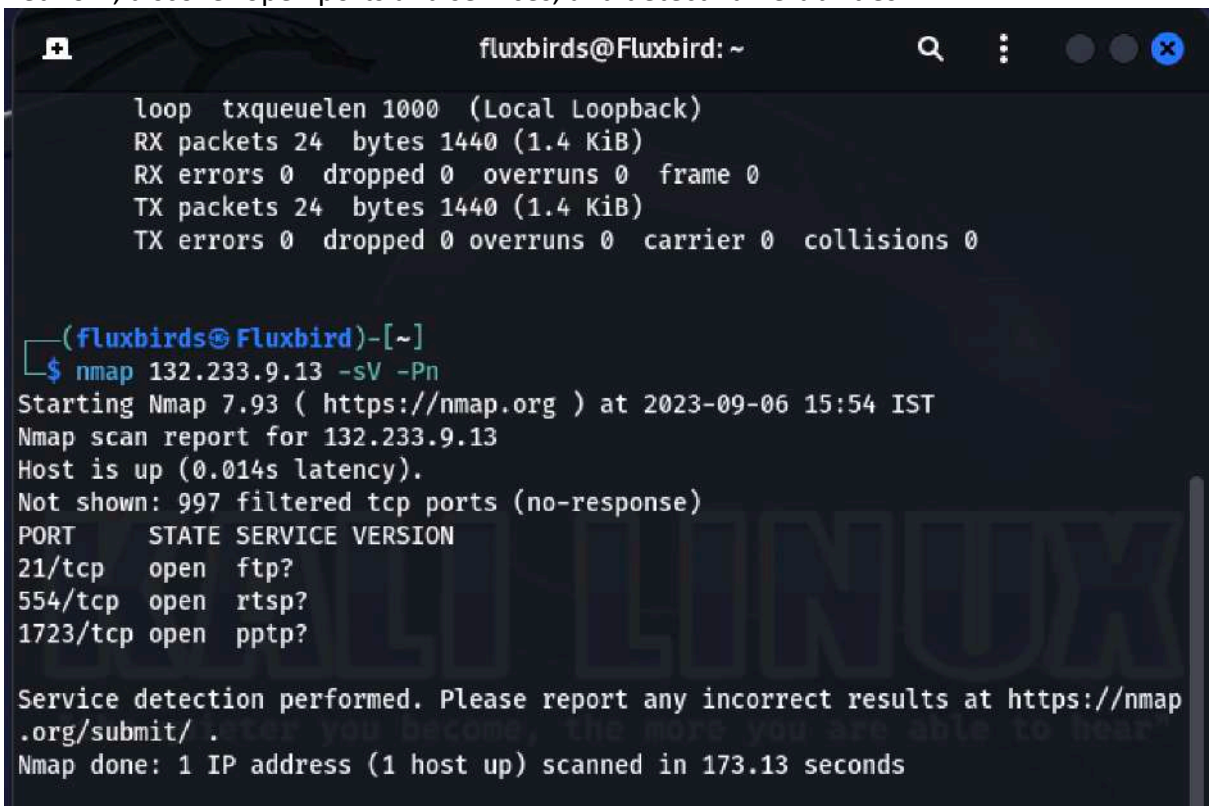
Siddharth Sharma

Nmap:

Nmap (Network Mapper) is a free and open-source tool for network discovery and security auditing. It is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.



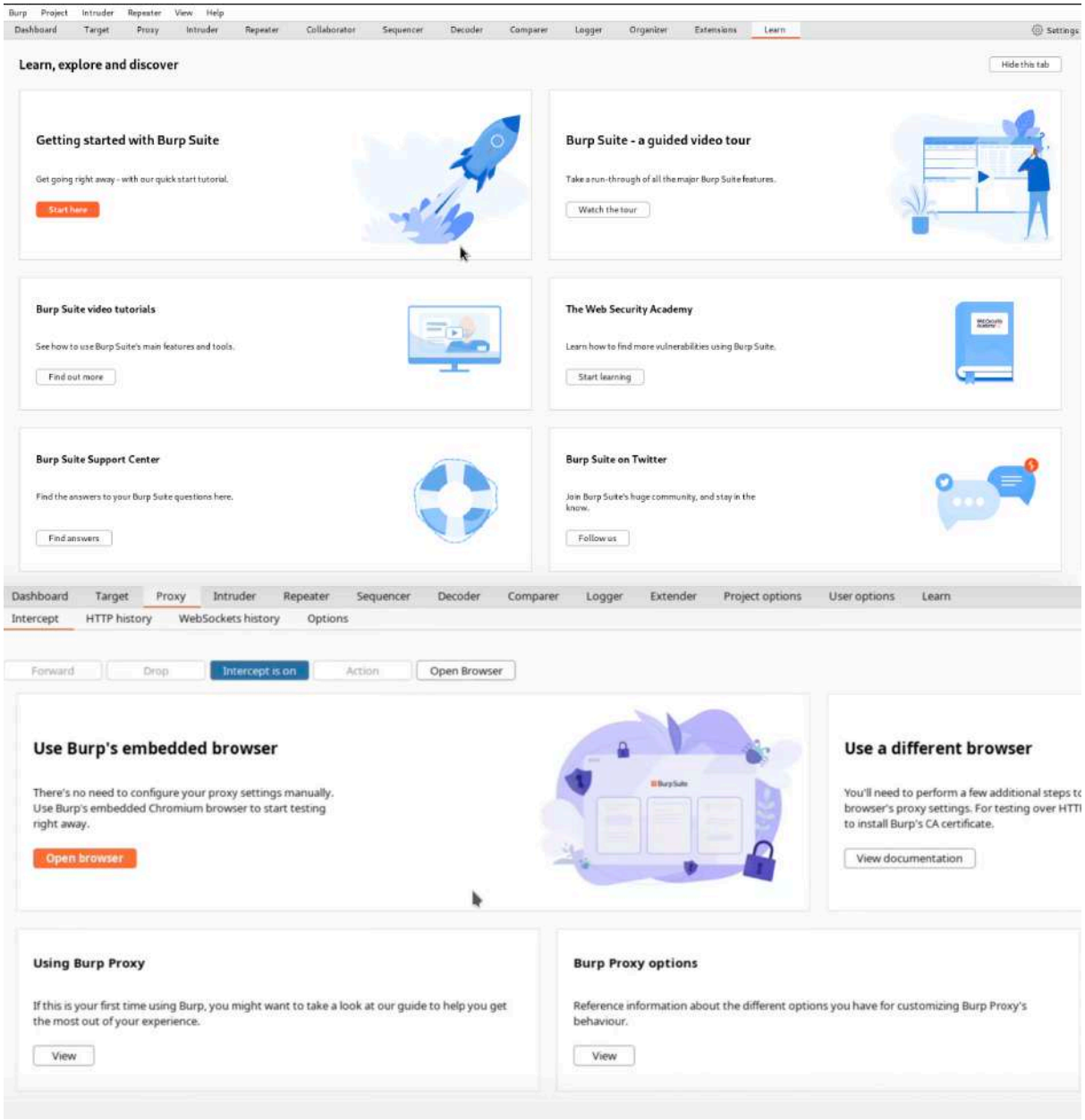
Burp suit:

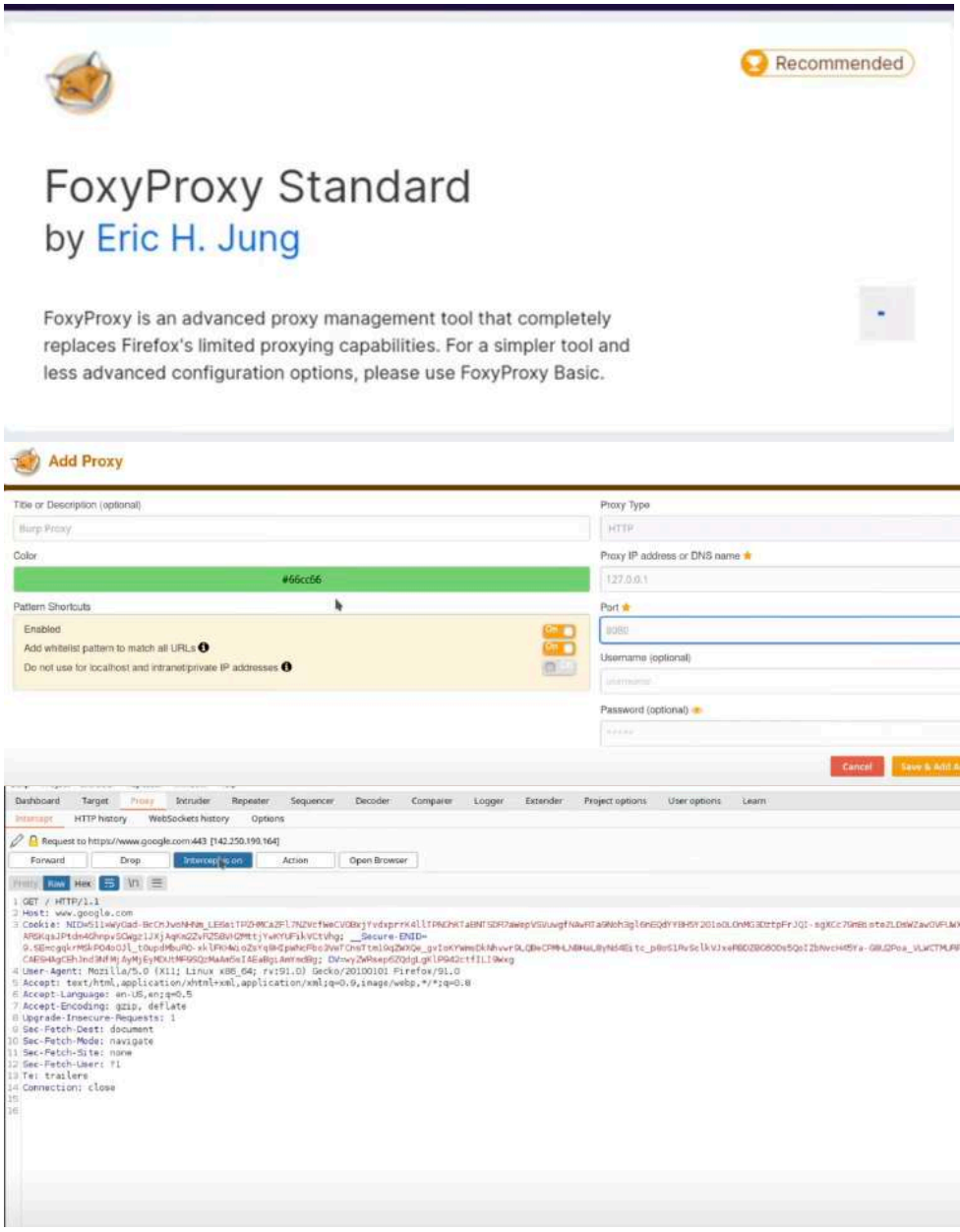
Burp Suite is a comprehensive suite of tools for web application security testing. It can be used to identify and exploit vulnerabilities in web applications, as well as to improve the security of web applications.

Burp Suite consists of a number of different tools, including:

- Proxy: The proxy intercepts all traffic between the user's browser and the web application. This allows Burp Suite to examine the traffic and identify potential vulnerabilities.
- Scanner: The scanner automatically scans web applications for known vulnerabilities.
- Intruder: The intruder tool can be used to fuzz web applications and to identify vulnerabilities that are not detected by the scanner.
- Repeater: The repeater tool allows the user to manually send requests to the web application and to see the responses. This can be used to debug web applications and to identify vulnerabilities.

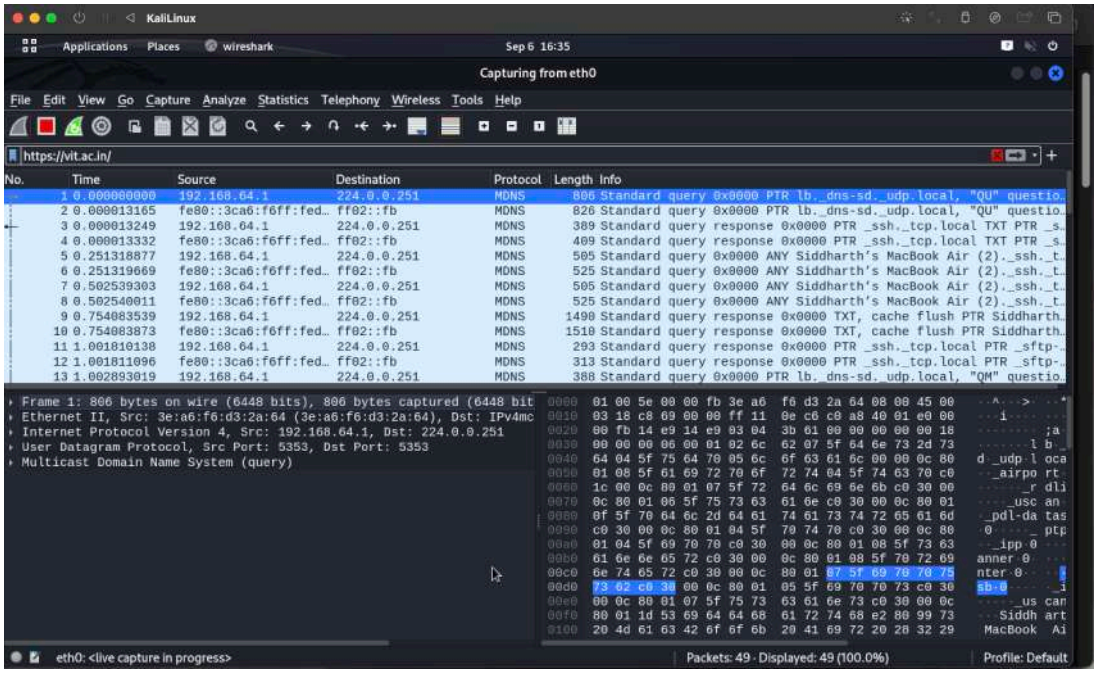
- Sequencer: The sequencer tool can be used to analyze the sequence of requests and responses in a web application. This can be used to identify vulnerabilities that are not detected by the other tools.
- Spider: The spider tool can be used to crawl a web application and to identify all of the pages and resources that are available. This can be used to find vulnerabilities that are not easily accessible.
- Extender: The extender allows the user to add custom functionality to Burp Suite. This can be used to extend the capabilities of Burp Suite and to automate tasks.





Wireshark:

Wireshark is a tool that can be used to see what is happening on a network. It can be used to troubleshoot problems, see how applications are communicating, and even find security vulnerabilities.
Wireshark works by capturing packets of data as they travel over the network. It then decodes these packets and displays them in a human-readable format. This allows you to see the contents of the packets, including the source and destination addresses, the protocol used, and the data being transmitted.

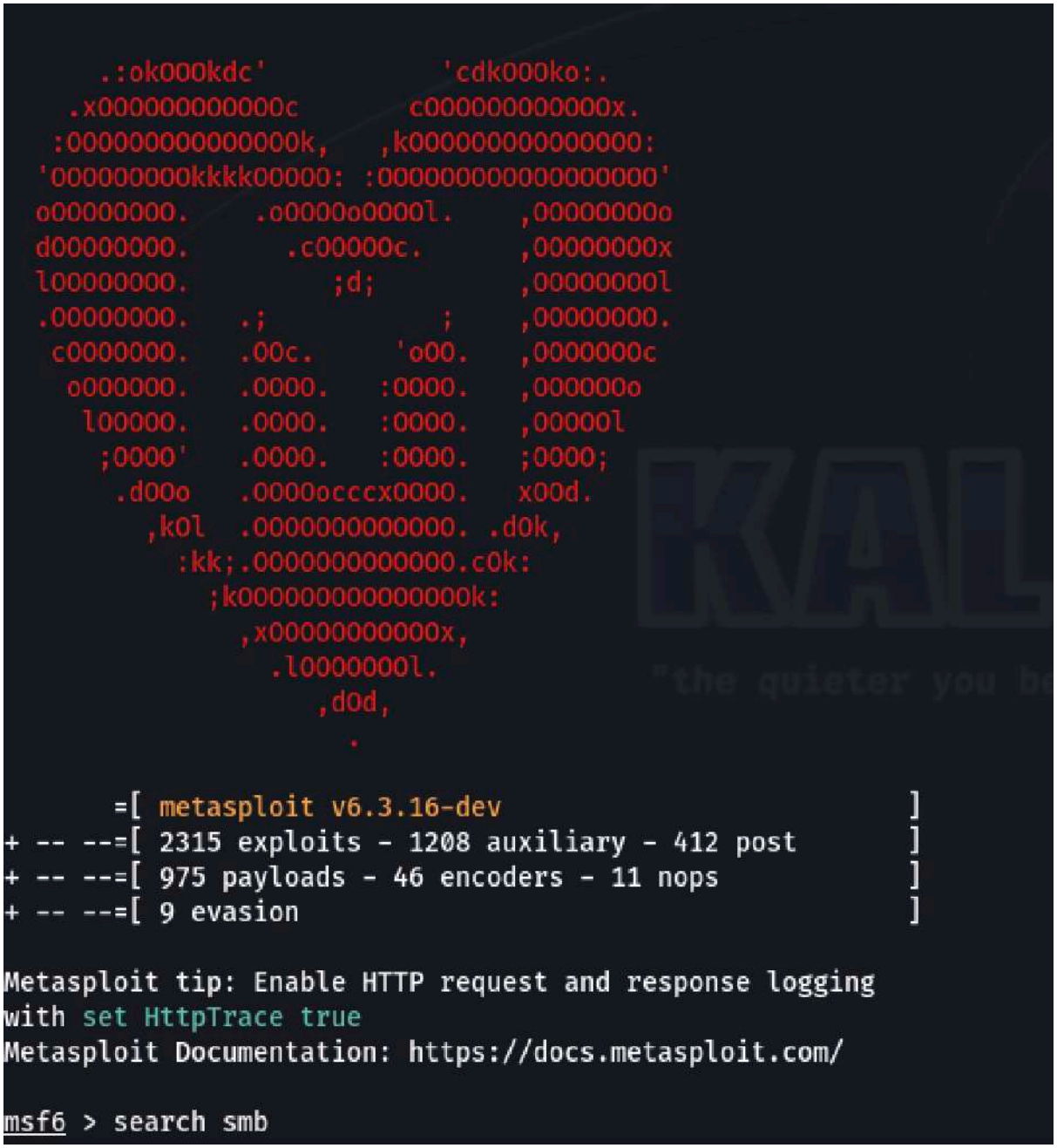


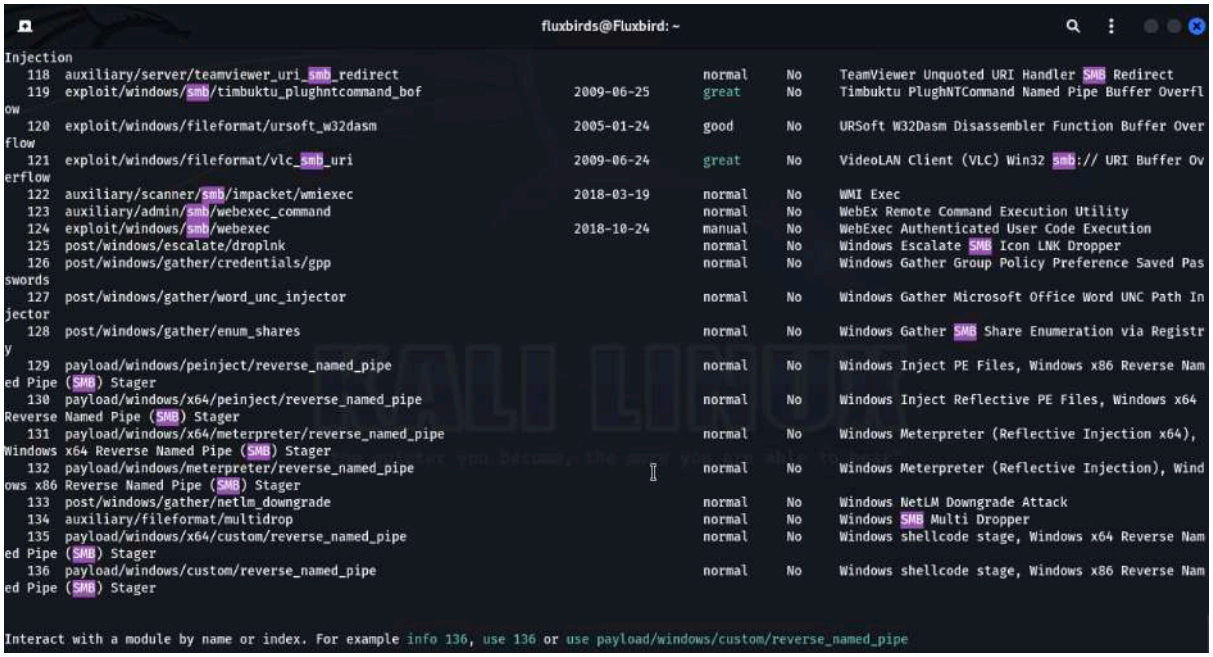
Metaspolit:

Metasploit is a penetration testing framework that is used to find and exploit vulnerabilities in computer systems and networks. It is a powerful tool that can be used by security professionals to test the security of their systems and by attackers to exploit vulnerabilities.

Metasploit has a large library of exploits that can be used to exploit known vulnerabilities. It also has a variety of tools that can be used to automate tasks, such as scanning for vulnerabilities and generating reports.

- Penetration testing: Metasploit can be used by penetration testers to identify and exploit vulnerabilities in computer systems and applications. This helps to improve the security of the systems and applications.
- Vulnerability scanning: Metasploit can be used to scan networks and systems for vulnerabilities. This can help organizations to identify and fix vulnerabilities before they can be exploited by attackers.
- Security research: Metasploit can be used by security researchers to study vulnerabilities and to develop new ways to exploit them. This helps to improve the understanding of vulnerabilities and how to prevent them.
- Cyberwarfare: Metasploit can be used by governments and militaries to exploit vulnerabilities in enemy systems. This can be used to gain intelligence or to disrupt enemy operations.


.:ok000kdc' 'cdk000ko:.
.x000000000000c c000000000000x.
:0000000000000000k, ,k0000000000000000:
'0000000000kkkk00000: :0000000000000000000'
o00000000. .o00000o0000l. ,00000000o
d00000000. .c00000c. ,00000000x
l00000000. ;d; ,00000000l
.00000000. .; ; ,00000000.
c0000000. .00c. 'o00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000l
;0000' .0000. :0000. ;0000;
.d000 .0000occcx0000. x000d.
,k0l .0000000000000. .d0k,
:kk;.0000000000000.c0k:
;k000000000000000k:
,x00000000000x,
.l0000000l.
,d0d,
.
=[metasploit v6.3.16-dev]
+ -- --=[2315 exploits - 1208 auxiliary - 412 post]
+ -- --=[975 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smb



Aircrack-ng:

Aircrack-ng is a suite of tools that can be used to crack wireless security protocols, such as WEP and WPA. It can also be used to monitor wireless networks and capture packets.

Aircrack-ng is a command-line tool, but there are also GUIs available. It is available for Linux, macOS, Windows, and FreeBSD.

To use Aircrack-ng, you will need to have a wireless adapter that supports monitor mode. You can check if your adapter supports monitor mode by running the following command:

If your adapter supports monitor mode, you will see a list of interfaces that can be used in monitor mode.

```
$ aircrack-ng --help

Aircrack-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:

    -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
    -e <essid> : target selection: network identifier
    -b <bssid> : target selection: access point's MAC
    -p <nbcpu> : # of CPU to use  (default: all CPUs)
    -q         : enable quiet mode (no status output)
    -C <macs>  : merge the given APs to a virtual one
    -l <file>  : write key to file. Overwrites file.

Static WEP cracking options:

    -c         : search alpha-numeric characters only
    -t         : search binary coded decimal chr only
    -h         : search the numeric key for Fritz!BOX
    -d <mask>  : use masking of the key (A1:XX:CF:YY)
    -m <maddr> : MAC address to filter usable packets
    -n <nbits> : WEP key length :  64/128/152/256/512
    -i <index> : WEP key index (1 to 4), default: any
    -f <fudge> : bruteforce fudge factor,  default: 2
    -k <korek> : disable one attack method  (1 to 17)
    -x or -x0  : disable bruteforce for last keybytes
    -x1        : last keybyte bruteforcing  (default)
    -x2        : enable last  2 keybytes bruteforcing
    -X         : disable  bruteforce   multithreading
    -y         : experimental  single bruteforce mode
    -K         : use only old KoreK attacks (pre-PTW)
    -s         : show the key in ASCII while cracking
    -M <num>   : specify maximum number of IVs to use
    -D         : WEP decloak, skips broken keystreams
    -P <num>   : PTW debug:  1: disable Klein, 2: PTW
```

```
┌──(root㉿Fluxbird)-[/home/fluxbirds]
└─# airmon-ng start

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    477 dhclient
    590 NetworkManager
   1035 wpa_supplicant

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

```
wlan0     IEEE 802.11  Mode:Master  Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

eth0      no wireless extensions.

wlan0-1   IEEE 802.11  Mode:Master  Tx-Power=17 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

wlan1mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off

br-lan    no wireless extensions.

eth1      no wireless extensions.
```

Jhon the ripper:

John the Ripper is a popular open source password cracking tool that combines several different cracking programs and runs in both brute force and dictionary attack modes.

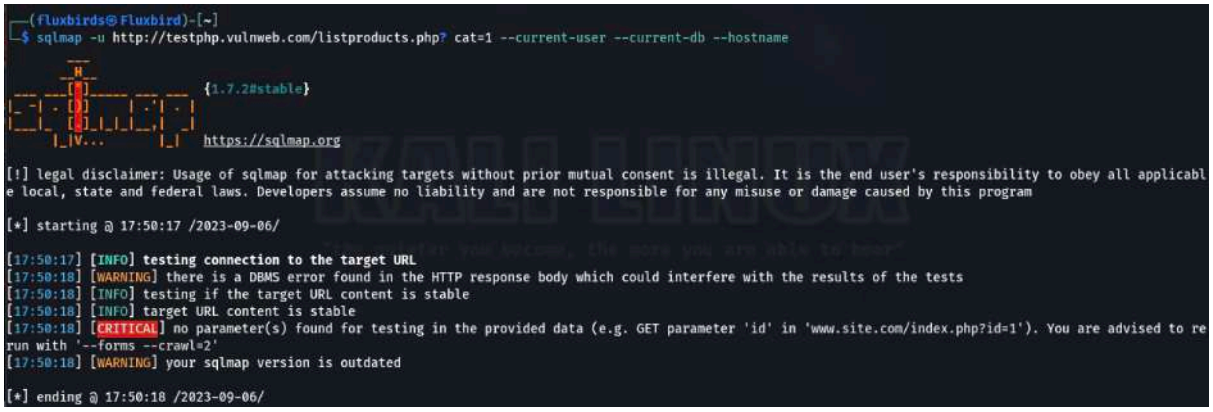
```
└─$ john b1.txt --format=RAW-MD5
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
12345            (?)
1234             (?)
123              (?)
Proceeding with incremental:ASCII
1234589          (?)
4g 0:00:00:06 DONE 3/3 (2021-05-10 01:19) 0.6557g/s 12892Kp/s 12892Kc/s 12892KC/s ts1gg16..1234532
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

```
└─# john --format=zip hash123.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Cost 1 (HMAC size) is 302322 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456           (demofile.zip/chinook.db)
1g 0:00:00:19 DONE 2/3 (2023-08-27 07:30) 0.05208g/s 2104p/s 2104c/s 2104C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Sqlmap:

- Penetration testing: SQLmap can be used by penetration testers to identify and exploit SQL injection vulnerabilities in web applications. This helps to improve the security of the applications and prevent attackers from exploiting them.
- Vulnerability scanning: SQLmap can be used to scan websites for SQL injection vulnerabilities. This can help organizations to identify and fix vulnerabilities before they can be exploited by attackers.
- Security research: SQLmap can be used by security researchers to study SQL injection vulnerabilities and develop new ways to exploit them. This helps to improve the understanding of SQL injection vulnerabilities and how to prevent them.

```
┌──(fluxbirds㉿Fluxbird)-[~]
└─$ sqlmap -u http: //testphp. vulnweb.com/ --crawl 2 --batch -v 4

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicabl
e local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:47:09 /2023-09-06/

[17:47:09] [DEBUG] cleaning up configuration parameters
[17:47:09] [DEBUG] setting the HTTP timeout
[17:47:09] [DEBUG] setting the HTTP User-Agent header
[17:47:09] [DEBUG] creating HTTP requests opener object
do you want to check for the existence of site's sitemap(.xml) [y/N] N
[17:47:09] [DEBUG] used the default behavior, running in batch mode
[17:47:09] [INFO] starting crawler for target URL 'http://http:'
[17:47:09] [INFO] searching for links with depth 1
[17:47:09] [TRAFFIC OUT] HTTP request [#1]:
GET http://http: HTTP/1.1
Cache-control: no-cache
User-agent: sqlmap/1.7.2#stable (https://sqlmap.org)
Host: http:
Accept: */*
Accept-encoding: gzip,deflate
Connection: close

[17:47:09] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[17:47:09] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--r
andom-agent' and/or proxy switches ('--proxy', '--proxy-file'...)
[17:47:09] [TRAFFIC OUT] HTTP request [#2]:
GET http://http: HTTP/1.1
```



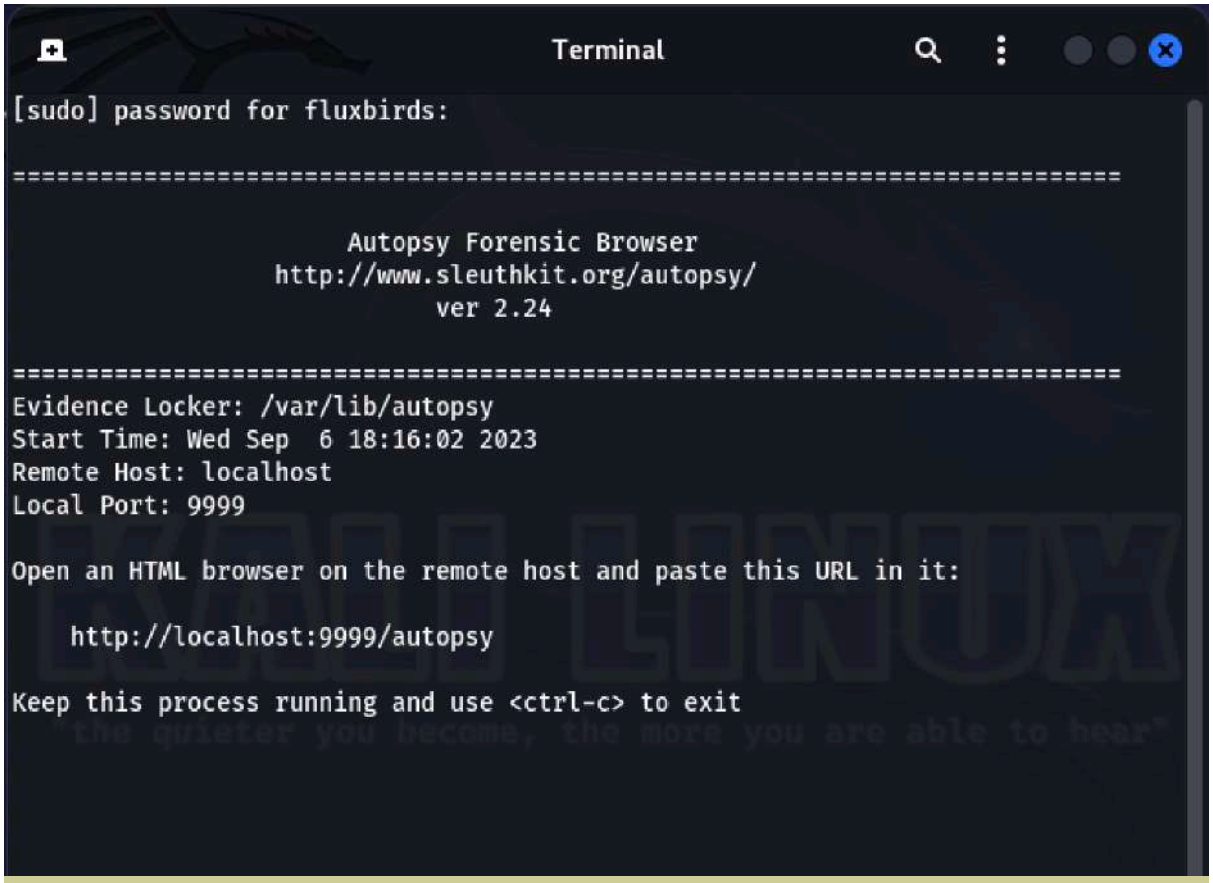
Autopsy:

Autopsy is a free and open-source digital forensics platform that can be used to investigate what happened on a computer. It is used by law enforcement, military, and corporate examiners to investigate cybercrimes, data breaches, and other incidents.

Autopsy can be used to:

- Analyze disk images: Autopsy can be used to analyze disk images, which are copies of hard drives or other storage devices. This can be used to recover deleted files, find hidden files, and identify malware.
- Extract files: Autopsy can be used to extract files from disk images or other sources. This can be used to recover files that have been deleted or encrypted.
- View file metadata: Autopsy can be used to view the metadata of files, such as the file creation date, file modification date, and file size. This can be used to track the movement of files and to identify suspicious activity.
- Search for keywords: Autopsy can be used to search for keywords in files or in the file metadata. This can be used to find specific information, such as emails, documents, or images.
- Generate reports: Autopsy can be used to generate reports that summarize the findings of the investigation. These reports can be used to share the findings with law enforcement or other stakeholders.

Autopsy is a powerful tool that can be used to investigate a wide variety of digital evidence. It is easy to use and can be used by investigators of all levels of experience.



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. b.
c. d.
e. f.
g. h.
i. j.

NEW CASE CANCEL HELP

The Harvester:

TheHarvester is a tool that can be used to collect information about hosts and domains on the internet, such as email addresses, IP addresses, and social media profiles. It can be used for a variety of purposes, including:

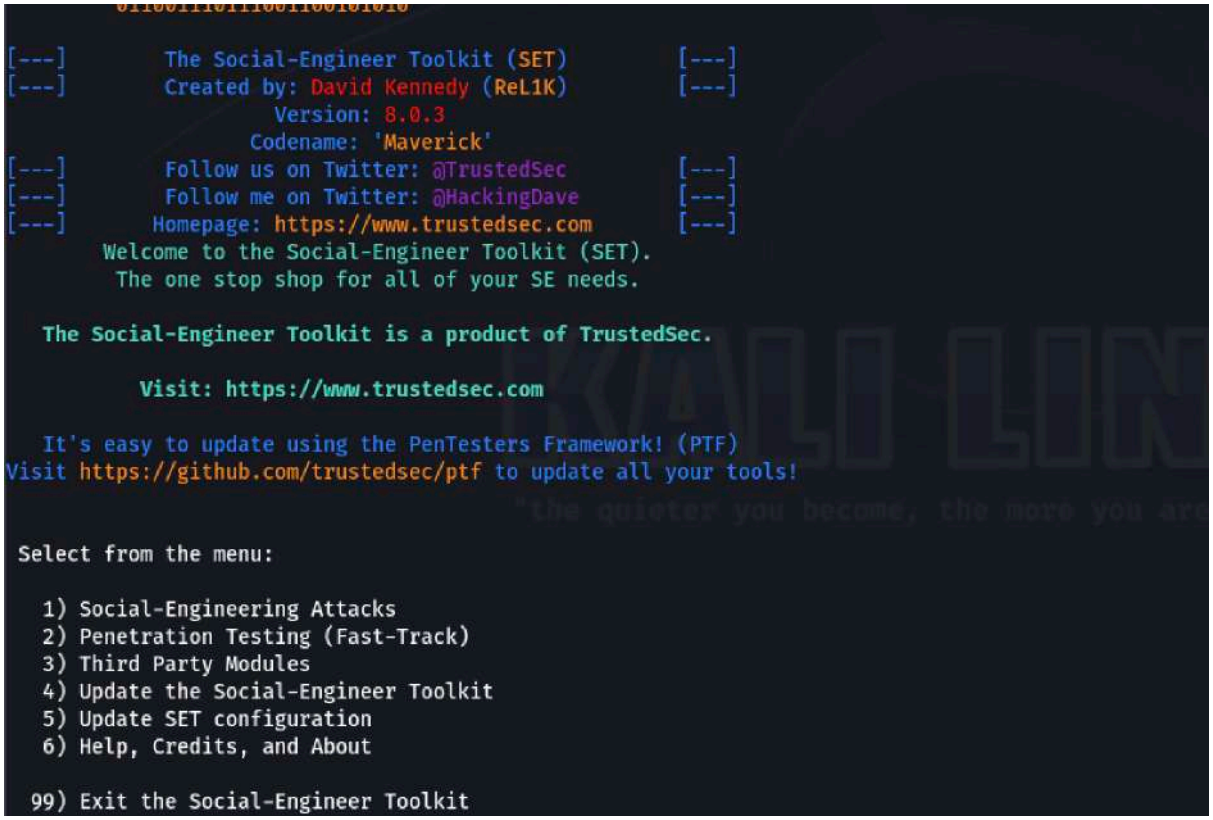
- Penetration testing: TheHarvester can be used by penetration testers to gather information about the target organization. This information can be used to identify potential vulnerabilities and to plan an attack.
- Cyber threat intelligence: TheHarvester can be used by cyber threat intelligence analysts to gather information about potential threats. This information can be used to identify and track threats, as well as to develop mitigation strategies.
- OSINT: TheHarvester can be used by open-source intelligence (OSINT) analysts to gather information about a wide variety of topics. This information can be used to support research, investigations, and decision-making.

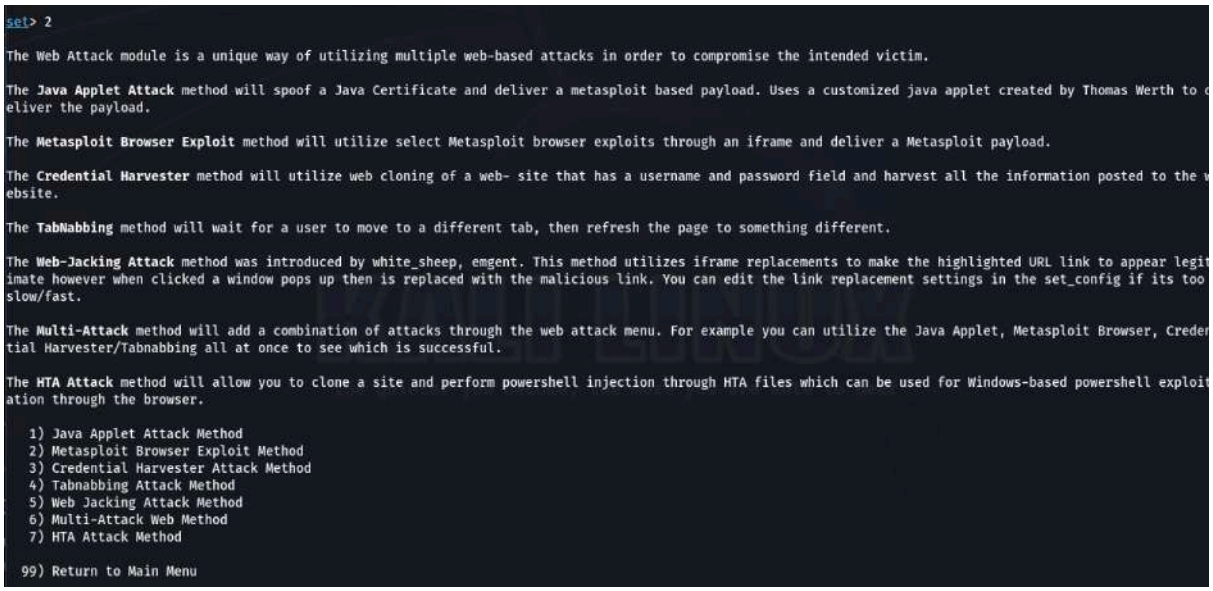
```
┌──(fluxbirds㉿Fluxbird)-[~]
└─$ theHarvester -d bug-bounty.com -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: bug-bounty.com
```

```
[*] ASNS found: 1
--------------------
AS13335

[*] Interesting Urls found: 1
--------------------
https://bug-bounty.com/

[*] LinkedIn Links found: 0
--------------------

[*] IPs found: 10
-------------------
104.26.4.94
104.26.5.94
104.28.20.90
104.28.21.90
172.66.40.55
172.66.43.201
172.67.73.242
172.67.133.165
2606:4700:3032::ac43:85a5
```

Setoolkit:

The Social engineering toolkit is an open sourced free python tool written by Dave Kennedy from TrustedSec. This open sourced tool is mostly used by penetration testers, black-hat hackers, blue and purple teams for performing social engineering attacks.





```
set:webattack>2

 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 supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.instagram.com/

 Enter the browser exploit you would like to use [8]:

   1) Adobe Flash Player ByteArray Use After Free (2015-07-06)
   2) Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow (2015-06-23)
   3) Adobe Flash Player Drawing Fill Shader Memory Corruption (2015-05-12)
   4) MS14-012 Microsoft Internet Explorer TextRange Use-After-Free (2014-03-11)
   5) MS14-012 Microsoft Internet Explorer CMarkup Use-After-Free (2014-02-13)
   6) Internet Explorer CDisplayPointer Use-After-Free (10/13/2013)
   7) Micorosft Internet Explorer SetMouseCapture Use-After-Free (09/17/2013)
   8) Java Applet JMX Remote Code Execution (UPDATED 2013-01-19)
   9) Java Applet JMX Remote Code Execution (2013-01-10)
  10) MS13-009 Microsoft Internet Explorer SLayoutRun Use-AFter-Free (2013-02-13)
  11) Microsoft Internet Explorer CDwnBindInfo Object Use-After-Free (2012-12-27)
  12) Java 7 Applet Remote Code Execution (2012-08-26)
  13) Microsoft Internet Explorer execCommand Use-After-Free Vulnerability (2012-09-14)
  14) Java AtomicReferenceArray Type Violation Vulnerability (2012-02-14)
  15) Java Applet Field Bytecode Verifier Cache Remote Code Execution (2012-06-06)
  16) MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory Corruption (2012-06-12)
  17) Microsoft XML Core Services MSXML Uninitialized Memory Corruption (2012-06-12)
  18) Adobe Flash Player Object Type Confusion  (2012-05-04)
  19) Adobe Flash Player MP4 "cprt" Overflow (2012-02-15)
  20) MS12-004 midiOutPlayNextPolyEvent Heap Overflow (2012-01-10)
  21) Java Applet Rhino Script Engine Remote Code Execution (2011-10-18)
  22) MS11-050 IE mshtml!CObjectElement Use After Free  (2011-06-16)
  23) Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability (2011-04-11)
  24) Cisco AnyConnect VPN Client ActiveX URL Property Download and Execute (2011-06-01)
  25) Internet Explorer CSS Import Use After Free (2010-11-29)
  26) Microsoft WMI Administration Tools ActiveX Buffer Overflow (2010-12-21)
  27) Internet Explorer CSS Tags Memory Corruption (2010-11-03)
  28) Sun Java Applet2ClassLoader Remote Code Execution (2011-02-15)
  29) Sun Java Runtime New Plugin docbase Buffer Overflow (2010-10-12)
```

```
set:payloads>1
set:payloads> Port to use for the reverse [443]:80

[*] Cloning the website: https://www.instagram.com/
[*] This could take a little bit...
[*] Injecting iframes into cloned website for MSF Attack....
[*] Malicious iframe injection successful...crafting payload.


**************************************************
Web Server Launched. Welcome to the SET Web Attack.
**************************************************

[--] Tested on Windows, Linux, and OSX [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
```