 1 - 23 of 23 (total: 23) PDF					
Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=					
Vulnerability	Severity	Host	Location	Actions	
Check for SSL Weak Ciphers	4.3 (Medium)	10.0.2.5	9390/tcp	 	
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	10.0.2.5	9390/tcp	 	
Check for SSL Weak Ciphers	4.3 (Medium)	10.0.2.5	9392/tcp	 	
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	10.0.2.5	9392/tcp	 	
CPE Inventory	0.0 (Log)	10.0.2.5	general/CPE-T	 	
Host Summary	0.0 (Log)	10.0.2.5	general/HOST-T	 	

14. Clique nas informações caso queira detalhes sobre cada tipo de vulnerabilidades, inclusive ele informa solução para o problema:

Vulnerability	Severity	Host	Location	Actions
Check for SSL Weak Ciphers	4.3 (Medium)	10.0.2.5	9390/tcp	 
Summary This routine search for weak SSL ciphers offered by a service.				
Vulnerability Detection Result Weak ciphers offered by this service: SSL3_RSA_RC4_128_MD5 SSL3_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA				
Solution The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.				
Vulnerability Insight These rules are applied for the evaluation of the cryptographic strength: <ul style="list-style-type: none"> - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. 				

15. Você pode gerar um relatório com as principais vulnerabilidades:

	High	Medium	Low	Log	False Pos.	Total	Run Alert	Download
Full report:	0	4	0	19	0	23		PDF 

Relatório de Vulnerabilidade

No teste de vulnerabilidade acima, mostramos as vulnerabilidades na Máquina Kali.

Execute um novo scan (**adicionando o nome que quiser**) seguindo o tutorial acima, e **faça uma análise em todas as máquinas da rede** e no final você deve gerar um relatório sobre as principais vulnerabilidades encontradas na rede, mostrando algo como:

- (a) Número de vulnerabilidades, níveis de severidade (Alto, Médio, Baixo)
- (b) Mostrando os resultados relativos à **Host-Porta-Serviço-Severidade**, quanto a indicação sobre um **“Security Hole”** (uma vulnerabilidade encontrada), uma **“Security Warning”** (advertência) ou uma **“Security Note”** (nota sobre segurança), **impacto, software afetado**, o que deve ser feito para **consertar a vulnerabilidade**, entre outras informações.

Crie um projeto simples e apresente ao Professora.

- (a) Informe o nome de sua tarefa.
- (b) O escopo de sua tarefa.
- (c) O seu alvo.
- (d) Quantas vulnerabilidades de nível ALTO.
- (e) Quantas vulnerabilidades de nível MÉDIO.
- (f) Quantas vulnerabilidades de nível BAIXO.
- (g) Exemplifique uma vulnerabilidade encontrada.
- (h) Indique o impacto.
- (i) Indique o software afetado.
- (j) Indique o que fazer para contornar a vulnerabilidade.
- (k) Válido consultar normas, livros, internet.
- (l) Incluir referencias.