Penetration Testing

Using Wireshark, John the Ripper and Social Engineering Toolkit

BRONX COMMUNITY COLLEGE
The City University of New York

Muhammad Amer
Rosa Huerta
Mentor: HARRISON CARRANZA

MARIST UNIVERSITY

Marist Computing Conference
November 7, 2025

Agenda

- Introduction: What is Penetration Testing?
- John the Ripper
- Types of Attacks
- Experimental Process
- Wireshark
- Social Engineering Toolkit
- SET Experiment
- How to Prevent Being a Victim
- Conclusion
- References

Introduction: What is Penetration Testing?

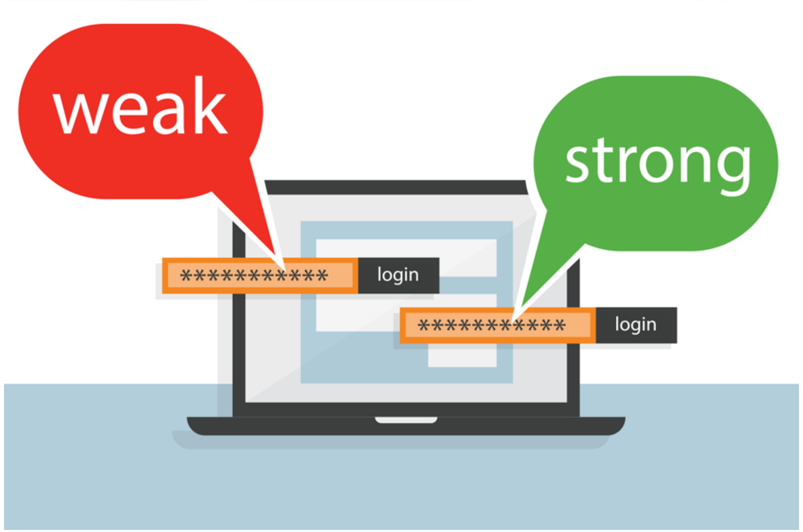
A simulated attack conducted on a computer system to assess its security using use the same techniques as attackers.

John The Ripper

- John The Ripper is a free built-in security tool in Kali Linux.
- It available for all different operating systems.

Uses for John the Ripper

- Crack passwords.
- Test password strength.
- Recover lost passwords.



Types of Attacks

Brute-force attack:

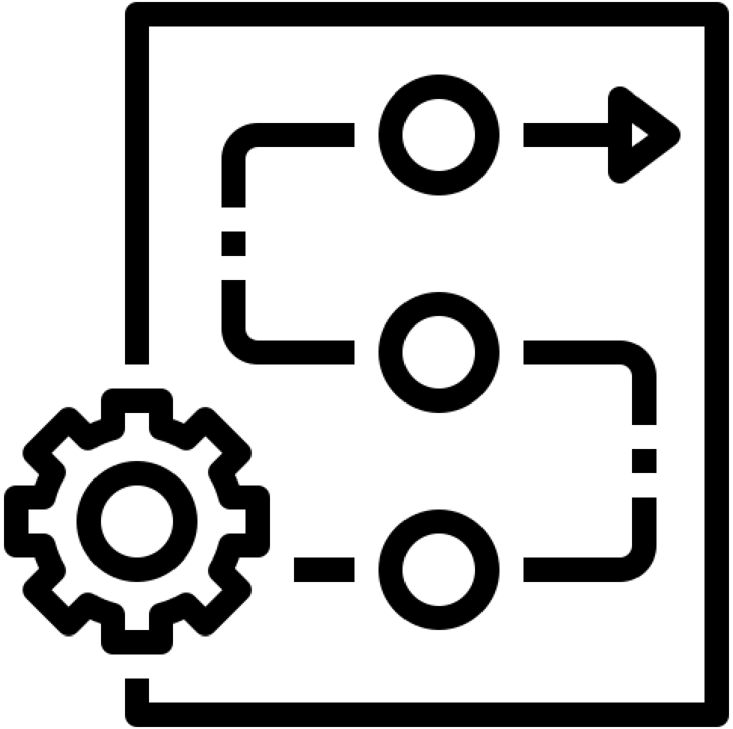
- Attack uses a large number of possible combinations of passwords including numbers.

Dictionary attack:

- Attack that uses all possible words on a list, starting from the most likely.

John the Ripper Procedure

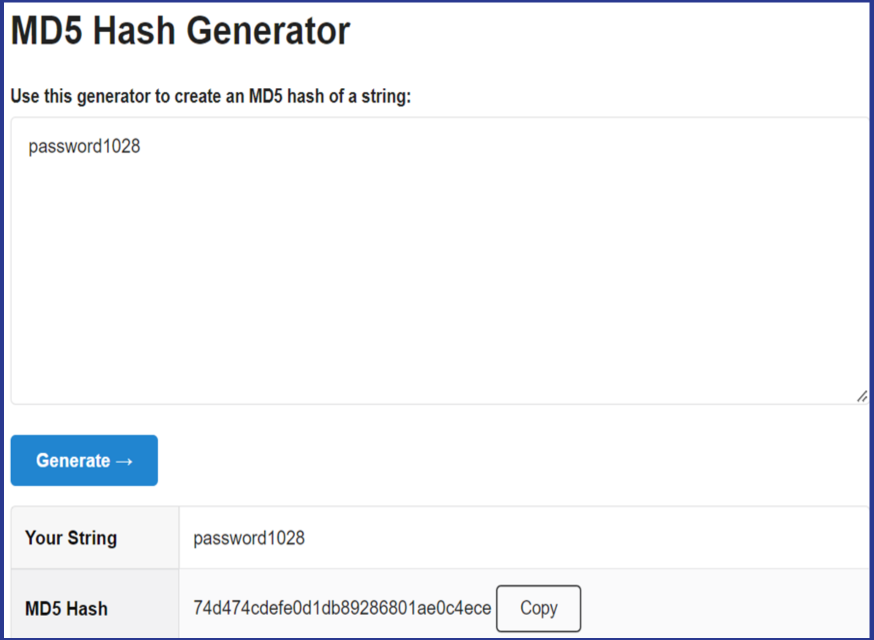
- Samples of a file are taken (words from a dictionary or common passwords).
- Samples are encrypted.
- John the Ripper compares their likeness.



Experimental Process

Create a password and get the hash.

Use Hash-Identifier to identify type of hash and save as a text file.

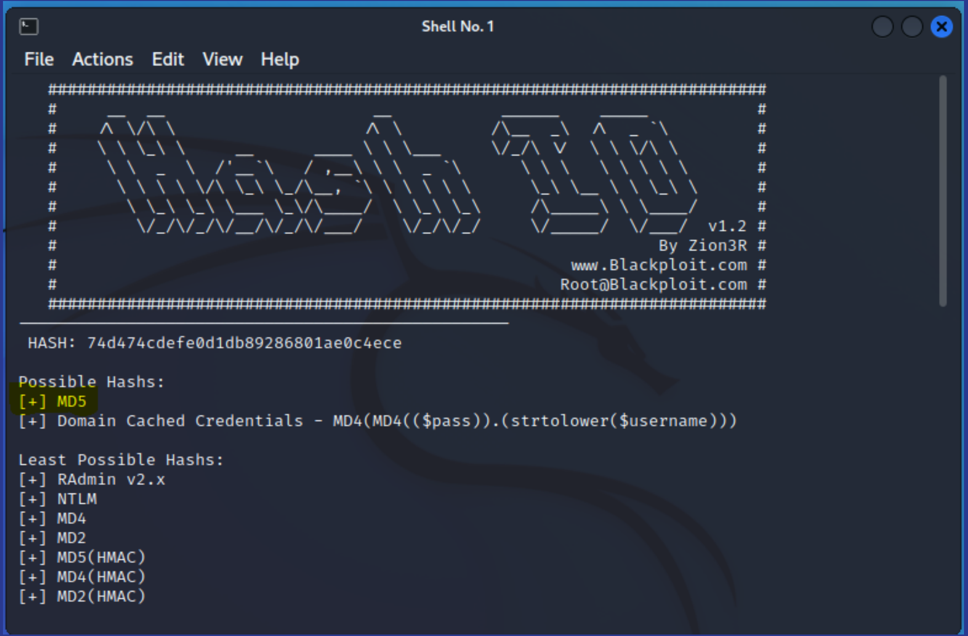


MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

password1028

Your String	password1028
MD5 Hash	74d474cdefe0d1db89286801ae0c4ece Copy



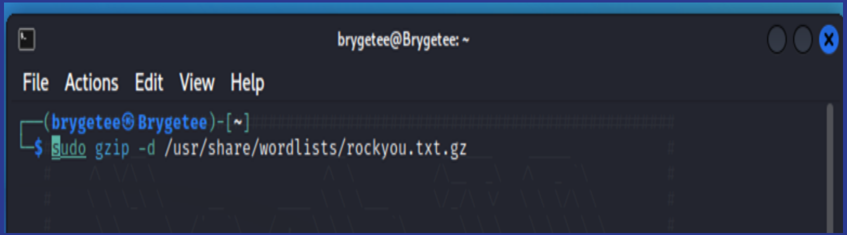
```
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: 74d474cdefe0d1db89286801ae0c4ece

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
```

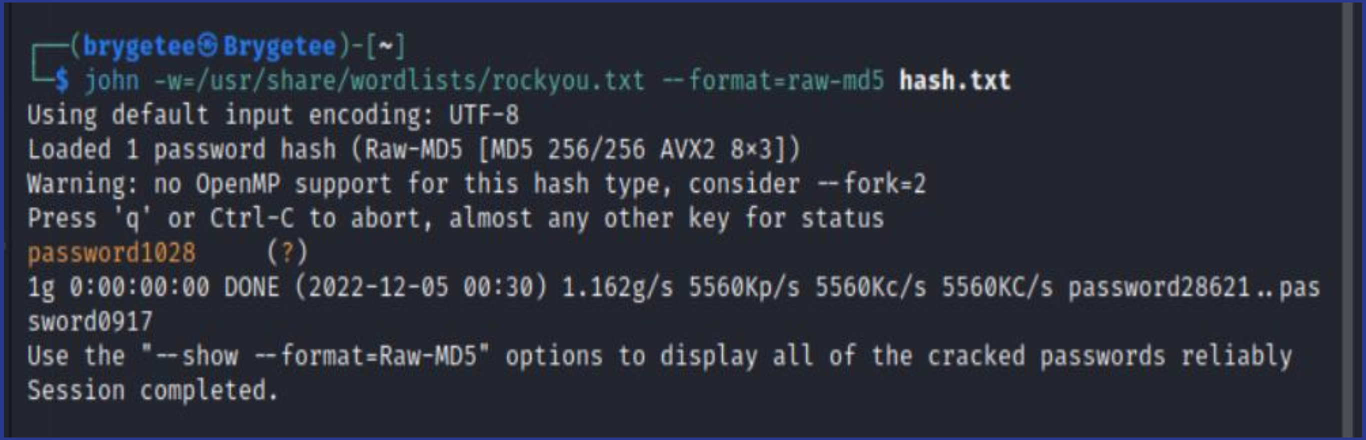
Experimental Process

Unzip text file if necessary



```
┌──(brygetee㉿Brygetee)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

Compare the text file to the wordlist and the password is cracked.



```
┌──(brygetee㉿Brygetee)-[~]
└─$ john -w=/usr/share/wordlists/rockyou.txt --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password1028     (?)
1g 0:00:00:00 DONE (2022-12-05 00:30) 1.162g/s 5560Kp/s 5560Kc/s 5560KC/s password28621..pas
sword0917
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Wireshark

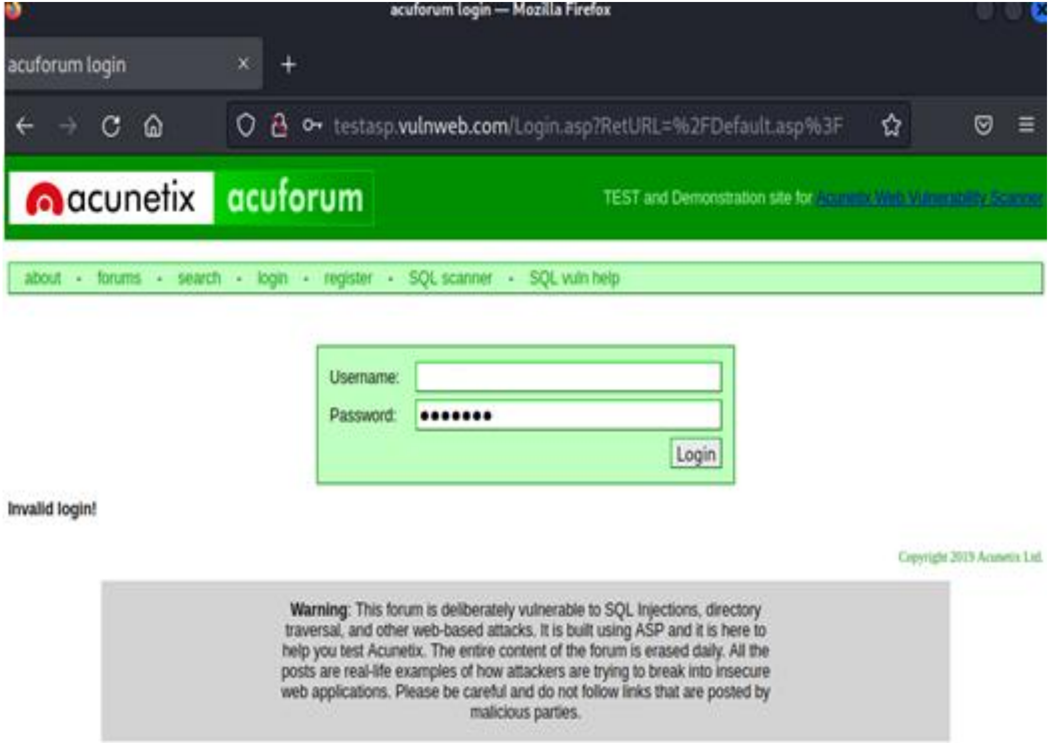
- Wireshark is **a network protocol analyzer**, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

- Packet is the name given to a discrete unit of data in a typical Ethernet network.

Uses for Wireshark

- Examining network traffic for security threats
- Identifying networks
- Managing network traffic and analyzing networks
- Allow the IT teams to have the ability to detect intrusion attempts, security issues, network misuse, packet loss, and network congestion
- Wireshark is capable of not only capturing passwords, but virtually any kind of information that may pass through the network such as usernames, email addresses, personal information, pictures, and videos.

How does it work ?


acuforum login — Mozilla Firefox
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
acunetix
acuforum
about · forums · search · login · register · SQL scanner · SQL vuln help
Login

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Username:

Password: ●●●●●●●

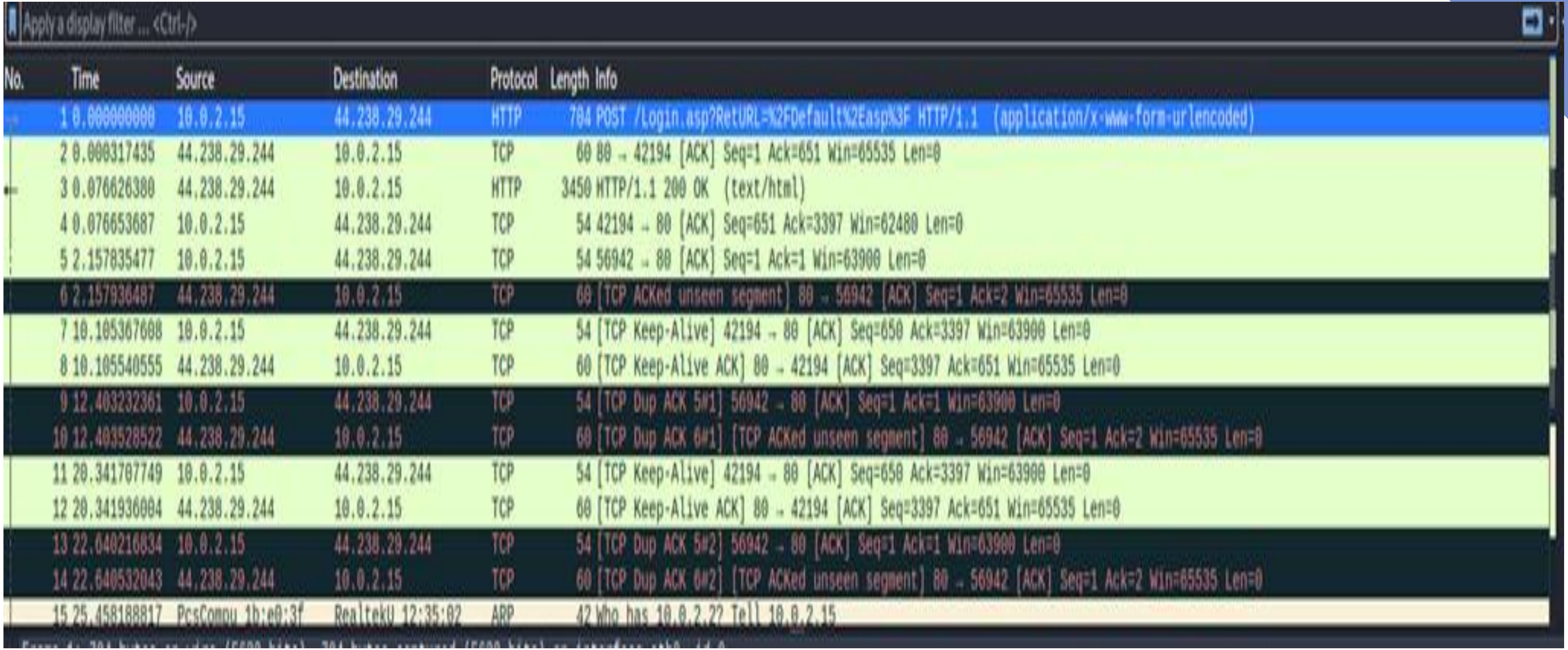
Invalid login!

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

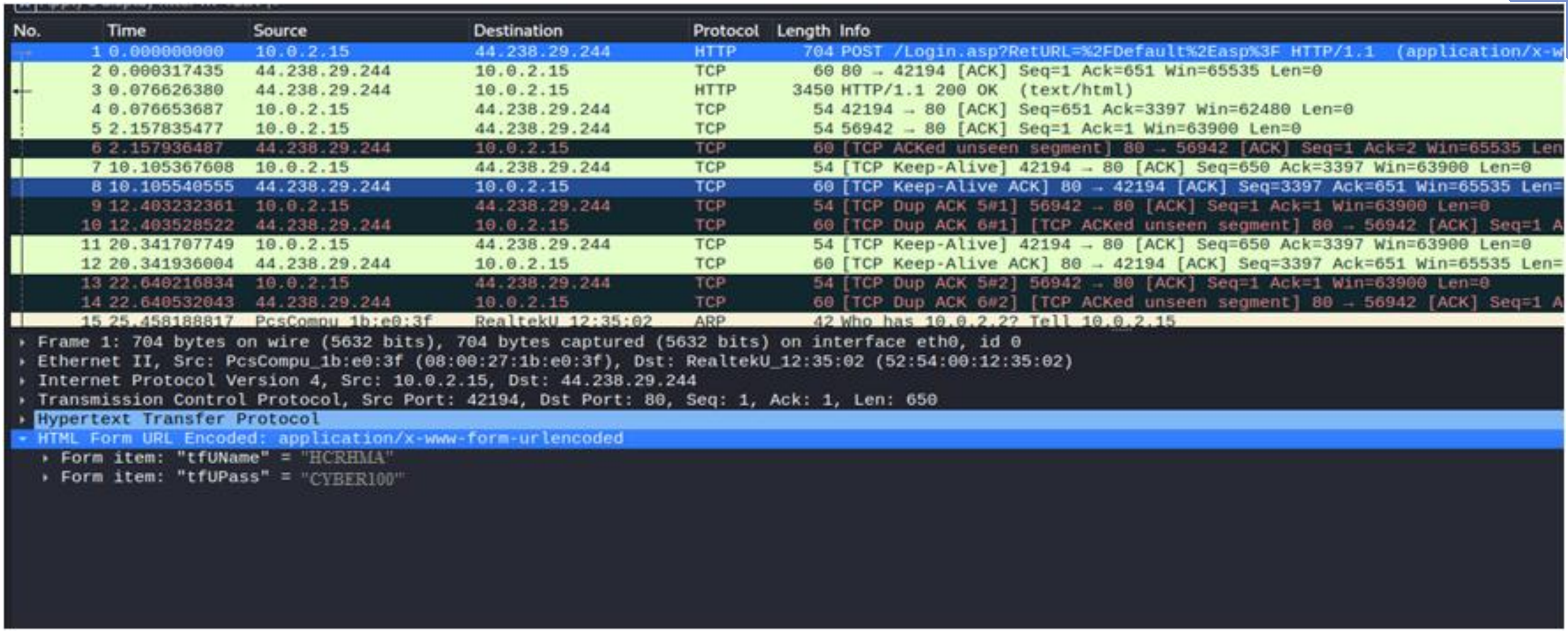
- select network that we want to sniff
- sniff data packets as they are transmitted over HTTP protocol.

This figure shows the packet that has the information that we need, so to find this packet easily and quickly we have to look for the packet that has “the HTTP verb POST” “



```
No.  Time          Source            Destination       Protocol Length Info
   1 0.000000000   10.0.2.15         44.238.29.244     HTTP      704 POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1  (application/x-www-form-urlencoded)
   2 0.000317435   44.238.29.244     10.0.2.15         TCP        60 80 → 42194 [ACK] Seq=1 Ack=651 Win=65535 Len=0
   3 0.076626380   44.238.29.244     10.0.2.15         HTTP     3450 HTTP/1.1 200 OK  (text/html)
   4 0.076653687   10.0.2.15         44.238.29.244     TCP        54 42194 → 80 [ACK] Seq=651 Ack=3397 Win=62480 Len=0
   5 2.157835477   10.0.2.15         44.238.29.244     TCP        54 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
   6 2.157936487   44.238.29.244     10.0.2.15         TCP        60 [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   7 10.105367608  10.0.2.15         44.238.29.244     TCP        54 [TCP Keep-Alive] 42194 → 80 [ACK] Seq=650 Ack=3397 Win=63900 Len=0
   8 10.105540555  44.238.29.244     10.0.2.15         TCP        60 [TCP Keep-Alive ACK] 80 → 42194 [ACK] Seq=3397 Ack=651 Win=65535 Len=0
   9 12.403232361  10.0.2.15         44.238.29.244     TCP        54 [TCP Dup ACK 5#1] 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
  10 12.403528522  44.238.29.244     10.0.2.15         TCP        60 [TCP Dup ACK 6#1] [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  11 20.341707749  10.0.2.15         44.238.29.244     TCP        54 [TCP Keep-Alive] 42194 → 80 [ACK] Seq=650 Ack=3397 Win=63900 Len=0
  12 20.341936004  44.238.29.244     10.0.2.15         TCP        60 [TCP Keep-Alive ACK] 80 → 42194 [ACK] Seq=3397 Ack=651 Win=65535 Len=0
  13 22.040216834  10.0.2.15         44.238.29.244     TCP        54 [TCP Dup ACK 5#2] 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
  14 22.040532043  44.238.29.244     10.0.2.15         TCP        60 [TCP Dup ACK 6#2] [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 Ack=2 Win=65535 Len=0
  15 25.458188817  PcsCompu_1b:e0:3f RealtekU_12:35:02 ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
```

“This figure shows the information we captured and sniffed from the website we want by checking “HTML form URL Encoded” “



```
No.  Time         Source              Destination         Protocol Length Info
   1 0.000000000  10.0.2.15           44.238.29.244       HTTP      704 POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1  (application/x-w
   2 0.000317435  44.238.29.244       10.0.2.15           TCP        60 80 → 42194 [ACK] Seq=1 Ack=651 Win=65535 Len=0
   3 0.076626380  44.238.29.244       10.0.2.15           HTTP     3450 HTTP/1.1 200 OK  (text/html)
   4 0.076653687  10.0.2.15           44.238.29.244       TCP        54 42194 → 80 [ACK] Seq=651 Ack=3397 Win=62480 Len=0
   5 2.157835477  10.0.2.15           44.238.29.244       TCP        54 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
   6 2.157936487  44.238.29.244       10.0.2.15           TCP        60 [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 Ack=2 Win=65535 Len
   7 10.105367608 10.0.2.15           44.238.29.244       TCP        54 [TCP Keep-Alive] 42194 → 80 [ACK] Seq=650 Ack=3397 Win=63900 Len=0
   8 10.105540555 44.238.29.244       10.0.2.15           TCP        60 [TCP Keep-Alive ACK] 80 → 42194 [ACK] Seq=3397 Ack=651 Win=65535 Len=
   9 12.403232361 10.0.2.15           44.238.29.244       TCP        54 [TCP Dup ACK 5#1] 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
  10 12.403528522 44.238.29.244       10.0.2.15           TCP        60 [TCP Dup ACK 6#1] [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 A
  11 20.341707749 10.0.2.15           44.238.29.244       TCP        54 [TCP Keep-Alive] 42194 → 80 [ACK] Seq=650 Ack=3397 Win=63900 Len=0
  12 20.341936004 44.238.29.244       10.0.2.15           TCP        60 [TCP Keep-Alive ACK] 80 → 42194 [ACK] Seq=3397 Ack=651 Win=65535 Len=
  13 22.640216834 10.0.2.15           44.238.29.244       TCP        54 [TCP Dup ACK 5#2] 56942 → 80 [ACK] Seq=1 Ack=1 Win=63900 Len=0
  14 22.640532043 44.238.29.244       10.0.2.15           TCP        60 [TCP Dup ACK 6#2] [TCP ACKed unseen segment] 80 → 56942 [ACK] Seq=1 A
  15 25.458188817 PcsCompu_1b:e0:3f   RealtekU_12:35:02   ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
```

```
▸ Frame 1: 704 bytes on wire (5632 bits), 704 bytes captured (5632 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_1b:e0:3f (08:00:27:1b:e0:3f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 44.238.29.244
▸ Transmission Control Protocol, Src Port: 42194, Dst Port: 80, Seq: 1, Ack: 1, Len: 650
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "tfUName" = "HCRHMA"
  ▸ Form item: "tfUPass" = "CYBER100"
```

Social Engineering Toolkit (SET)

- SET is specifically designed to perform advanced attacks against the human element.
- SET is free and Open Source.

How SET Works

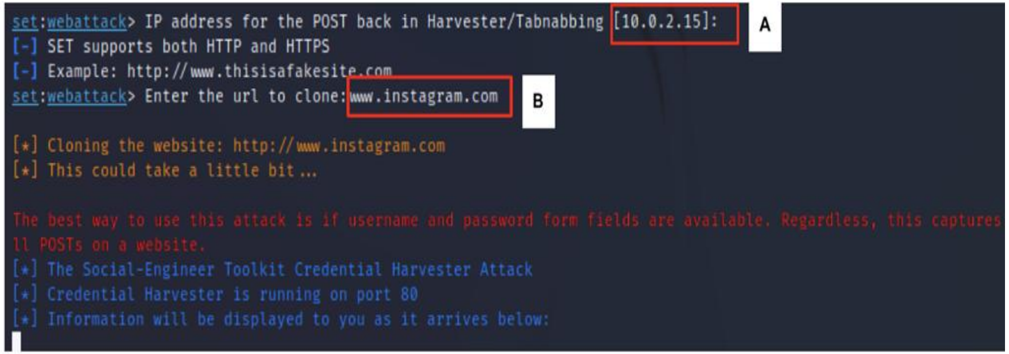
- Research the target.
- Make contact with the target.
- Attack.

Types of Social Engineering Attacks

- Phishing
- Visihing
- Baiting Attacks
- Impersonation

SET Experiment

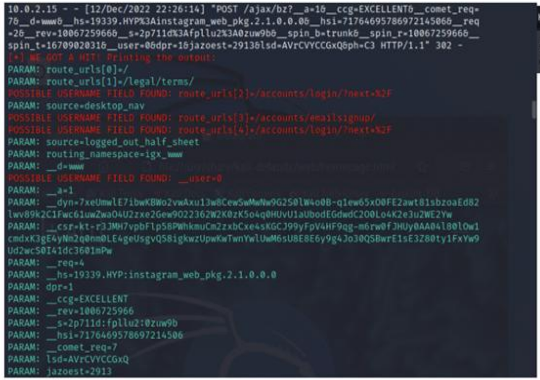
1. Social-Engineering Attack
2. Website Attack Vector
3. Credential Harvester Attack Method
4. Site Cloner
5. Host Web Server
6. Type IP Address of Website to Clone
7. Login
8. Collect Victim’s Credentials



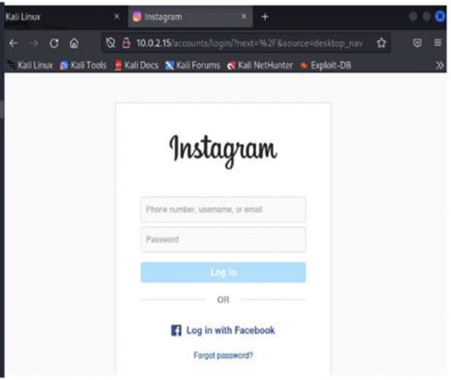
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.instagram.com

[*] Cloning the website: http://www.instagram.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
ll 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:
```



```
10.0.2.15 - - [12/Dec/2022 22:26:14] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet_req=
7&__d=www&__hs=19339.HYP%3Ainstagram_web_pkg.2.1.0.0.0&__hsi=7176469578697214506&__req
=2&__rev=1006725966&__s=2p711d%3Afpllu2%3A0zuw9b&__spin_b=trunk&__spin_r=1006725966&__
spin_t=1670902031&__user=0&dpr=1&jazoest=2913&lsd=AVrCVYCCGxQ&ph=C3 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: route_urls[0]=/
PARAM: route_urls[1]=/legal/terms/
POSSIBLE USERNAME FIELD FOUND: route_urls[2]=/accounts/login/?next=%2F
PARAM: source=desktop_nav
POSSIBLE USERNAME FIELD FOUND: route_urls[3]=/accounts/emailsignup/
POSSIBLE USERNAME FIELD FOUND: route_urls[4]=/accounts/login/?next=%2F
PARAM: source=logged_out_half_sheet
PARAM: routing_namespace=igx_www
PARAM: __d=www
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __dyn=7xeUmwlE7ibwKBWo2vwAxu13w8CewSwMwNw9G2S0lW4o0B-q1ew65xO0FE2awt81sbzoaEd82
lwv89k2C1Fwc61uwZwaO4U2zxe2Gew9O22362W2K0zK5o4q0HUvU1aUbodEGdwdC2O0Lo4K2e3u2WE2Yw
PARAM: __csr=kt-r3JMH7vpbFlp58PWhkmuCm2zxbCxe4sKGCJ99yFpV4HF9qg-m6rw0fJHUy0AA04l80lOw1
cmdxK3gE4yNm2q0nm0LE4geUsgvQ58igkwzUpwKwTwnYwlUwM6sU8E8E6y9g4Jo30QSBwrE1sE3Z80ty1FxYw9
Ud2wcS0I41dc3601mPw
PARAM: __req=4
PARAM: __hs=19339.HYP:instagram_web_pkg.2.1.0.0.0
PARAM: dpr=1
PARAM: __ccg=EXCELLENT
PARAM: __rev=1006725966
PARAM: __s=2p711d:fpllu2:0zuw9b
PARAM: __hsi=7176469578697214506
PARAM: __comet_req=7
PARAM: lsd=AVrCVYCCGxQ
PARAM: jazoest=2913
```



How to Prevent Being a Victim

- Be aware of all the possible attack vectors around you.
- Don’t go into a conversation that its topic can lead to leaking sensitive information.
- Don’t open emails from unknown sources.
- Don’t share your life details online.
- Don’t tell your passwords to anyone.
- Be aware of what you are revealing to strangers.

Conclusion

- We may use John the Ripper to safeguard our sensitive information by testing password strength, recovering lost passwords, and cracking weak passwords.
- Wireshark allows us to break any passwords used on any dangerous website by collecting the website's packet.
- The user is the most susceptible link in the security chain, and SET includes choices for attack paths to quickly create a credible attack.

References

- “What Is Penetration Testing: Step-by-Step Process & Methods: Imperva.” *Imperva*, 29 Dec. 2019, https://www.imperva.com/learn/application-security/penetration-testing/.
- Kamel, Samer. “Wireshark- Life Capturing.” *Wireshark*, https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html.
- Contributor, TechTarget. “What Is a Dictionary Attack? - Definition from Whatis.com.” *Security*, TechTarget, 30 June 2021, https://www.techtarget.com/searchsecurity/definition/dictionary-attack.
- Borges, Esteban.The Social Engineering Toolkit. Security Trails. https://securitytrails.com/blog/the-social-engineering-toolkit

THANK YOU!
QUESTIONS?