



# Lab: Social Engineering Attacks

Mariano Ceccato  
mariano.ceccato@univr.it



# Kali Linux – offensive security

- Linux distribution maintained and funded by Offensive Security
- Designed for digital forensics and penetration testing
- Many security auditing tools are pre-installed and configured
  - exploiting a victim network or application
  - performing network discovery/scanning
  - scanning a target IP address
  - penetration testing
  - password crack
- <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

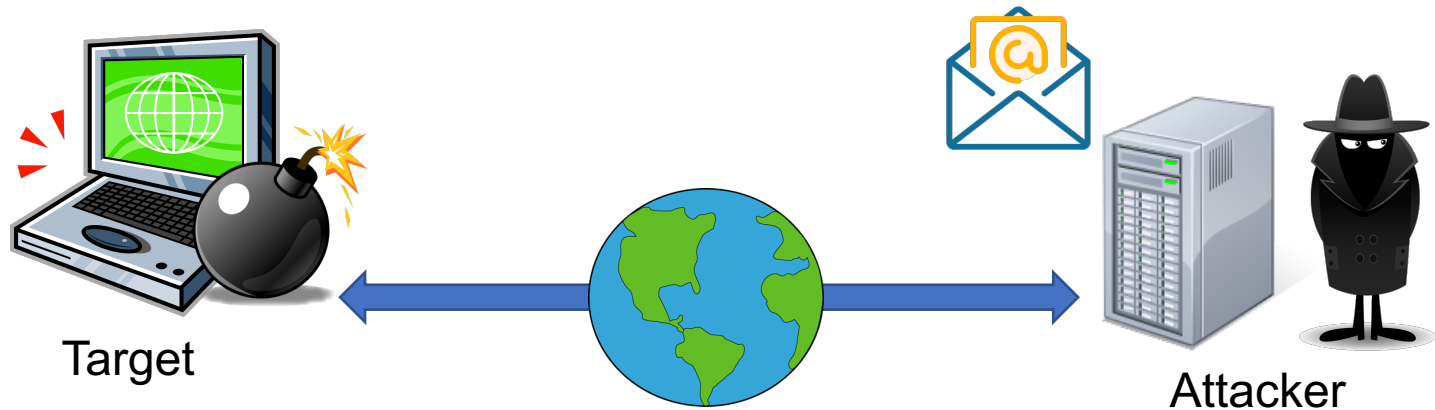


# **Lab 1:**

## **Social Engineering attack to gain remote target control**



# Remote target control via Social Engineering attack





# SET: Social Engineering Toolkit

- Open-source penetration testing framework developed by David Kennedy (TrustedSec)
  - Teaching security
  - Corporate security assessment
  - Includes custom attack vectors to make a believable attack very fast
- Only for testing purposes
- Can only be used where strict consent has been given



# Manual installation

- Directly from sources
- Requirements:
  - Git
  - Python 3
  - Pip

```
git clone https://github.com/trustedsec/social-engineer-toolkit/  
cd social-engineer-toolkit  
pip3 install -r requirements.txt  
python3 setup.py
```



# Sendmail

```
sudo apt-get update  
sudo apt-get install sendmail  
sudo vim /etc/setoolkit/set_config.py
```



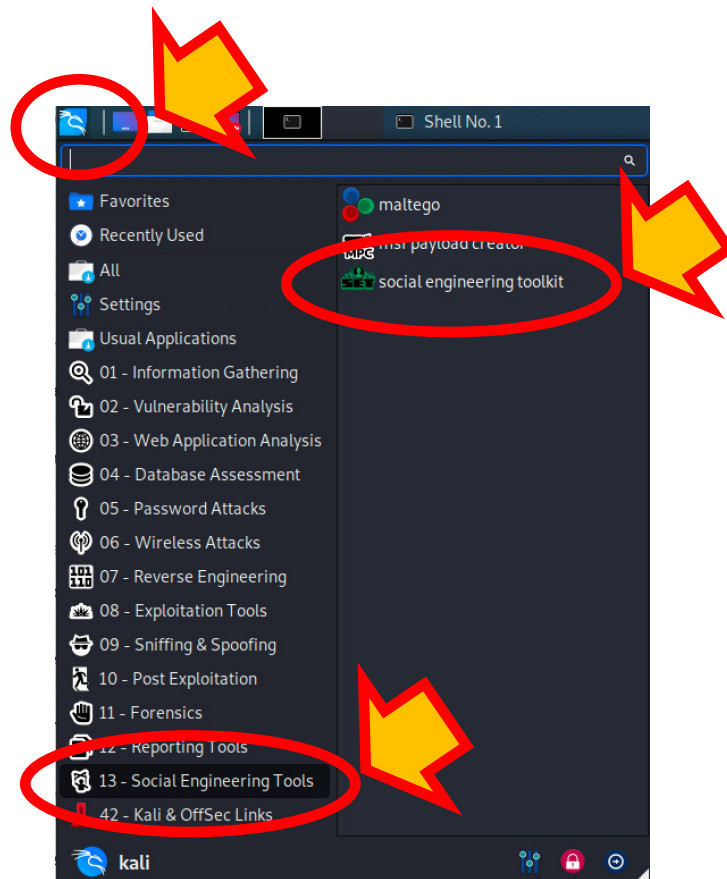
```
AUTO_DETECT=False  
SENDMAIL=True  
EMAIL_PROVIDER="GMAIL"
```



# Starting SET

- From the command line

```
sudo setoolkit
```







# Confirming license & adoption

The Social-Engineer Toolkit is designed purely **for good** and not evil. If you are planning on using this tool for malicious purposes that are not **authorized by the company** you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for **lawful purposes only**.



# Initial dashboard



```
[---]ols - The Social-Engineer Toolkit (SET) tell rep [---]ts
[---]a-sett Created by: David Kennedy (ReL1K)BIA graph [---]river
nvidia-settings-lega Version: 8.0.3 for configuring the NVIDIA gra
nvidia-settings-tes Codename: 'Maverick'figuring the NVIDIA graphi
[---]a-sett Follow us on Twitter: @TrustedSecg the M [---]graphi
[---]a-sett Follow me on Twitter: @HackingDave the M [---]graphi
[---]a-sett Homepage: https://www.trustedsec.com the M [---]graphi
nvidia- Welcome to the Social-Engineer Toolkit (SET).non-free NVID
winetricks The one stop shop for all of your SE needs.ems in Wine
lvm-8 Modular compiler and toolchain technologies
The Social-Engineer Toolkit is a product of TrustedSec.libraries
lvm-8-runtime Modular compiler and toolchain technologies, IR i
python-dns Visit: https://www.trustedsec.com
root@kali:~#
root@kali:~# cd /set/
root@kali:~/set# cd reports/
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
```



# Spear-Phishing Attack Vectors

```
[---] xconf The Social-Engineer Toolkit (SET) for no[---] NVIDIA dr
[---] ticks - Created by: David Kennedy (ReL1K) problems[---] ine
llvm-8 - Modular comp Version: 8.0.3 in technologies
llvm-8-dev - Modula Codename: 'Maverick' in technologies, libraries and
[---] 8-runin Follow us on Twitter: @TrustedSec technol[---], IR interp
[---] 8-dnspr Follow me on Twitter: @HackingDave [---]
[---] 8als Homepage: https://www.trustedsec.com [---]
root@kali:~# Welcome to the Social-Engineer Toolkit (SET).
root@kali:~# The one stop shop for all of your SE needs.
root@kali:~# cd /set/
root@kali:~/set# The Social-Engineer Toolkit is a product of TrustedSec.
root@kali:~/set# set/reportsp ls
2021-02-16 Visit: https://www.trustedsec.com
root@kali:~/set# set/reportsp ls -l
-rw-r--r-- 1 root root 4096 Feb 16 12:25 19675.xml
root@kali:~/set# set/reportsp vim
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infrared Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
```



# Spear-Phishing Attack Vectors



- Creation of email messages (and sending them) with attached file-format malicious payloads.
- Sender email address can be spoofed
- E.g., sending malicious PDF document which, if the victim opens, it will compromise the system.
- Options:
  1. **Perform a Mass Email Attack**
  2. Create a FileFormat Payload
  3. Create a Social-Engineering Template



# Perform a Mass Email Attack



1. SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2. SET Custom Written Document UNC LM SMB Capture Attack
3. MS15-100 Microsoft Windows Media Center MCL Vulnerability
4. MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5. Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6. Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7. Adobe Flash Player "Button" Remote Code Execution
8. Adobe CoolType SING Table "uniqueName" Overflow
9. Adobe Flash Player "newfunction" Invalid Pointer Use
10. Adobe Collab.collectEmailInfo Buffer Overflow
11. Adobe Collab.getIcon Buffer Overflow
12. Adobe JBIG2Decode Memory Corruption Exploit
13. Adobe PDF Embedded EXE Social Engineering
14. Adobe util.printf() Buffer Overflow
15. Custom EXE to VBA (sent via RAR) (RAR required)
16. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17. **Adobe PDF Embedded EXE Social Engineering (NOJS)**
18. Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19. Apple QuickTime PICT PnSize Buffer Overflow
20. Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21. Adobe Reader u3D Memory Corruption Vulnerability
22. MSCOMCTL ActiveX Buffer Overflow (ms12-027)



# PDF Embedded EXE - Available attacks

Attack	Description
Windows Reverse TCP Shell	Spawn a command shell on victim and send back to attacker
Windows Meterpreter Reverse_TCP	Spawn a meterpreter shell on victim and send back to attacker
Windows Reverse VNC DLL	Spawn a VNC server on victim and send back to attacker
Windows Reverse TCP Shell (x64)	Windows X64 Command Shell, Reverse TCP Inline
<b>Windows Meterpreter Reverse_TCP (X64)</b>	Connect back to the attacker (Windows x64), Meterpreter
Windows Shell Bind_TCP (X64)	Execute payload and create an accepting port on remote system
Windows Meterpreter Reverse HTTPS	Tunnel communication over HTTP using SSL and use Meterpreter



# Meterpreter (Metasploit)



- Extensible console for controlling compromised remote hosts
- It communicates over socket and provides a comprehensive client-side Ruby API.
  - Command history, tab completion, channels, and more.
- In-memory DLL injection stagers and is extended over the network at runtime.



Target



# How Meterpreter works



- The target executes the initial stager (possibly from a Social Engineering attack) and a DLL is load/injected
- The Meterpreter core initializes on the target, establishes a TLS/1.0 link over the socket and sends a GET.
- Metasploit receives this GET and configures the attacker client.







# Meterpreter features



## STEALTHY

- Resides entirely in memory and writes nothing to disk
- No new process created
  - Meterpreter injects itself into the compromised process and can migrate to other running processes easily
- Meterpreter uses encrypted communications
- So, limited forensic evidence and impact on the victim machine

## POWERFUL

- Meterpreter utilizes a channelized communication system

## EXTENSIBLE

- Features can be augmented at runtime and are loaded over the network
- New features can be added to Meterpreter without having to rebuild it.



# Meterpreter commands



Command	Description
help	display commands and description
background	Suspend Meterpreter shell process
cat	Display file content
cd pwd ls / lcd lpwd	Move in the target/attacker file system
clearev	Clear the <i>Application</i> , <i>System</i> , and <i>Security</i> logs on a Windows system
download/upload	Download/upload a file from/to the target to/from the attacker
edit	Open a file in the target
ipconfig	Network interfaces and addresses on the target
migrate	Migrate to another process on the victim.



# Meterpreter commands



Command	Description
execute	Run a command on the target
ps	displays a list of running processes on the target
resource	Run the local Meterpreter script on the target host
search	locating specific files on the target host
shell	Opens standard shell on the target system.
webcam_list	display currently available web cams on the target
webcam_snap	grabs a picture from a connected web cam on the target



# Exercise: Spear-Phishing Attack

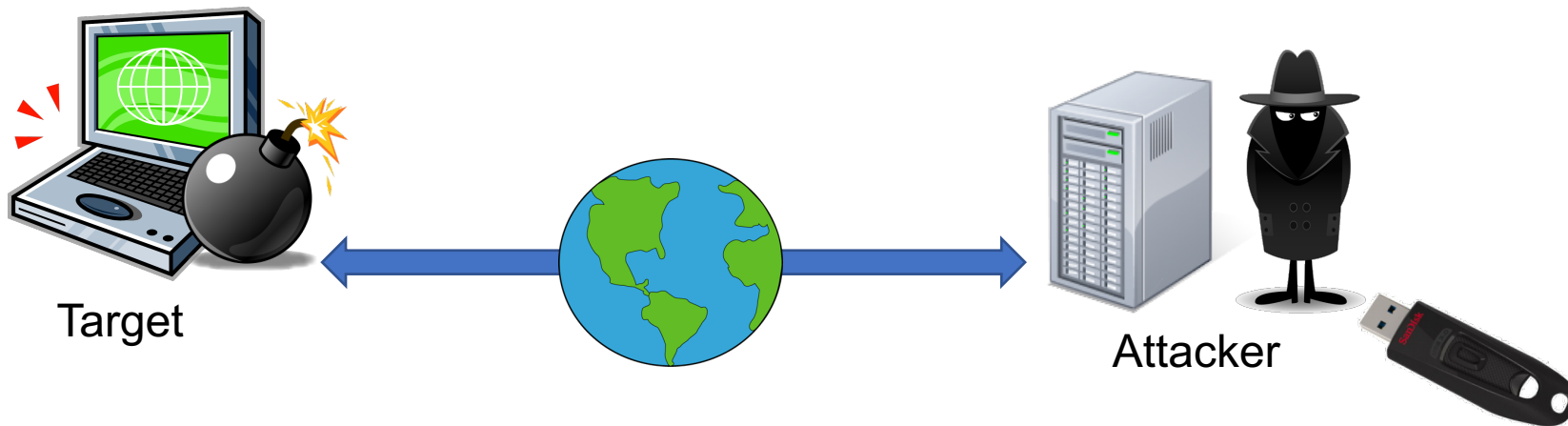
- Use a PDF document that looks realistic to the target (including file name)
- Use a custom email message content, that looks legitimate
- Send the email to an address own by you



# Lab 2: malicious USB stick



# Malicious USB stick





# Infectious Media Generator

```
[---] xconf The Social-Engineer Toolkit (SET) ol for nc [---] e NVIDIA dr
[---] ticks - Created by: David Kennedy (ReL1K) problems [---] ine
llvm-8 - Modular comp Version: 8.0.3 in technologies
llvm-8-dev - Modula Codename: 'Maverick' in technologies, libraries and
[---] s-runbu Follow us on Twitter: @TrustedSec technol [---], IR interp
[---] n-dnspp Follow me on Twitter: @HackingDave [---]
[---] kals Homepage: https://www.trustedsec.com [---]
root@kali: Welcome to the Social-Engineer Toolkit (SET).
root@kali: The one stop shop for all of your SE needs.
root@kali: # cd /etc/
root@kali: The Social-Engineer Toolkit is a product of TrustedSec.
root@kali: # set reportsp ls
2021-02-16 Visit: https://www.trustedsec.com
root@kali: # set update
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools! 9675.x
[---] xconf root root Zero Feb 16 12:35 files
[---] ticks reportsp vim
[---] kals reportsp vim

Select from the menu: 9675.xml files/
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
```



# Available attacks

- File-Format Exploits
  - The USB stick contains a document that executes Meterpreter
- Standard Metasploit Executable
  - Meterpreter is run when the USB stick is connected





# Payloads

1. SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2. SET Custom Written Document UNC LM SMB Capture Attack
3. MS15-100 Microsoft Windows Media Center MCL Vulnerability
4. MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
5. Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
6. Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
7. Adobe Flash Player "Button" Remote Code Execution
8. Adobe CoolType SING Table "uniqueName" Overflow
9. Adobe Flash Player "newfunction" Invalid Pointer Use
10. Adobe Collab.collectEmailInfo Buffer Overflow
11. Adobe Collab.getIcon Buffer Overflow
12. Adobe JBIG2Decode Memory Corruption Exploit
13. Adobe PDF Embedded EXE Social Engineering
14. Adobe util.printf() Buffer Overflow
15. Custom EXE to VBA (sent via RAR) (RAR required)
16. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17. **Adobe PDF Embedded EXE** Social Engineering (NOJS)
18. Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19. Apple QuickTime PICT PnSize Buffer Overflow
20. Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21. Adobe Reader u3D Memory Corruption Vulnerability
22. MSCOMCTL ActiveX Buffer Overflow (ms12-027)



# PDF Embedded EXE - Available attacks

Attack	Description
Windows Reverse TCP Shell	Spawn a command shell on victim and send back to attacker
Windows Meterpreter Reverse_TCP	Spawn a meterpreter shell on victim and send back to attacker
Windows Reverse VNC DLL	Spawn a VNC server on victim and send back to attacker
Windows Reverse TCP Shell (x64)	Windows X64 Command Shell, Reverse TCP Inline
<b>Windows Meterpreter Reverse_TCP (X64)</b>	Connect back to the attacker (Windows x64), Meterpreter
Windows Shell Bind_TCP (X64)	Execute payload and create an accepting port on remote system
Windows Meterpreter Reverse HTTPS	Tunnel communication over HTTP using SSL and use Meterpreter



# Exercise: Malicious USB stick

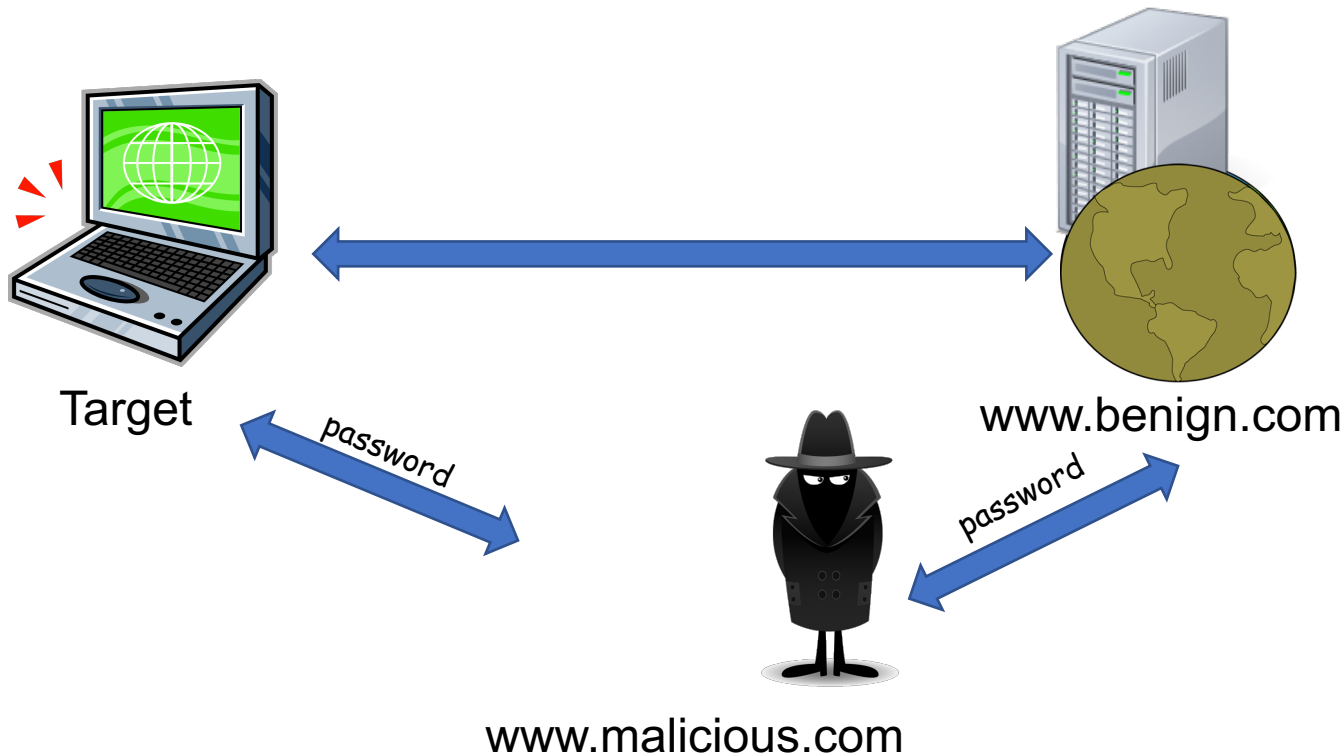
- Write a SUB stick that run Meterpreter when connected



# Lab 3: steal credentials



# Phishing attack to steal credentials





# Website Attack Vectors

```
[---] xconf The Social-Engineer Toolkit (SET) ol for nc [---] e NVIDIA dr
[---] ticks Created by: David Kennedy (ReL1K) problems [---] ine
llvm-8 - Modular comp Version: 8.0.3 in technologies
llvm-8-dev - Modula Codename: 'Maverick' in technologies, libraries and
[---] 8-run Follow us on Twitter: @TrustedSec technol [---], IR interp
[---] 8-dns Follow me on Twitter: @HackingDave [---]
[---] 8-kali Homepage: https://www.trustedsec.com [---]
root@kali: Welcome to the Social-Engineer Toolkit (SET).
root@kali: The one stop shop for all of your SE needs.
root@kali: cd set
root@kali: The Social-Engineer Toolkit is a product of TrustedSec.
root@kali: set/reporter ls
2021-02-1 Visit: https://www.trustedsec.com
root@kali: set
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools! 9675.x
[---] 8-kali root root zero Feb 10 12:35 files
[---] 8-kali set/reporter vim
Select from the menu: 9675.xml files/
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
```



# Website Attack Vectors: Available attacks

Attack	Description
Java Applet Attack	Spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet
Metasploit Browser Exploit	Metasploit browser exploits through an iframe and deliver a Metasploit payload.
<b>Credential Harvester</b>	<b>clone a website that has a username and password field and harvest all the information posted to the website</b>
Tab Nabbing	wait for a user to move to a different tab, then refresh the page to something different.
Web-Jacking Attack	iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link.
Multi-Attack	combination of attacks through the web attack menu. For example Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which one succeeds
HTA Attack	clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser



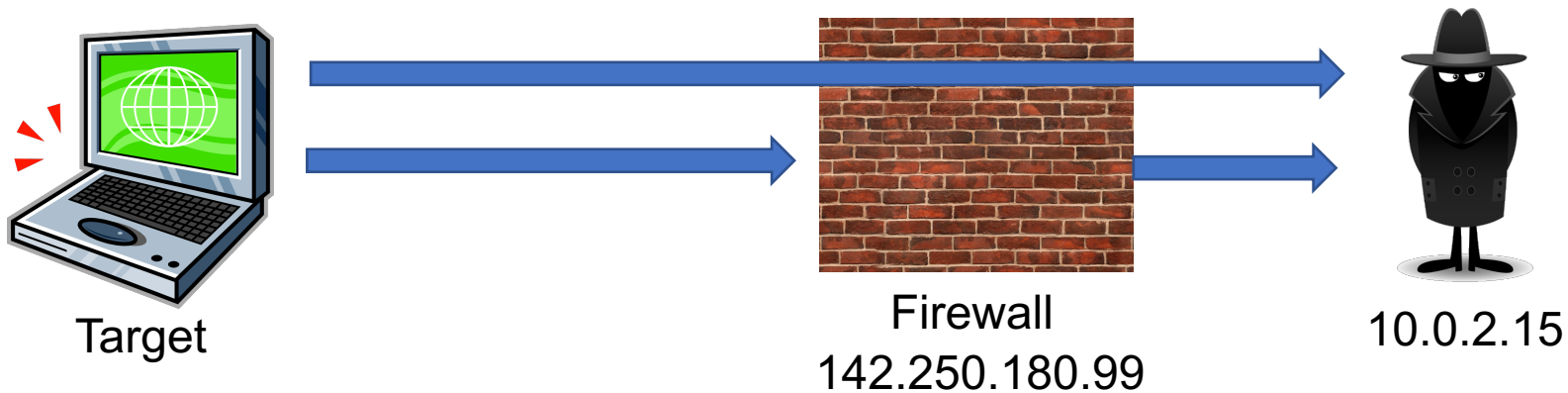
# Credential Harvester

- Several options
  - Web Templates
  - Site cloner
  - Custom Import
- IP address for the POST back in Harvester/Tabnabbing
  - Your (attacker) address
  - In case of NAT (e.g., in virtualbox) or firewall, you should set port forwarding
- The url to clone
- Share a link containing your (attacker address) and make the victim use it
- Collect credentials
  - In the screen log
  - In the attack report `/root/.set/reports`





# Port forwarding

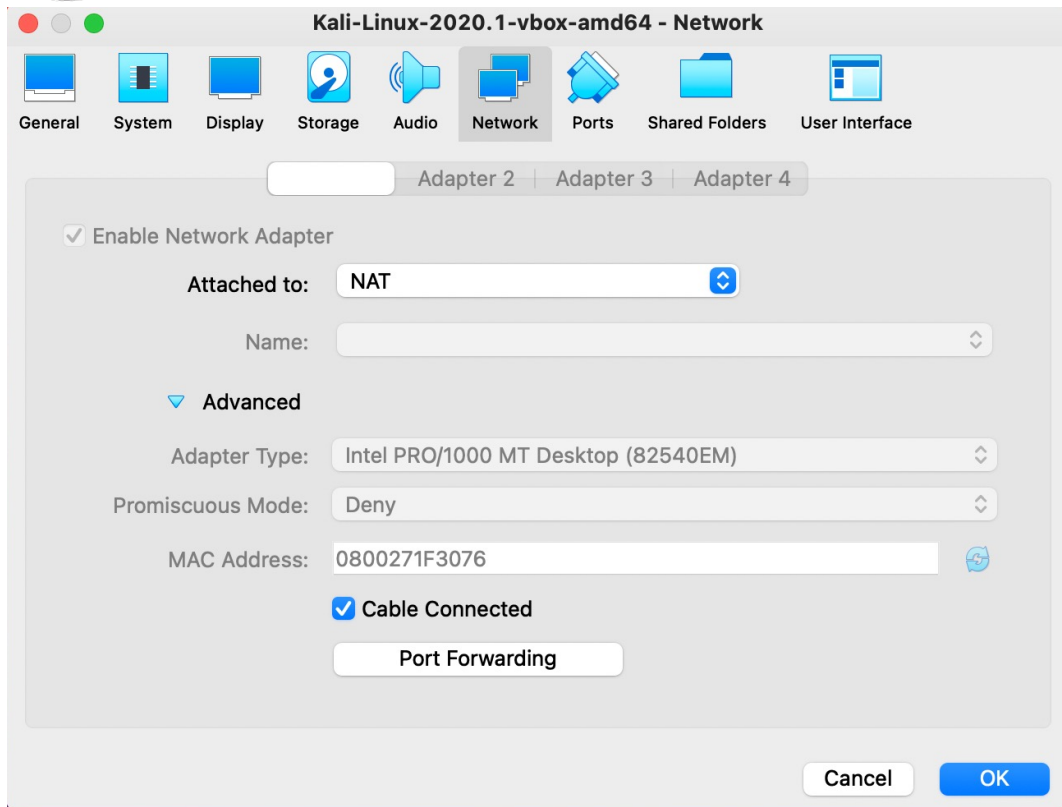


Port forward rule:

`142.250.180.99:80 → 10.0.2.15:80`



# Port forwarding in VirtualBox



- Name: a label for the rule
- Protocol: TCP
- Host IP: address of your computer
- Host port: 80
- Guest IP: address of kali VM
- Guest port: 80



# Exercise

- Clone the UNIVR authentication service
  - <https://giasso.univr.it/opensso/UI/Login>
- Try and steal (your own) password