Segurança
Experimento N°03
Frameworks e Aplicativos e Códigos-Fonte

Disciplina	**Segurança em Redes de Computadores**
Professor:	**Rafael Timóteo de Sousa Júnior**
Monitores:	**Valério Martins (valerioaymoremartins@gmail.com)** **Mariana Stieljes**

1. Introdução:

O modelo desse experimento é mostrar a possibilidade de realizar testes de penetração através de códigos gerados usando bibliotecas Python, aplicativos em linha de comando do Linux Kali ou frameworks completos.

Serão realizados os primeiros procedimentos para reconhecimento de aplicações dentro do ambiente Linux Kali, ainda com foco na recuperação de informações (1) e Análise de Vulnerabilidades (2).

Lembramos que para estudo de tal atividade, não serão aceitas realizações pelos alunos que envolvam sites de terceiros e/ou externos ao ambiente controlado do laboratório, pois, como já exposto em diversas aulas, essas atividades são passíveis do entendimento da realização de um crime cibernético, passível de punição judicial.

2. Ambiente e Necessidades Preliminares

- **apt install firefox-esr**
- **Conhecimentos Adicionais:** Conhecimento da navegação no ambiente Linux Kali

1) Recupere seu IP e do servidor

2) Ative o wireshark dentro de seu ambiente virtual

3) Edite o arquivo "/usr/share/wordlists/nmap.lst"
insira o a palavra "postgres" no início da lista

Obs.: se você quiser economizar esforços faça uma lista idêntica somente com a palavra "postgres". Anote o nome desse novo arquivo.

4) Ative o apache2
service apache2 start

4) Instale e ative o postgresql
apt-get install postgresql postgresql-contrib
vi /etc/postgresql/10/main/postgresql.conf
    listen_address='*'
service postgresql start

sudo -u postgres psql postgres
psql
\password postgres
<password>=postgres
\q

vi /etc/postgresql/10/main/pg_hba.conf
obs.: mude os peer por md5...
local all all peer -----> md5
service postgresql restart

obs.: teste ...
psql -U postgres
<senha>: postgres
\q

5) Instale e ative o vsftp
apt-get install vsftpd
service vsftpd start

6) Para próximo aula estude os elementos envolvidos no que se refere a comunidade **OWASP (Open Web Applicatuon Security Project)**

3. Experimento

3.1) Aplicativos:

3.1.1) nmap:

Nmap (network mapper) é o mais otimizado scanners de porta (custo x benefício) usados para descoberta de rede e a base para a maioria das varreduras de segurança durante os estágios iniciais de um teste de penetração. <https://nmap.org/book/nmap-phases.html>

3.1.2) nikto:

Nikto Web Scanner é um é um scanner de servidor da Web que testa servidores da Web para arquivos / CGIs perigosos, software desatualizados no servidor e outros problemas. Ele executa verificações genéricas e específicas do tipo de servidor. Também captura e imprime quaisquer cookies recebido.

Há uma série de ferramentas e aplicativos para encontrar vulnerabilidades em sites, mas um dos mais simples é o nikto. Embora seja extremamente útil e eficaz, não é tão "furtiva". Qualquer site com um IDS ou outras medidas de segurança implementadas detectarão que você está scaneando-o. Para uso em modelos de ataque para avaliações locais ele tem interesse

Anote a questão: Explique os recursos do nikto.

3.1.3) hydra:

Hydra é um cracker de login paralelizado que suporta vários protocolos para atacar. É muito rápido e flexível, e novos módulos são fáceis de adicionar. Essa ferramenta possibilita que pesquisadores e consultores de segurança mostrem como seria fácil obter acesso não autorizado a um sistema remotamente

Anote a questão e explique os resultados:

hydra –L /usr/share/wordlists/nmap.lst –P /root/Desktop/pass.txt 192.168.1.120 postgres

veja em: <http://www.hackingarticles.in/6-ways-to-hack-postgressql-login/>

3.1.4) cisco-torch

É uma ferramenta de varredura em massa, identificação (fingerprint) e exploração da Cisco. A principal característica é o seu uso extensivo de ***fork*** para lançar vários processos de *scanning* em segundo plano para obter melhor eficiência no tempo. Além disso, ele usa vários métodos de identificação (fingerprint) da camada de aplicação simultaneamente, se necessário.

cisco-torch <options> <IP,hostname,network>
cisco-torch <options> -F <hostlist>

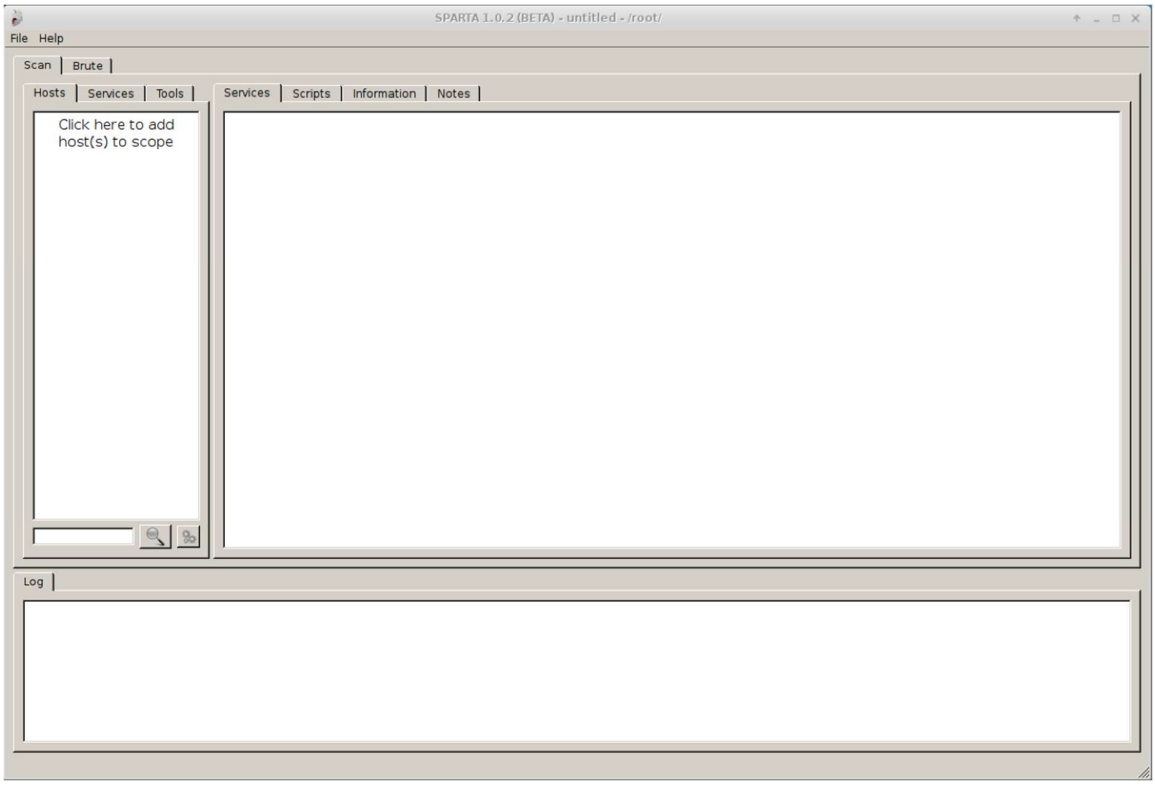
-A All fingerprint scan types combined
-t Cisco Telnetd scan
-s Cisco SSHd scan
-u Cisco SNMP scan
-g Cisco config or tftp file download
-n NTP fingerprinting scan
-j TFTP fingerprinting scan
-l <type> loglevel, c critical (default), v verbose, d debug
-w Cisco Webserver scan
-z Cisco IOS HTTP Authorization Vulnerability Scan
-c Cisco Webserver with SSL support scan
-b Password dictionary attack (use with -s, -u, -c, -w , -j or -t)
-V Print tool version and exit
Exemplos:
cisco-torch -A 10.10.0.0/16
cisco-torch -s -b -F sshtocheck.txt
cisco-torch -w -z 10.10.0.0/16
cisco-torch -j -b -g -F tftptocheck.txt

Anote a questão: Execute e explique um simples comando cisco-torch.

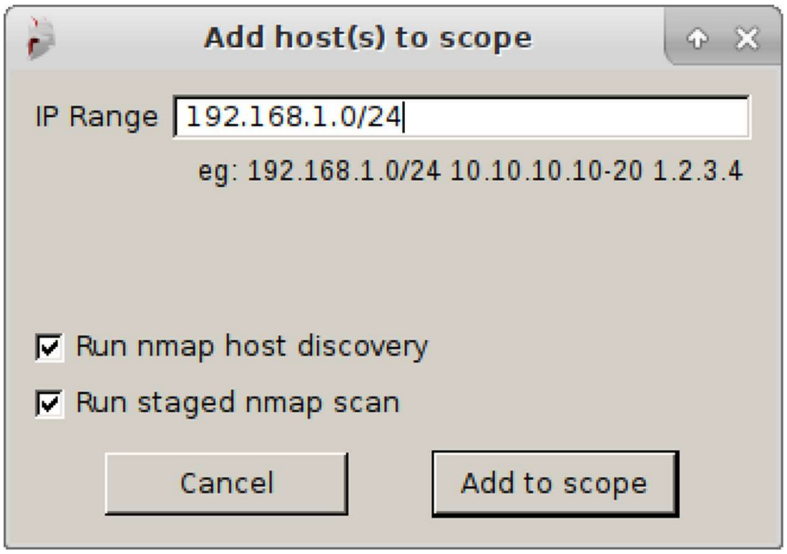
3.2) Frameworks

3.2.1) Sparta

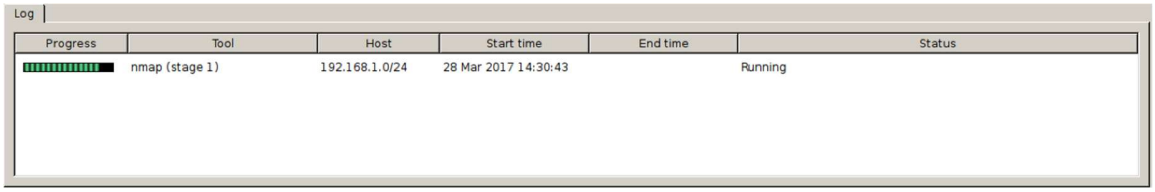
Quando o SPARTA é lançado pela primeira vez, seja através do menu Kali ou executando o “sparta” na linha de comando, a interface principal será aberta, apresentando o seu espaço de trabalho. Inicialmente, o painel de hosts estará vazio para que você possa importar um arquivo de resultados de varredura do Nmap ou, como mostra este exemplo, clicar no painel no texto “Click here to add host(s) to scope“.

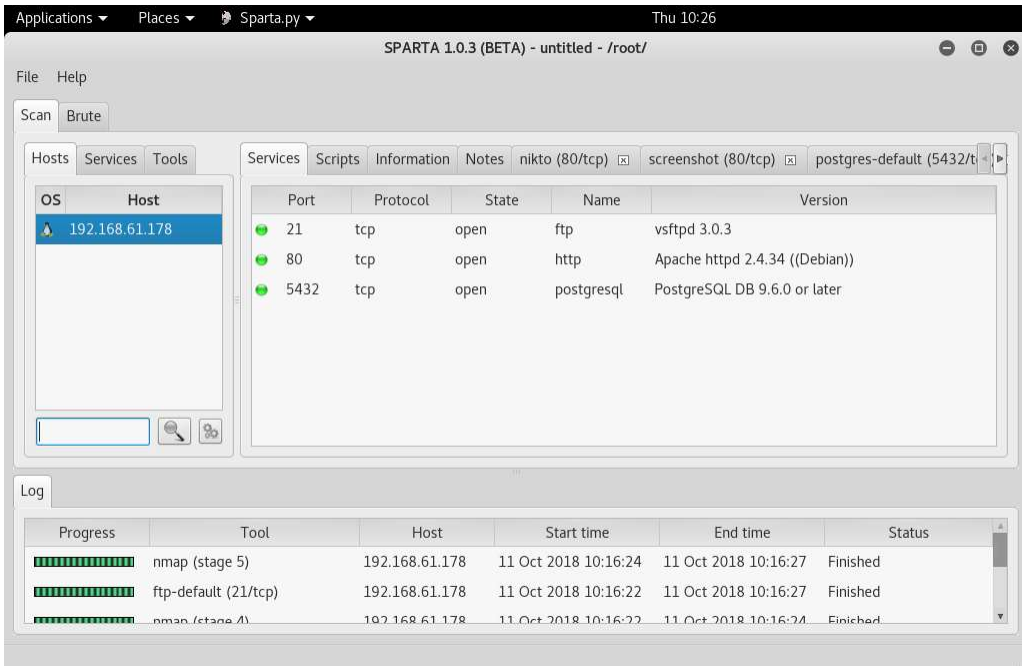


a) **Adicione inicialmente o SEU host (IP).**
Anote a questão: o que é “staged nmap scan”.



b) **Depois de clicar em "Add to scope", a verificação do Nmap começará e nos será apresentado um indicador de progresso no painel Log.**
Anote a questão: o Sparta é uma aplicação integrada ou ele está usando recursos de outros aplicativos. Identifiquw esses.
Demora um tempo para o Sparta fazer uma detecção completa, mas quando alguns hosts (no caso o seu) e serviços são encontrados ele vai apresentando





c) Navegue em cada lapela.
Anote a questão: Explique o resultado em cada lapela.
Na lapela Tools aparecem algumas ferramemtas. Porquê somente essas ferramentas? (ftp-default, postgres-deafult)?

Serviços que requerem um login, como telnet, SSH, HTTP, etc. podem ser enviados para a ferramenta de força bruta para tentar quebrar a senha.

d) Voltando a lapela Hosts, selecione com o botão direito sobre o serviço (porta/protocolo) do postgres. ... "Send to Brute".

e) Defina o usuário "postgres" e aponte a lista de senhas para o arquivo "/usr/share/wordlists/nmap.lst"

Depois dessas configurações, deixamos o SPARTA começar a atacar a senha do postgres (que nós colocamos na lista de palavras pré-definidas).

Anote a questão: como são esses ataques (você acionou o wireshark?). O que o SPARTA mostra nesse momento.