

# Pentest+ Tools Study Guide

- Tools and demonstrations
- Common tools you can see on the test or use on a pentest



Written by  
CyberMedic  
AKA: Robert Boettger

SCANNERS

# nikto

Nikto is a widely used open-source web server scanner that helps identify potential vulnerabilities in web servers and web applications. It's designed to perform comprehensive scans and security assessments to detect various issues that could be exploited by attackers

# Nikto

a Practical Website Vulnerability Scanner



```
Scanner Source IP: 66.175.214.247
1 Scanner Source IP: 66.175.214.247
2 User Agent: Nikto 2.1.5
3
4 - Nikto v2.1.5
5 -----
6 + Target IP:          65.x.x.x
7 + Target Hostname:   example.com
8 + Target Port:       80
9 + Start Time:        2019-02-01 12:17:06 (GMT0)
10 -----
11 + Server: Microsoft-IIS/8.5
12 + Retrieved x-powered-by header: ASP.NET
13 + Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;
14 + Uncommon header 'content-security-policy' found, with contents: default-src 'self' 'unsafe-inline' examp
'self' 'unsafe-inline' 'unsafe-eval' example.com; style-src 'self' 'unsafe-inline' example.com maxcdn.boot
15 + Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN example.com
16 + Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
17 + Retrieved x-aspnet-version header: 4.0.1219
18 + Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x4e234235saed08bddd:0
19 + robots.txt contains 2 entries which should be manually viewed.
20 + RFC-1918 IP address found in the 'location' header. The IP is 10.23.1.3.
21 + OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images di
is http://10.23.1.3/images/.
22 + Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
23 + Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
24 + Cookie PHPSESSID created without the httponly flag
25 + /login.php: Admin login page/section found.
26 + 5567 items checked: 0 error(s) and 14 item(s) reported on remote host
27 + End Time:          2019-02-01
```

Nikto detects security related issues in web scripts and web server configuration

Unusual items are always worth investigating

Ran 5567 tests and found 14 items of interest

# openvas

- OpenVAS, which stands for "Open Vulnerability Assessment System," is a comprehensive open-source vulnerability scanning and management tool designed to help users detect and manage security vulnerabilities in computer systems and networks. It is a powerful tool for identifying potential security issues, misconfigurations, and weaknesses in the target environment.
- Key point – types of scans



# OpenVAS

Open Vulnerability Assessment Scanner



Filter



**Report** **Wed, May 3, 2023 12:35 PM**  
**t: UTC**

Done

ID: 008b5e66-5c8e-4136-abfe-0c9dc3c00c83

Created: Wed, May 3, 2023 12:35 PM UTC

Modified: Wed, May 3, 2023 1:00 PM UTC

Owner: admin

Information

**Results**  
(259 of 341)

Hosts  
(1 of 1)

Ports  
(4 of 9)

Applications  
(7 of 7)

Operating Systems  
(1 of 1)

CVEs  
(107 of 107)

Closed CVEs  
(7 of 7)

TLS Certificates  
(2 of 2)

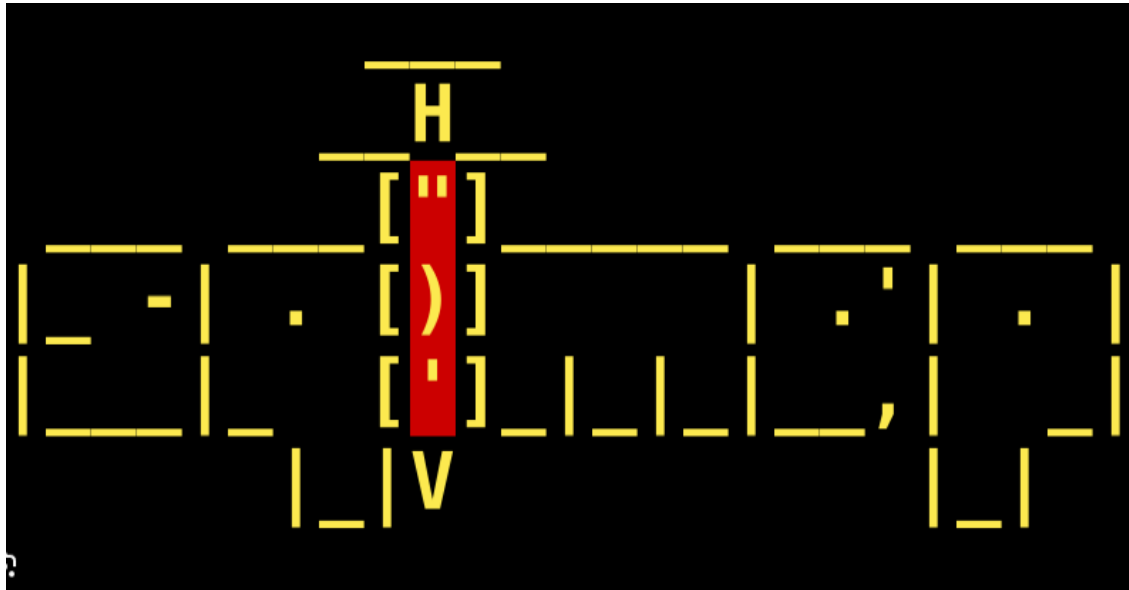
Error Messages  
(0 of 0)

User Tags  
(0)

1 - 100 of 259

Vulnerability	Severity	QoD	Host		Location	Created
			IP	Name		
OpenSSL End of Life (EOL) Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP End Of Life Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP End Of Life Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:43 PM UTC
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	general/tcp	Wed, May 3, 2023 12:37 PM UTC
OpenSSL End of Life (EOL) Detection (Windows)	10.0 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:43 PM UTC
jQuery End of Life (EOL) Detection (Windows)	9.9 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	80/tcp	Wed, May 3, 2023 12:44 PM UTC
PHP Multiple Vulnerabilities - 01 - Aug16 (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Windows)	9.8 (High)	80 %	10.10.183.198	ip-10-10-183-198.eu-west-1.compute.inter...	443/tcp	Wed, May 3, 2023 12:43 PM UTC

- sqlmap
- SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. SQL injection is a common and potentially serious security flaw that occurs when an attacker can manipulate an application's SQL query by injecting malicious SQL code







nessus

- . It is designed to help organizations identify and assess security vulnerabilities in their computer systems, networks, and web applications. Nessus is known for its extensive vulnerability database, ease of use, and robust reporting capabilities
- Key points – types of scans



## FOLDERS

- My Scans
- All Scans
- Trash

## RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

## Lab Scan

[← Back to My Scans](#)

Configure

Launch ▾

Export ▾

Hosts 9

Vulnerabilities 144

Remediations 216

History 1

1 Filter ▾

Search Vulnerabilities



144 Vulnerabilities

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

## Scan Details

Name: Lab Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 5:31 PM  
End: Today at 6:01 PM  
Elapsed: 30 minutes

## Vulnerabilities



- Critical
- High
- Medium
- Low
- Info



```
(cybermedic@) ~ -[~]
$ wapiti -u http://10.10.147.81/
```



Wapiti-3.0.4 (wapiti.sourceforge.io)

[\*] Resuming scan from previous session, please wait

[\*] Saving scan state, please wait...

Note

This scan has been saved in the file /home/cybermedic/.wapiti/scans/10.10.147.81\_folder\_8269cd49.db

[\*] Wapiti found 5 URLs and forms during the scan

[\*] Loading modules:

backup, blindsqli, brute\_login\_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http\_headers, methods, nikto, permanentx

[\*] Launching module csp

CSP is not set

[\*] Launching module http\_headers

Checking X-Frame-Options :

X-Frame-Options is not set

Checking X-XSS-Protection :

X-XSS-Protection is not set

Checking X-Content-Type-Options :

X-Content-Type-Options is not set

Checking Strict-Transport-Security :

Strict-Transport-Security is not set

[\*] Launching module cookieflags

# wpscan

- open-source security scanning tool specifically designed for WordPress websites and web applications. It is used to identify security vulnerabilities and weaknesses in WordPress installations, themes, and plugins.

```
(cybermedic@~)-[~]
$ wpscan -h

WordPress Security Scanner by the WPScan Team
Version 3.8.24

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Usage: wpscan [options]
  --url URL           The URL of the blog to scan
                     Allowed Protocols: http, https
                     Default Protocol if none provided: http
                     This option is mandatory unless update or help or h
  -h, --help         Display the simple help and exit
  --hh              Display the full help and exit
  --version          Display the version and exit
```

```
(cybermedic@kali:~)
$ wpscan --url http://10.10.124.7
```



Watch on YouTube

WordPress Security Scanner by the WPScan Team  
Version 3.8.24

Sponsored by Automattic - <https://automattic.com/>  
@WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

Active Machine

	Title	IP Address
[+] URL:	http://10.10.124.7/ [10.10.124.7]	10.10.124.7
[+] Started:	Tue Sep 12 18:45:30 2023	

### Interesting Finding(s):

#### [+] Headers

| Interesting Entries:

| - Server: Apache

| - X-Mod-Pagespeed: 1.9.32.3-4523

| Found By: Headers (Passive Detection)

| Confidence: 100%

#### [+] robots.txt found: http://10.10.124.7/robots.txt

| Found By: Robots Txt (Aggressive Detection)

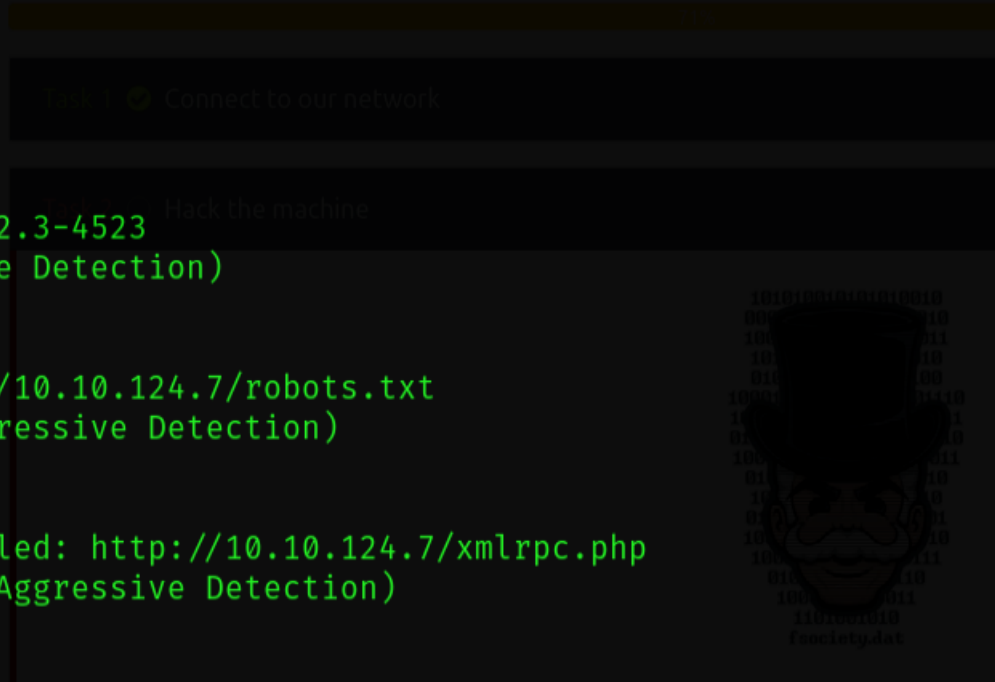
| Confidence: 100%

#### [+] XML-RPC seems to be enabled: http://10.10.124.7/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:



brakeman • an open-source security scanning tool specifically designed for Ruby on Rails applications. It is used to identify security vulnerabilities and potential security risks in Ruby on Rails web applications. Brakeman is often used by developers, security professionals, and DevOps teams to assess and improve the security of Ruby on Rails applications.



Generating report...

== Brakeman Report ==

Application Path: /Users/[REDACTED]/redstore

Rails Version: 7.0.4.2

Brakeman Version: 5.4.1

Scan Date: 2023-02-22 20:12:45 +0700

Duration: 0.419307 seconds

Checks Run: BasicAuth, BasicAuthTimingAttack, CSRFTokenForgeryCVE, ContentTag, CookieSerialization, CreateWith, CrossSiteScripting, DefaultRoutes, Deseriali ze, DetailedExceptions, DigestDoS, DynamicFinders, EOLRails, EOLRuby, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, Forge rySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONEntityEscape, JSONParsing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAcce ssible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass, NumberToCurrency, PageCachingCVE, Pathname, PermitAttributes, QuoteTableN ame, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManipulation, SanitizeConfigCve, S anitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter, Sprocket sPathTraversal, StripTags, SymbolDoSCVE, TemplateInjection, TranslateBug, UnsafeReflection, UnsafeReflectionMethods, ValidationRegex, VerbConfusion, WeakRSA Key, WithoutProtection, XMLDoS, YAMLParsing

== Overview ==

Controllers: 1

Models: 1

Templates: 2

Errors: 0

Security Warnings: 0

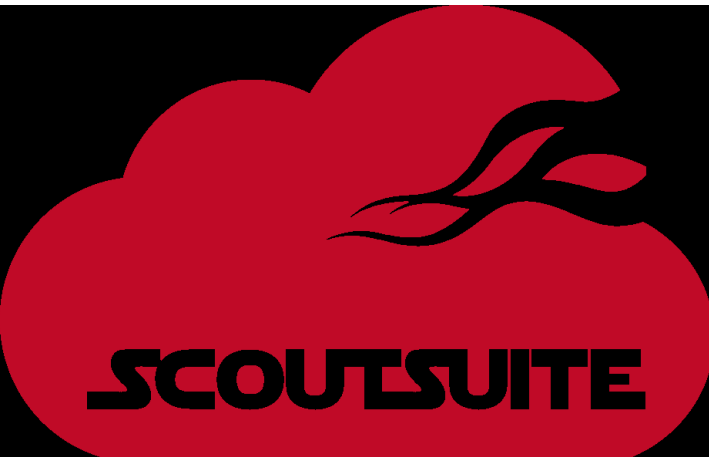
== Warning Types ==

No warnings found



# Scout suite

- an open-source multi-cloud security auditing tool designed to assess the security posture of cloud environments. It supports major cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)



CREDINATIAL  
HARVESTING  
TOOLS

# hashcat

- open-source password recovery tool that is used for cracking password hashes through various attack methods
- Hashcat supports a broad range of cryptographic hash algorithms, including popular ones like MD5, SHA-1, SHA-256, and bcrypt, among many others. It can also handle custom hash algorithms.





# medusa

- used open-source network login brute force tool. It is designed to perform various forms of brute force attacks against network services to gain unauthorized access.
- **Brute Force Attacks:** Medusa primarily conducts brute force attacks against network services that require authentication, such as SSH, FTP, Telnet, HTTP, and more. It tries multiple username and password combinations until it finds a valid one.



# hydra

- Hydra is a popular and powerful password-cracking tool and network logon cracker that can be used to perform various types of attacks against network services. It is often used by cybersecurity professionals and hackers to test the security of systems and applications.
- Hydra supports a wide range of protocols and services, including:
  - SSH (Secure Shell)
  - FTP (File Transfer Protocol)
  - HTTP (Hypertext Transfer Protocol)
  - SMB (Server Message Block)
  - RDP (Remote Desktop Protocol)
  - Telnet
  - MySQL
  - PostgreSQL
  - VNC (Virtual Network Computing)
  - SNMP (Simple Network Management Protocol)



```
root@kali:~# hydra -l testuser -P /usr/share/wordlists/rockyou.txt -f localhost ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 16:40:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344238 to do in 1484:55h, 16 active
[22][ssh] host: localhost login: testuser password: peanut
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 16:41:37

root@kali:~#
```

```
([REDACTED])-[~/hydra]
```

```
$ hydra -l molly -P /usr/share/wordlists/rockyou.txt.gz 10.10.76.78 -t 4 ssh
```

```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-03 15:17:26
```

```
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
```

```
[DATA] attacking ssh://10.10.76.78:22/
```

```
[22][ssh] host: 10.10.76.78 login: molly password: butterfly
```

```
1 of 1 target successfully completed, 1 valid password found
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-03 15:18:26
```

```
([REDACTED])-[~/hydra]
```

```
$
```



# CeWL

- The name "CEWL" stands for "Custom Word List generator."
- This tool is used to generate custom wordlists or dictionaries by crawling and scraping web content from a target website



```
└─$ cewl -m 2 -w Possible_Passwords.txt https://www.robertboettger.com/  
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)  
^C Hold on, stopping here ...
```

```
└─$ cat Possible_Passwords.txt  
the  
and  
to Robert Boettger  
is  
of  
in  
on  
this  
with  
for
```

# John The Ripper

- "John," is a powerful and widely used open-source password cracking tool.
- designed to identify weak passwords by conducting various types of password attacks, including dictionary attacks, brute-force attacks, and hybrid attacks.



# John the ripper cont...

- **Dictionary Attacks:** John can perform dictionary attacks, where it uses a predefined list of words and phrases (the "dictionary") to guess passwords.
- **Brute-Force Attacks:** It can conduct brute-force attacks by systematically trying all possible password combinations until the correct one is found.
- **Hybrid Attacks:** John supports hybrid attacks, which combine elements of dictionary attacks and brute-force attacks, making them more efficient.

```
(██████████)-[~/Downloads/first_task_hashes]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-whirlpool hash4.txt
```

Unknown ciphertext format name requested

```
(██████████)-[~/Downloads/first_task_hashes]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=whirlpool hash4.txt
```

Using default input encoding: UTF-8

Loaded 1 password hash (whirlpool [WHIRLPOOL 32/64])

Warning: poor OpenMP scalability for this hash type, consider --fork=8

Will run 8 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status

colossal (?)

1g 0:00:00:00 DONE (2023-07-03 20:30) 5.882g/s 4047Kp/s 4047Kc/s 4047KC/s davita1..blah2007

Use the "--show" option to display all of the cracked passwords reliably

Session completed.

# Cain

- Cain & Abel, often referred to simply as "Cain," is a versatile and popular password recovery and hacking tool designed primarily for Windows operating systems. It is widely known in the information security community and can be used for various purposes, including password cracking, network sniffing, and security assessments



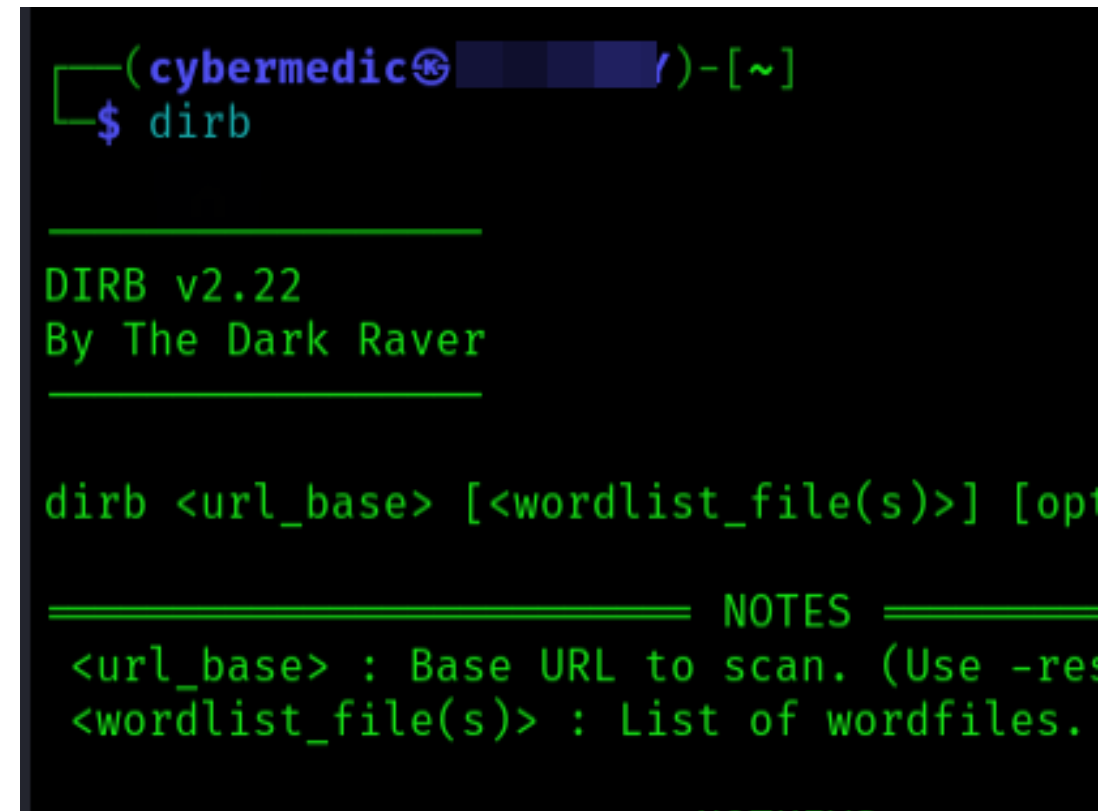
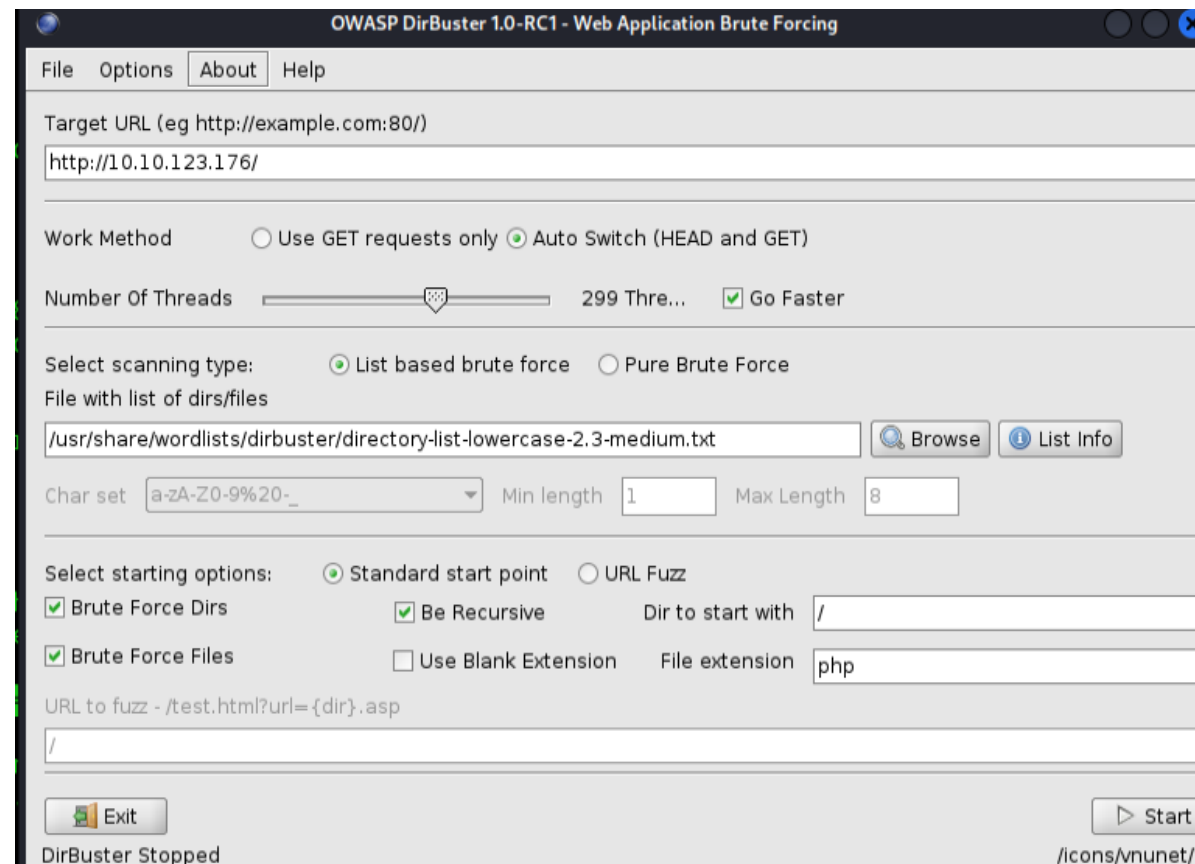
**Cain and Abel**

# Mimikatz

- Mimikatz is a powerful post-exploitation tool used for retrieving sensitive information from Windows-based systems, particularly credentials and authentication tokens stored in memory.
- **Credential Extraction:** Mimikatz is primarily used to extract credentials and related information from memory, including passwords, NTLM hashes, Kerberos tickets, and plaintext passwords, as well as cached and stored credentials.
- Most common – downloaded onto host target during pentest
- Remove after pentest!! Clean up process

# Dirbuster Dirb as well

- an open-source web application security tool designed to help identify hidden directories and files on web servers.
- **Directory and File Enumeration:** DirBuster performs directory and file brute-forcing or wordlist-based enumeration, attempting to locate directories and files that are not explicitly linked from a website's visible pages.





```
└─$ dirb http://10.10.123.176:80
```

---

```
DIRB v2.22  
By The Dark Raver
```

---

```
START_TIME: Tue Sep 12 18:25:03 2023  
URL_BASE: http://10.10.123.176:80/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

---

```
GENERATED WORDS: 4612
```

```
—— Scanning URL: http://10.10.123.176:80/ ——  
-→ Testing: http://10.10.123.176:80/_vti_cnf
```

File Options About Help

http://10.10.124.7:80/

Scan Information Results - List View: Dirs: 1 Files: 1 Results - Tree View Errors: 0

Type	Found	Response	Size
File	/index.php	301	275
Dir	/	200	1477
Dir	/images/	403	399

Current speed: 8 requests/sec

(Select and right click for more options)

Average speed: (T) 9, (C) 10 requests/sec

Parse Queue Size: 0

Current number of running threads: 100

Total Requests: 316/882192

 Change

Time To Finish: 24:29:47

Back

Pause

Stop

Report

Starting dir/file list based brute forcing

/crack

- w3af
- "Web Application Attack and Audit Framework," is an open-source and widely used web application security testing tool.
  - w3af combines automated scanning with manual testing capabilities, making it a versatile tool for web application security assessments.





Scan config Log Results Exploit

Profiles

OWASP\_TOP10

diamantes

fast\_scan

full\_audit

full\_audit\_manual\_disc

test

Target:  Start

Plugin	Active
▶ audit	<input type="checkbox"/>
▶ bruteforce	<input type="checkbox"/>
▼ discovery	<input type="checkbox"/>
MSNSpider	<input type="checkbox"/>
_mailer	<input type="checkbox"/>
_web20Spider	<input type="checkbox"/>
afd	<input type="checkbox"/>
<b>allowedMethods</b>	<input type="checkbox"/>
archiveDotOrg	<input type="checkbox"/>
crossDomain	<input type="checkbox"/>
detectReverseProxy	<input type="checkbox"/>
detectTransparentProxy	<input type="checkbox"/>
detectWAF	<input type="checkbox"/>
diqitSum	<input type="checkbox"/>

Plugin	Active
▼ output	<input type="checkbox"/>
console	<input type="checkbox"/>
gtkOutput	<input checked="" type="checkbox"/>
htmlFile	<input type="checkbox"/>
textFile	<input type="checkbox"/>
webOutput	<input type="checkbox"/>

**allowedMethods**

This plugin finds what HTTP methods are enabled for a URI.

Two configurable parameters exist:

- execOneTime
- reportDavOnly

If "execOneTime" is set to True, then only the methods in the webroot are enumerated.

If "reportDavOnly" is set to True, this plugin will only report the enabled method list if DAV methods have been found.

The plugin will try to use the OPTIONS method to enumerate all available methods, if that fails, a manual enumeration is done, when doing a manual enumeration.

execOneTime

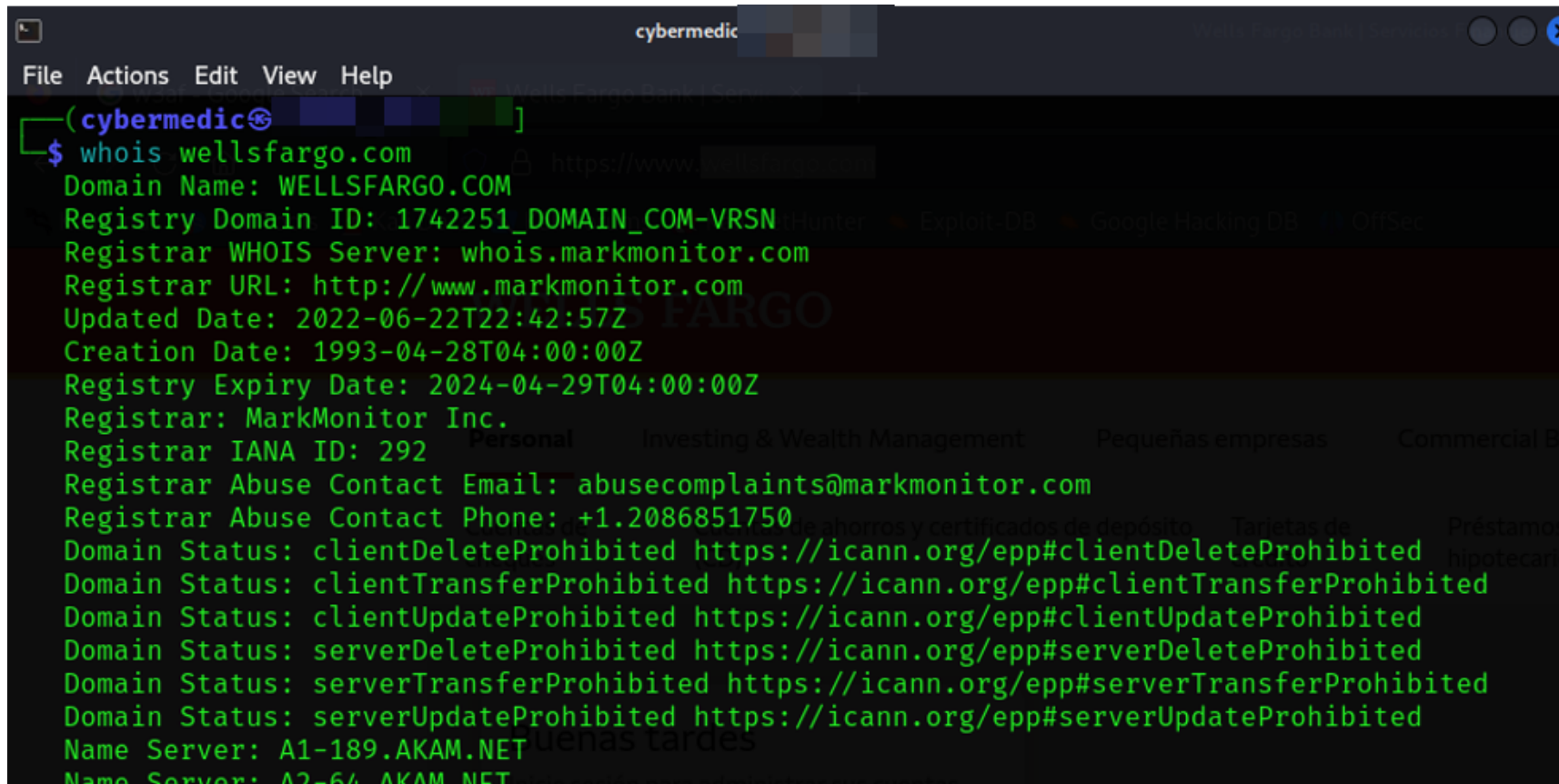
reportDavOnly

Save configuration Revert to previous values

OSINT

# WHOIS

- querying and retrieving information about domain names, IP addresses, and network entities. It provides valuable information about the ownership, registration, and contact details of domain names and IP addresses.
- Does not touch the target itself. This is considered open source intelligence



```
cybermedic
File Actions Edit View Help
(cybermedic)
$ whois wells Fargo.com
Domain Name: WELLSFARGO.COM
Registry Domain ID: 1742251_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-06-22T22:42:57Z
Creation Date: 1993-04-28T04:00:00Z
Registry Expiry Date: 2024-04-29T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: A1-189.AKAM.NET
Name Server: A2-64.AKAM.NET
```

Updated Date: 2022-06-22T22:18:28+0000

Creation Date: 1993-04-28T07:00:00+0000

Registrar Registration Expiration Date: 2024-04-29T00:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750

Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)

Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)

Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)

Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)

Registry Registrant ID:

Registrant Name: Domain Administrator

Registrant Organization: Wells Fargo & Company

Registrant Street: 420 Montgomery St,

Registrant City: San Francisco

Registrant State/Province: CA

Registrant Postal Code: 94104

Registrant Country: US

Registrant Phone: +1.4158083158

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: hostmaster@wellsfargo.com

Registry Admin ID:

Admin Name: Domain Administrator

Admin Organization: Wells Fargo & Company

Admin Street: 420 Montgomery St,

Admin City: San Francisco

Admin State/Province: CA

Admin Postal Code: 94104

Admin Country: US

Admin Phone: +1.4158083158

Pequeñas empresas

Commercial Ba

Cuentas de

Cuentas de ahorros y certificados de depósito

Tarjetas de

Préstamos

crédito

hipotecario

\$200 de bo  
recompens

Cuota anual: \$0. Se aplicar

Guarde el usuario

Inicie sesión

Inscríbese

Más información

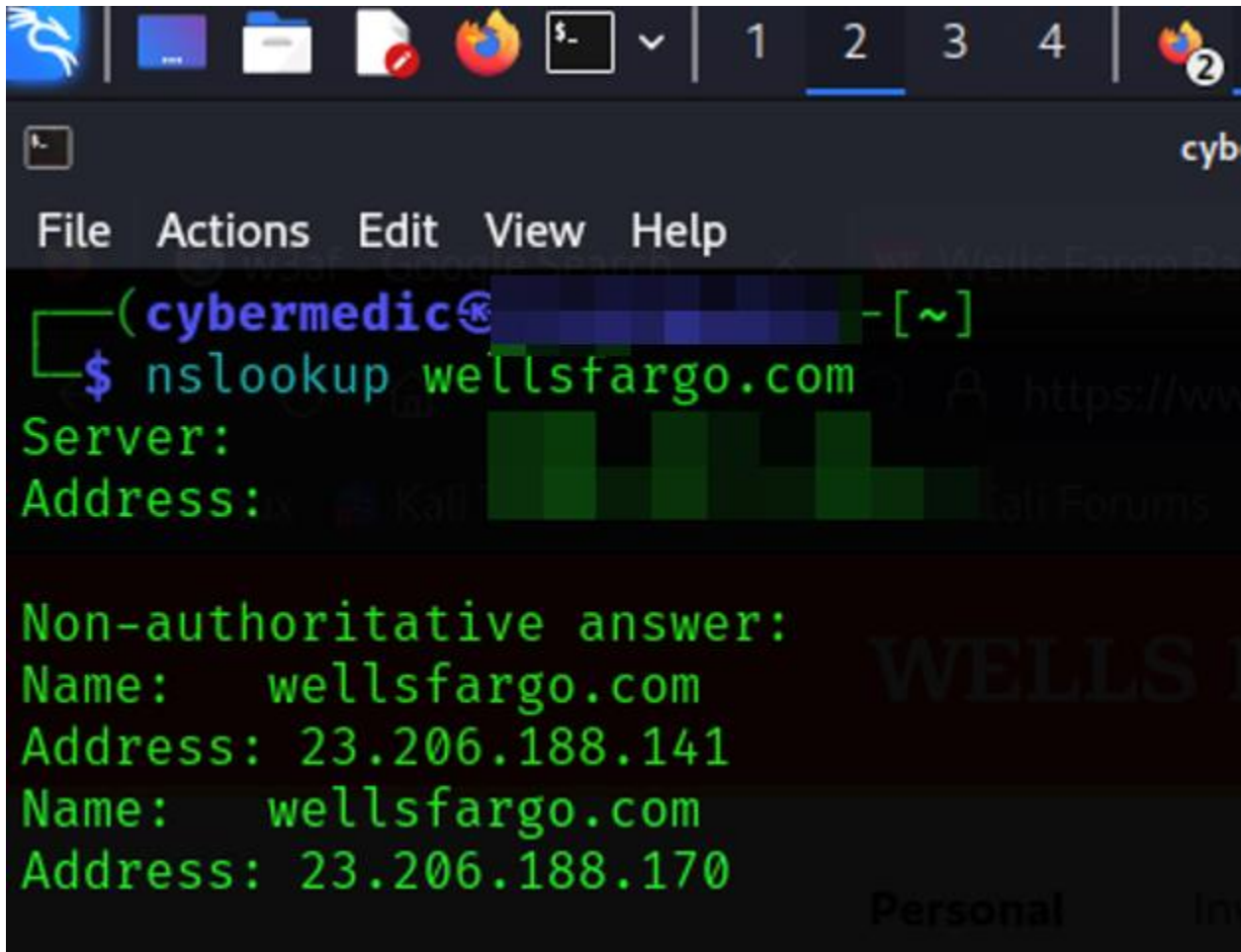
¿Olvidó su usuario o contraseña?

Centro de seguridad

Políticas y asuntos legales

# Nslookup

- used to query Domain Name System (DNS) servers to obtain domain name or IP address information
- is a versatile tool used for various purposes, including diagnosing DNS-related issues, looking up DNS records, and resolving domain names to IP addresses.

A screenshot of a terminal window with a dark background and green text. The terminal shows the execution of the 'nslookup wellsfargo.com' command. The output displays the server and address used for the query, followed by a 'Non-authoritative answer:' section listing two IP addresses for the domain: 23.206.188.141 and 23.206.188.170. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The top of the window shows a taskbar with various application icons and window numbers.

```
(cybermedic@ [redacted] ~)
└─$ nslookup wellsfargo.com
Server: [redacted]
Address: [redacted]

Non-authoritative answer:
Name:   wellsfargo.com
Address: 23.206.188.141
Name:   wellsfargo.com
Address: 23.206.188.170
```

Does not touch target itself. Uses DNS servers to gather info

This is also considered Open source intelligence







- # Shodan
- a search engine and online service that is focused on collecting and indexing information about internet-connected devices and systems.
  - IOT devices / security cameras outside of building question!

Shodan Search Engine — Mozilla Firefox

Shodan Search Engine

https://www.shodan.io

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing Search... Login

## Search Engine for the Internet of Everything

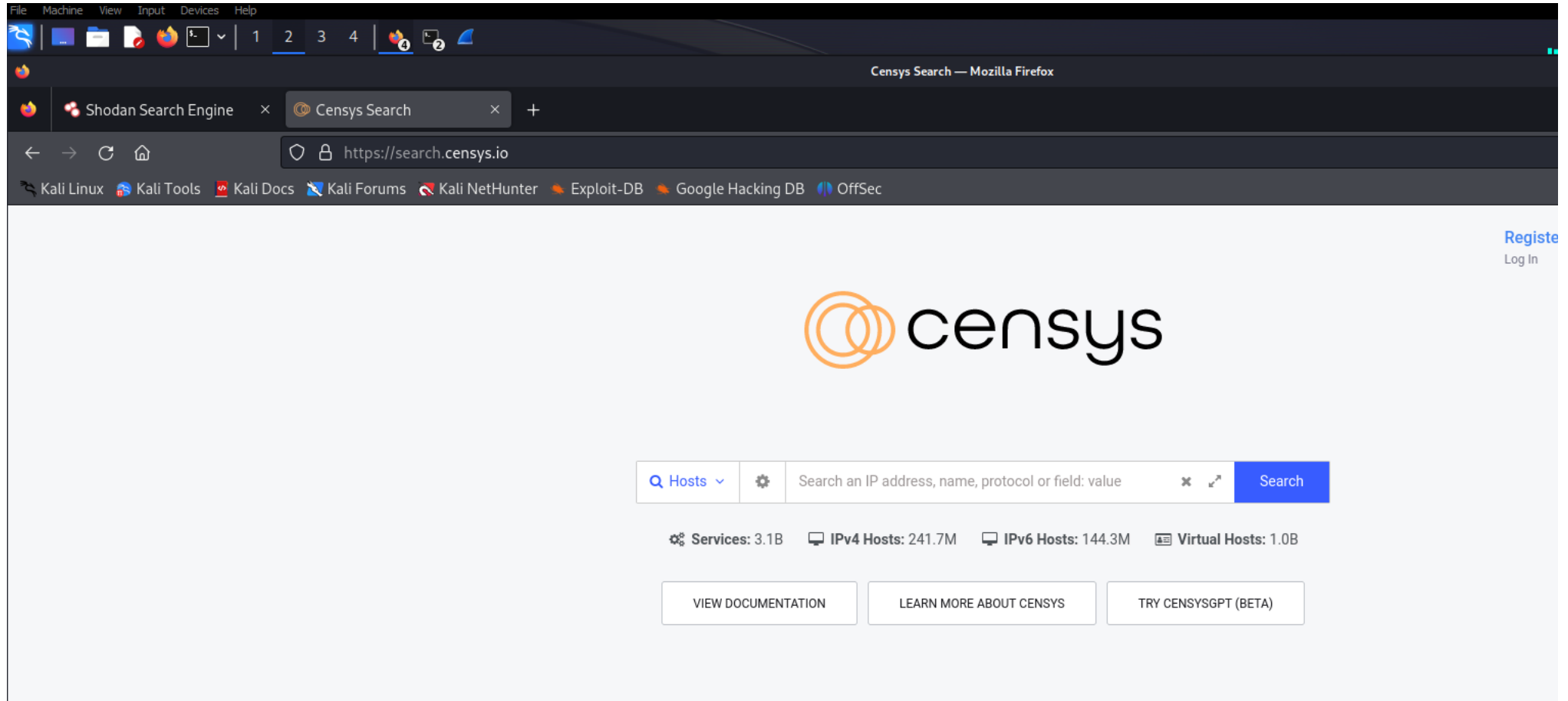
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)

// EXPLORE THE PLATFORM

- Beyond the Web**  
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators, and
- Monitor Network Exposure**  
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to
- Internet Intelligence**  
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology

# Censys.io like shodan, but free



# Maltego

- Maltego is a popular and powerful open-source intelligence and data visualization tool used for information gathering, link analysis, and data mining.
- Maltego is designed to help users understand the relationships between pieces of information and identify patterns or connections.



**MALTEGO**

# MALTEGO

Docs Blog in

## Software and Service Advisories

### Maltego Desktop Client Version 4.5.0 Release

Update your Maltego to Version 4.5.0 and embrace the powerful graph-in and graph-out features: Using graphs as Transform inputs and receiving graphs as outputs! Check out the updates [here](#).

**Feature 1: Context-Based and Multi-Input Transforms**

The graph-in feature allows investigators to run Transforms on multiple interrelated Entities in a graph-like structure as input, providing a comprehensive view of the investigation.

**Feature 2: Simplified Process to Answer High-Level Questions**









The new Transform Protocol makes it easier for investigators to find any common data between Entities and identify their relationship with fewer Transform runs or custom automated Transforms.

**Feature 3: More Meaningful Results with Less Clicks**

The graph-out feature of the V3 Transform Protocol provides a more user-friendly way to interpret complex data sets. Investigators will receive a whole graph instead of running a list of Transforms.

### New Learning Platform

#### TRANSFORM HUB PARTNERS 49/84 shown

 <b>Etherscan</b> by Maltego Technologies Track cryptocurrencies and NFTs based on Ether tokens. <b>New</b>	 <b>Dorking Transforms</b> by Maltego Technologies Advanced search techniques using the Google search engine. <b>New</b>	 <b>RegEx</b> Maltego Regex Tran... by Maltego Technologies Extract matching objects from web pages using "Regular Expressions" ... <b>New</b>	 <b>OpenSanctions</b> by Maltego Technologies Identify sanctions targets, politicians and persons of interest. <b>Featured</b> <b>Data Subscription</b>
 <b>Abuse.ch URLhaus</b> by Maltego Technologies Identify malicious URLs and explore underlying malware activity	 <b>AbuseIPDB</b> by Maltego Technologies Find and report abusive IP addresses.	 <b>AlienVault OTX</b> by Maltego Technologies Transforms for the world's first truly open threat intelligence community.	 <b>alphaMountain</b> by alphaMountain.ai Host/IP/URL risk and categorization <b>Featured</b> <b>Data Subscription</b>

# Web Application tools

# OWASP ZAP

- OWASP ZAP, or the OWASP Zed Attack Proxy, is an open-source security testing tool developed by the OWASP (Open Web Application Security Project) community. ZAP is designed for finding security vulnerabilities in web applications during development and testing phases





Untitled Session - OWASP ZAP 2.13.0

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites + Quick Start Request Response Requester +


Contexts

- Default Context
- Sites


# Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.


If you are new to ZAP then it is best to start with one of the options below.



Automated Scan



Manual Explore



Learn More

News

What should the ZAP developers focus on? [Learn More](#) ✕

History Search Alerts Output +

Filter: OFF Export

ID	Sou...	Req. Timestamp	Met...	URL	C...	Reason	...	Size Resp. ...	Highest ...	N...	Tags
----	--------	----------------	--------	-----	------	--------	-----	----------------	-------------	------	------

Alerts 0 0 0 0 Main Proxy: localhost:8080 Current Scans 0 4 0 0 0 0 0 0 0 0

# Burp Suite

- Burp Suite is a widely used web vulnerability scanner and security testing tool developed by PortSwigger. It is designed for security professionals, ethical hackers, and penetration testers to assess and identify security vulnerabilities in web applications. Burp Suite provides a comprehensive set of features for various aspects of web application security testing



Browser window titled "Login Test" with address bar showing "vbsca.ca/".  
Kali Linux, Kali Tools, Kali Docs

### Login Test

Username:   
Password:

Burp Suite Community Edition v2023.9.3 - Temp

Menu: Burp Project Intruder Repeater View Help  
Sub-menu: Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Lc

Intercept HTTP history WebSockets history Proxy settings

Request to http://vbsca.ca:80 [163.182.194.25]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /login/login_results.asp HTTP/1.1
2 Host: vbsca.ca
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 56
9 Origin: http://vbsca.ca
10 Connection: close
11 Referer: http://vbsca.ca/login/login.asp
12 Cookie: ASPSESSIONIDQCTRQST=HNOHKPHAGMOPNFMMBLEGNDPL
13 Upgrade-Insecure-Requests: 1
14
15 txtUsername=cybermedic&txtPassword=super+secret+password
```

# Gobuster

- Gobuster is an open-source tool used for directory and file brute-forcing on web servers. It's primarily used by penetration testers and security professionals to discover hidden or unlinked resources on a web server or to identify potential security vulnerabilities related to directory and file naming

```
(cybermedic@)~]
$ gobuster dir -u http://10.10.123.176 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.123.176
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
```

```
└─$ gobuster dir -u http://10.10.124.7 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

---

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

---

[+] Url: http://10.10.124.7  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
[+] Negative Status codes: 404  
[+] User Agent: I gobuster/3.6  
[+] Timeout: 10s

---

Starting gobuster in directory enumeration mode

---

/images (Status: 301) [Size: 234] [→ http://10.10.124.7/images/]  
/blog (Status: 301) [Size: 232] [→ http://10.10.124.7/blog/]  
/rss (Status: 301) [Size: 0] [→ http://10.10.124.7/feed/]  
/sitemap (Status: 200) [Size: 0]  
/login (Status: 302) [Size: 0] [→ http://10.10.124.7/wp-login.php]  
Progress: 63 / 220561 (0.03%)█

# Social engineering tool

- Phishings – email
- Vishing – voice
- Smishing – sms message

# Social engineering toolkit SET

- The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them

**The Social-Engineer Toolkit is a product of TrustedSec.**

NMAP

**Visit: <https://www.trustedsec.com>**

It's easy to update using the PenTesters Framework! (PTF)

Visit <https://github.com/trustedsec/ptf> to update all your tools!

HTTP-HTTPS

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) Third Party Modules
  
- 99) Return back to the main menu.

set> █



# BeEF

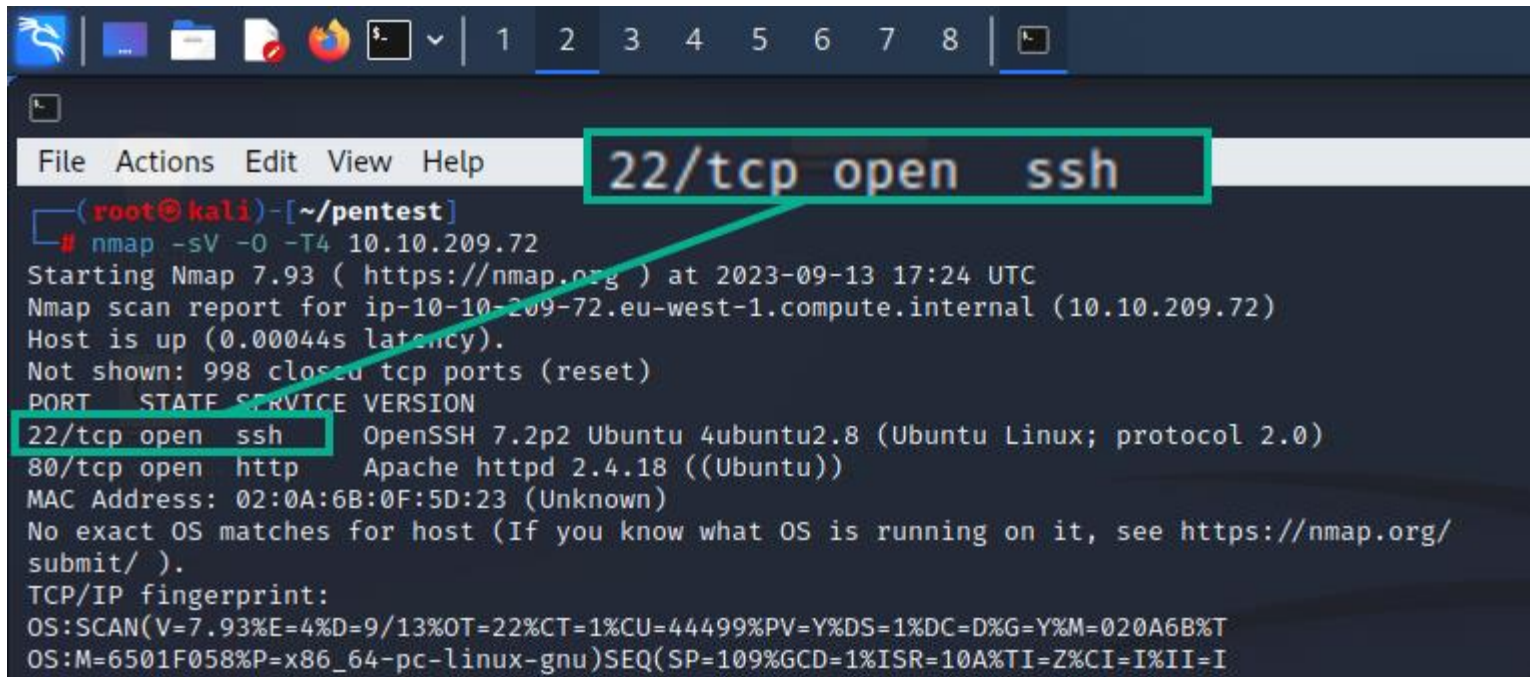
- "Beef" refers to the Browser Exploitation Framework, which is an open-source penetration testing tool used by security professionals to test the security of web applications



# Remote access tools

# SSH Secure Shell

- SSH, which stands for Secure Shell, is a cryptographic network protocol used for secure communication over an unsecured network. It is commonly used for remote administration of network devices and secure file transfers.



```
File Actions Edit View Help 22/tcp open ssh
(root@kali)-[~/pentest]
# nmap -sV -O -T4 10.10.209.72
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-13 17:24 UTC
Nmap scan report for ip-10-10-209-72.eu-west-1.compute.internal (10.10.209.72)
Host is up (0.00044s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 02:0A:6B:0F:5D:23 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/13%OT=22%CT=1%CU=44499%PV=Y%DS=1%DC=D%G=Y%M=020A6B%T
OS:M=6501F058%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=I%II=I
```

```
(root@kali)-[~/Documents]
└─# ssh jessie@10.10.209.72 -i id_rsa
```

Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

- \* Documentation: <https://help.ubuntu.com>
- \* Management: <https://landscape.canonical.com>
- \* Support: <https://ubuntu.com/advantage>

8 packages can be updated.  
8 updates are security updates.

```
jessie@CorpOne:~$ pwd
/home/jessie
```

```
jessie@CorpOne:~$ ls
```

Desktop

Downloads

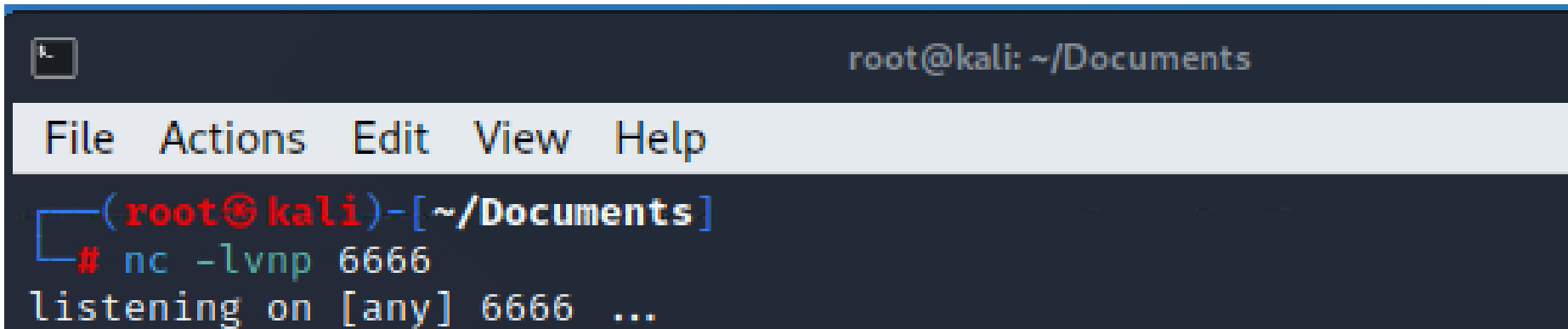
Music

Public

Videos

# Netcat

- Netcat, often abbreviated as "nc," is a versatile networking utility that is sometimes referred to as the "Swiss Army knife" of networking tools. It can be used for a wide range of network-related tasks, including port scanning, banner grabbing, transferring files, creating reverse shells, and much more



```
root@kali: ~/Documents
File Actions Edit View Help
(root@kali)-[~/Documents]
# nc -lvnp 6666
listening on [any] 6666 ...
```



root@kali: ~/Documents

File Actions Edit View Help

(root@kali)-[~/Documents]

# nc -lvp 6666

listening on [any] 6666 ...

connect to [10.10.29.64] from (UNKNOWN) [10.10.209.72] 58894

POST / HTTP/1.1

User-Agent: Wget/1.17.1 (linux-gnu)

Accept: \*/\*

Accept-Encoding: identity

Host: 10.10.29.64:6666

Connection: Keep-Alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 33

b1b[REDACTED]1daaf[REDACTED]3d



MISC

(important tools to  
know)

# searchsploit

- a command-line search tool for the Exploit Database, a comprehensive collection of exploits, vulnerabilities, and related tools

```
(cybermedic@kali) [~/Downloads]
└─$ searchsploit
Usage: searchsploit [options] term1 [term2] ... [termN]

=====
Examples
=====

searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | jq
searchsploit --cve 2021-44228

For more examples, see the manual: https://www.exploit-db.com/searchsploit
```



```
(cybermedic@Divergence)-[~/Downloads]
```

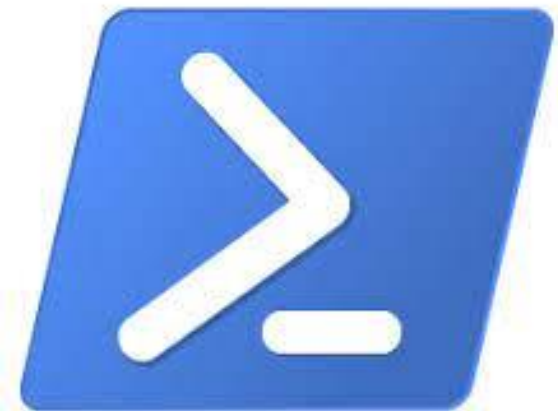
```
$ searchsploit medic
```

Exploit Title	Path
Art <b>medic</b> CMS 3.4 - 'index.php' Local File Inclusion	php/webapps/4538.txt
Art <b>medic</b> Event - 'index.php' Remote File Inclusion	php/webapps/27767.txt
Art <b>medic</b> Links 5.0 - 'index.php' Remote File Inclusion	php/webapps/28594.txt
Art <b>medic</b> NewsLetter 4.1 - 'Log.php' Remote Script Execution	php/webapps/27900.txt
Art <b>medic</b> Webdesign Kleinanzeigen Script - Remote File Inclusion	php/webapps/24289.c
art <b>medic</b> webdesign weblog - Multiple Local File Inclusions	php/webapps/31201.txt
art <b>medic</b> weblog 1.0 - Multiple Local File Inclusions	php/webapps/5116.txt
Horos 2.1.0 DICOM <b>Medical</b> Image Viewer - Denial of Service	osx/dos/40929.py
<b>Medical</b> Center Portal Management System 1.0 - 'id' SQL Injection	php/webapps/49274.txt
<b>Medical</b> Center Portal Management System 1.0 - 'login' SQL Injection	php/webapps/49138.txt
<b>Medical</b> Center Portal Management System 1.0 - Multiple Stored XSS	php/webapps/49236.txt
<b>Medical</b> Clinic Website Script - SQL Injection	php/webapps/41091.txt
<b>Medicine</b> Tracker System v1.0 - Sql Injection	php/webapps/51338.txt
<b>Mediconta</b> 3.7.27 - 'server <b>medic</b> ontservice' Unquoted Service Path	windows/local/51064.txt
OpenEMR Electronic <b>Medical</b> Record Software 3.2 - Multiple Vulnerabilities	php/webapps/14011.txt
Pharmacy <b>Medical</b> Store and Sale Point 1.0 - 'catid' SQL Injection	php/webapps/48752.txt
Pharmacy/ <b>Medical</b> Store & Sale Point 1.0 - 'email' SQL Injection	php/webapps/49132.py
Smiths <b>Medical</b> Medfusion 4000 - 'DHCP' Denial of Service	hardware/dos/43776.py
WordPress Theme <b>Medic</b> v1.0.0 - Weak Password Recovery Mechanism for Forgotten Password	php/webapps/51531.py

```
Shellcodes: No Results
```

# powershell

- It is primarily used for system administration, configuration management, and task automation in Windows environments.



Windows PowerShell



Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

PS C:\> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=187ms TTL=113

Reply from 8.8.8.8: bytes=32 time=241ms TTL=113

Reply from 8.8.8.8: bytes=32 time=247ms TTL=113

Reply from 8.8.8.8: bytes=32 time=61ms TTL=113

# metasploit

- penetration testing and exploitation framework. Metasploit is designed for security professionals, ethical hackers, and penetration testers to test the security of systems and networks, identify vulnerabilities, and validate security controls.



Metasploit



# WireShark

- open-source network protocol analyzer and packet capture tool. It is used for network troubleshooting, analysis, and security auditing. Wireshark allows users to capture and inspect data traveling over a network, providing detailed information about network packets and their contents



tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsc\_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio\_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

    [Request In: 348]

    [Time: 0.034338000 seconds]

    Transaction ID: 0x2188

    > Flags: 0x8180 Standard query response, No error

    Questions: 1

    Answer RRs: 4

    Authority RRs: 9

    Additional RRs: 9

▼ Queries

    > cdn-0.nflximg.com: type A, class IN

    > Answers

    > Authoritative nameservers

```

0020  00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01  ...5.... ?!....
0030  00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c  .....c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00  ximg.com .....
0050  05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73  .....). ".images
0060  07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67  .netflix .com.edg
0070  65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00  esuite.n et./...

```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default