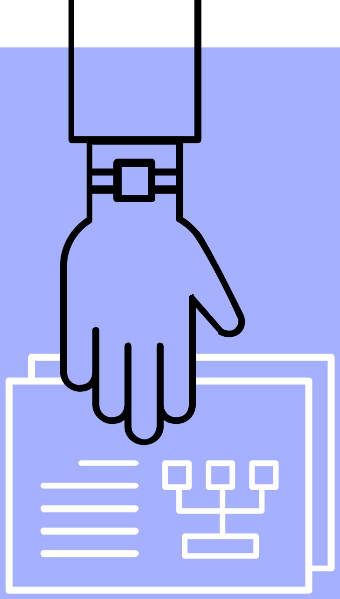
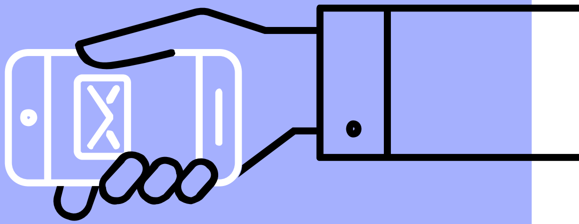
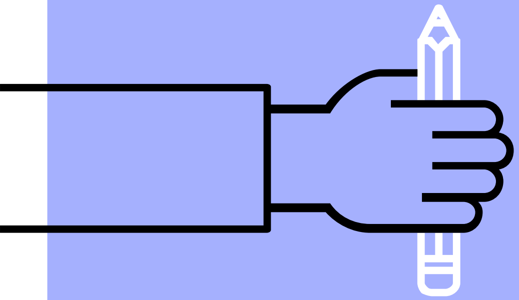
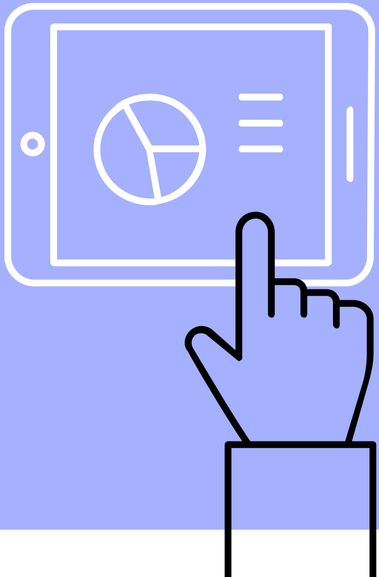




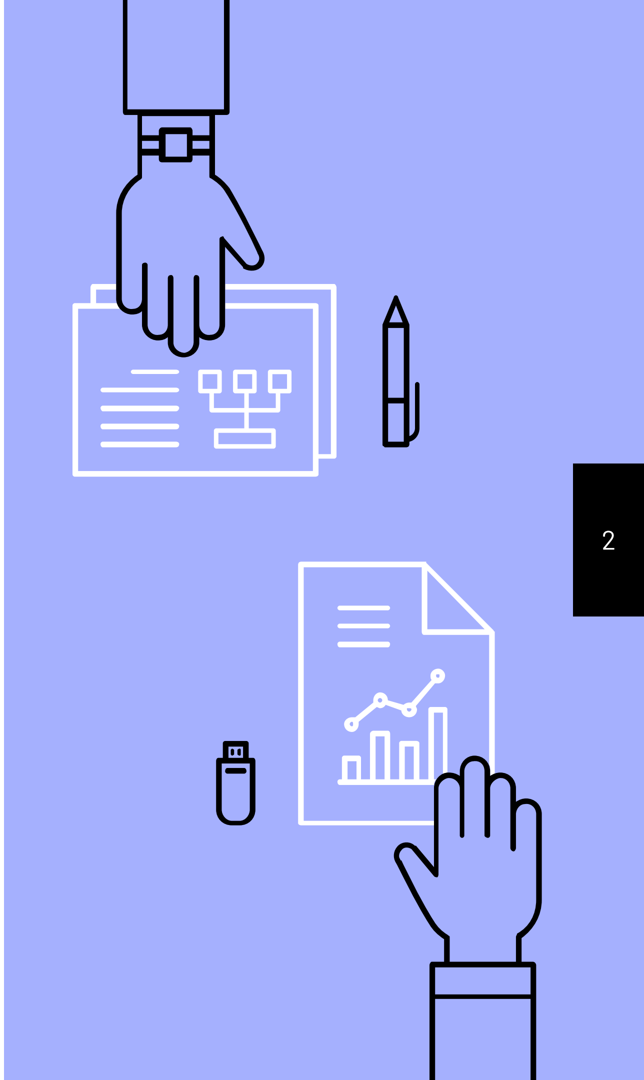
Network Vulnerability Assessment & Penetration Testing (VAPT)





Disclaimer

Lets hope I do a good job!



> *For every lock, there is someone out there trying to pick it or break in.*

David Bernstein
President, The Bernstein Agency

What are we here for?

★ Information Security

★ Cyber Security Process

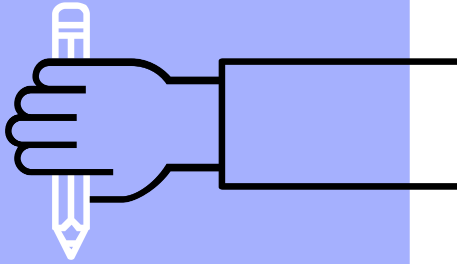
★ Introduction to VAPT

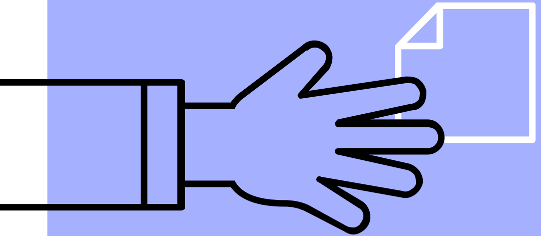
★ Process of VAPT

★ Types of Attacks

★ Tools of VAPT

★ Cyber Security Best Practices





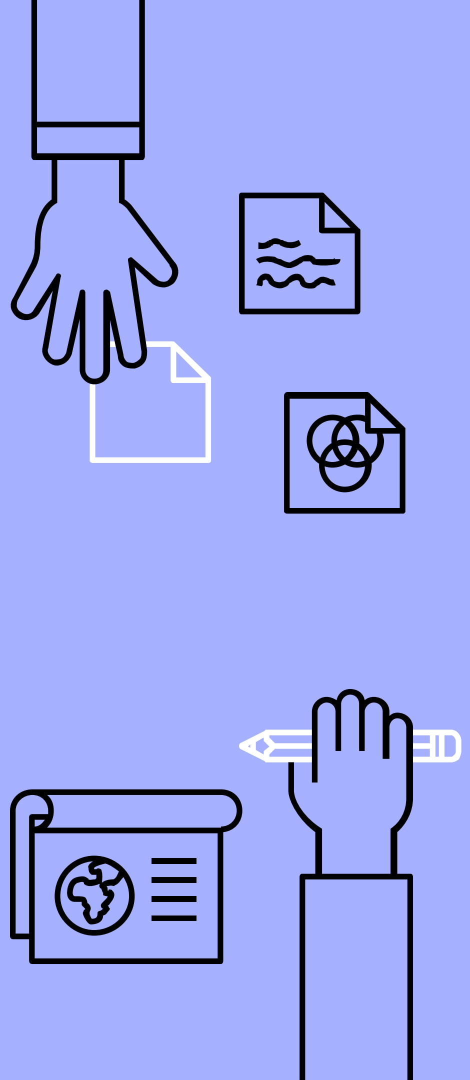
There are only two types of companies: those that have been hacked, and those that will be.

Robert Mueller

FBI Director

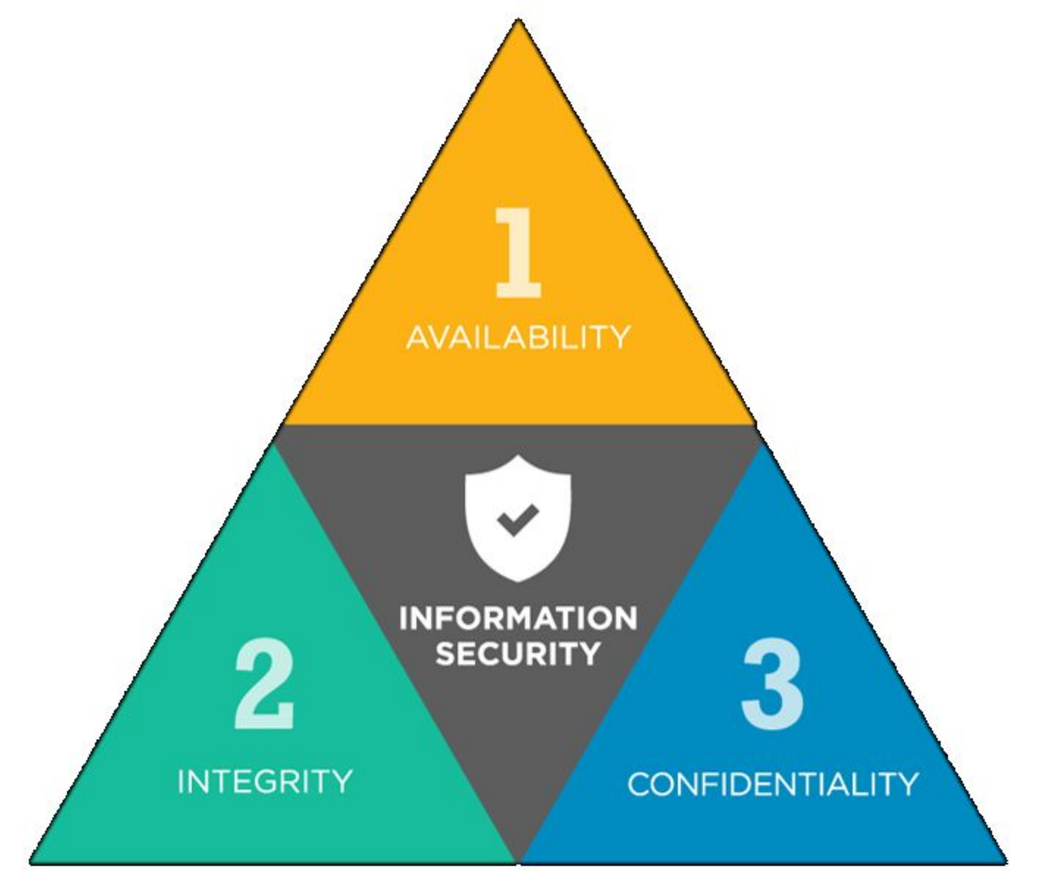
What is Information Security?

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.



The CIA Concept

1. Confidentiality
2. Integrity
3. Availability



Cybersec Process of CIA

- *Security Audits*

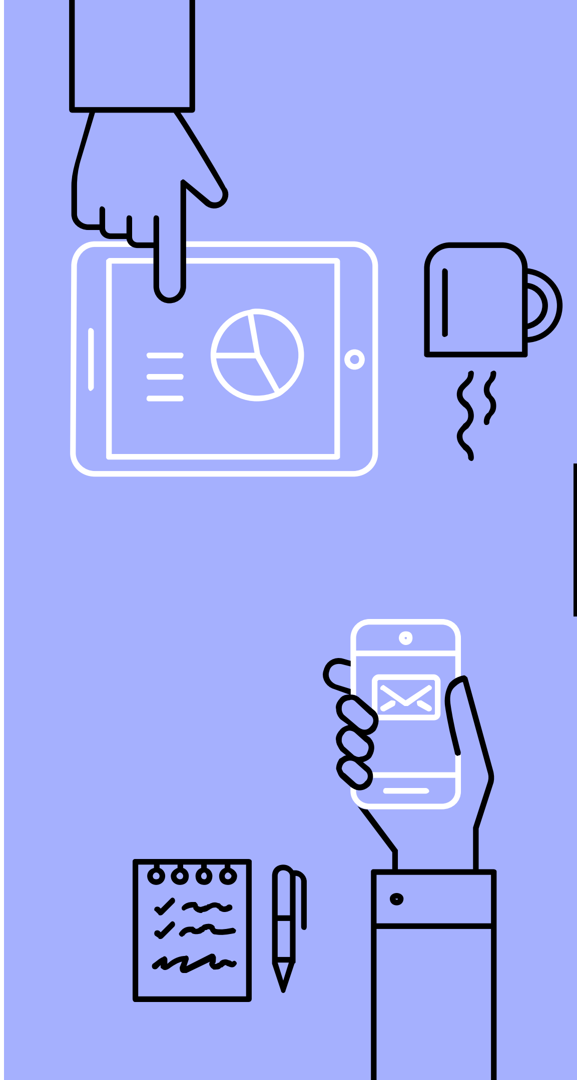
Measure a system performance against a list of criteria or configuration

- *Vulnerability Assessment*

Involves a comprehensive study of an entire network, seeking potential security awareness

- *Penetration Testing*

Covert operation, in which security expert tries number of attacks to ascertain whether or not a network could withstand same type of attack from a malicious hacker



What is a Vulnerability?

- In computer security, a vulnerability is a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorized actions within a computer system

- They are used to facilitate attacks that can lead to data theft, malware injection and server takeover, among other consequences

What is VA?

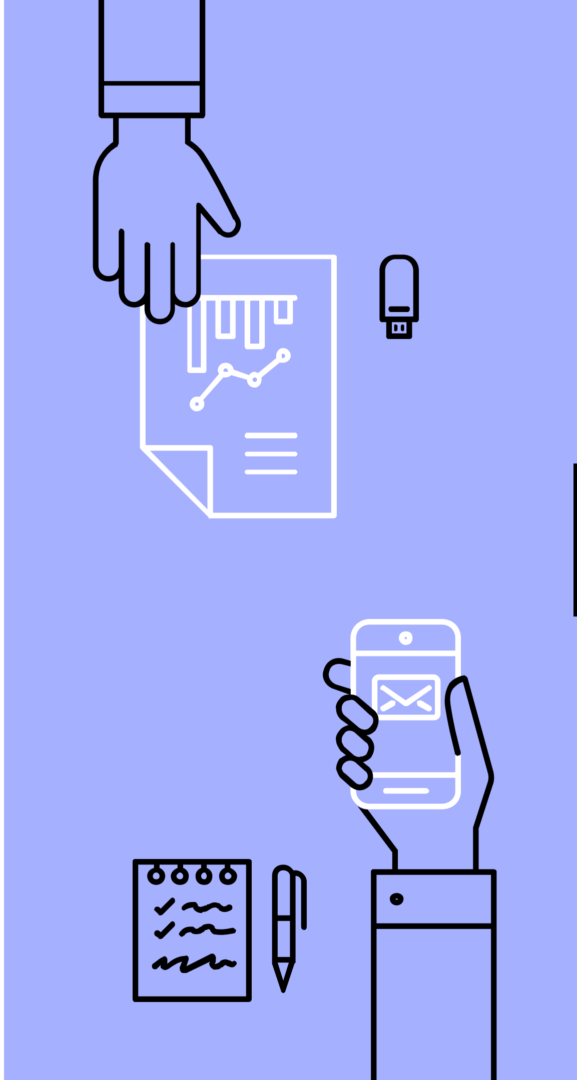
- Process that is intended to identify threats and the risks they poses

- It involves the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

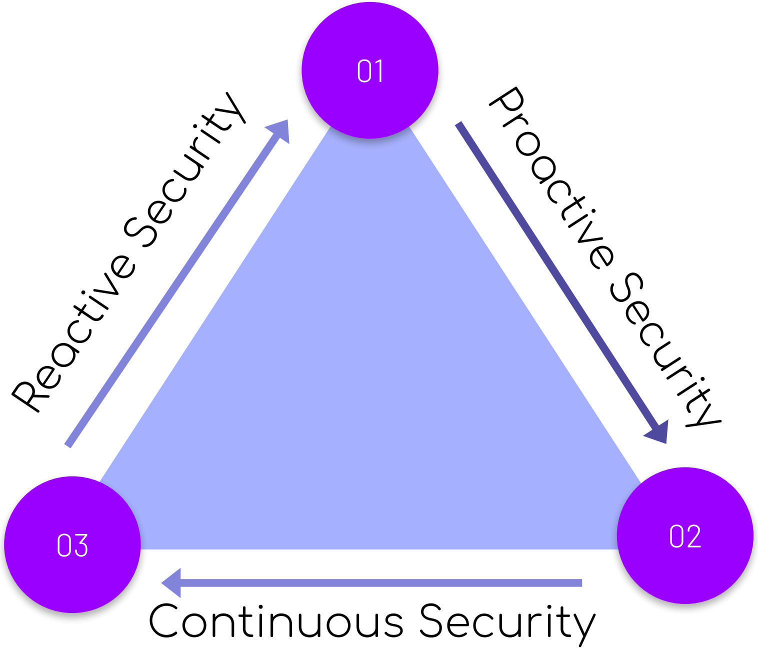
Penetration Testing

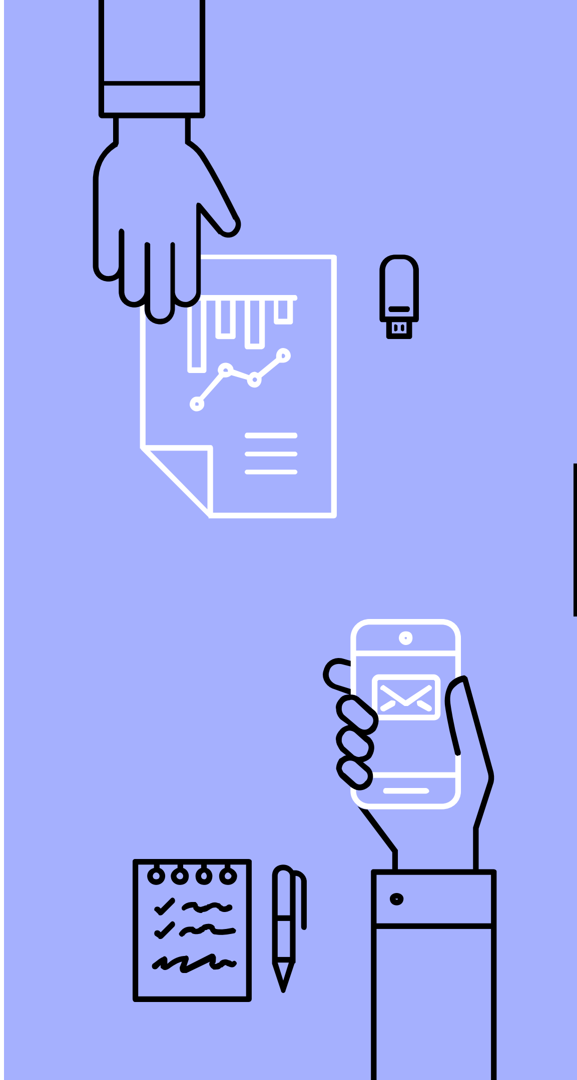
- A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities

- The pen testing process can be broken down into five stages

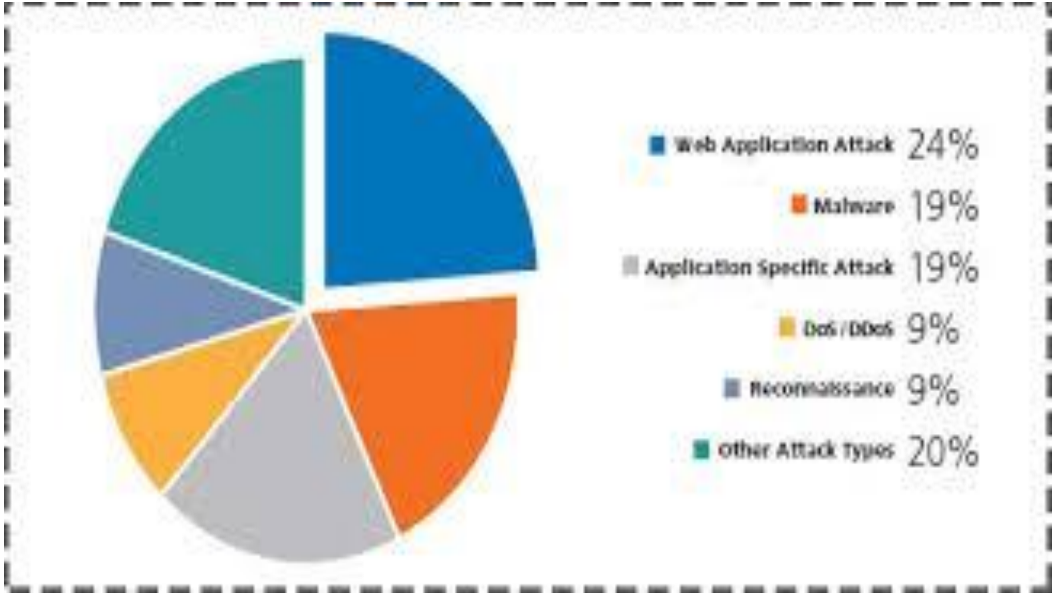


Robust Model of Security Process

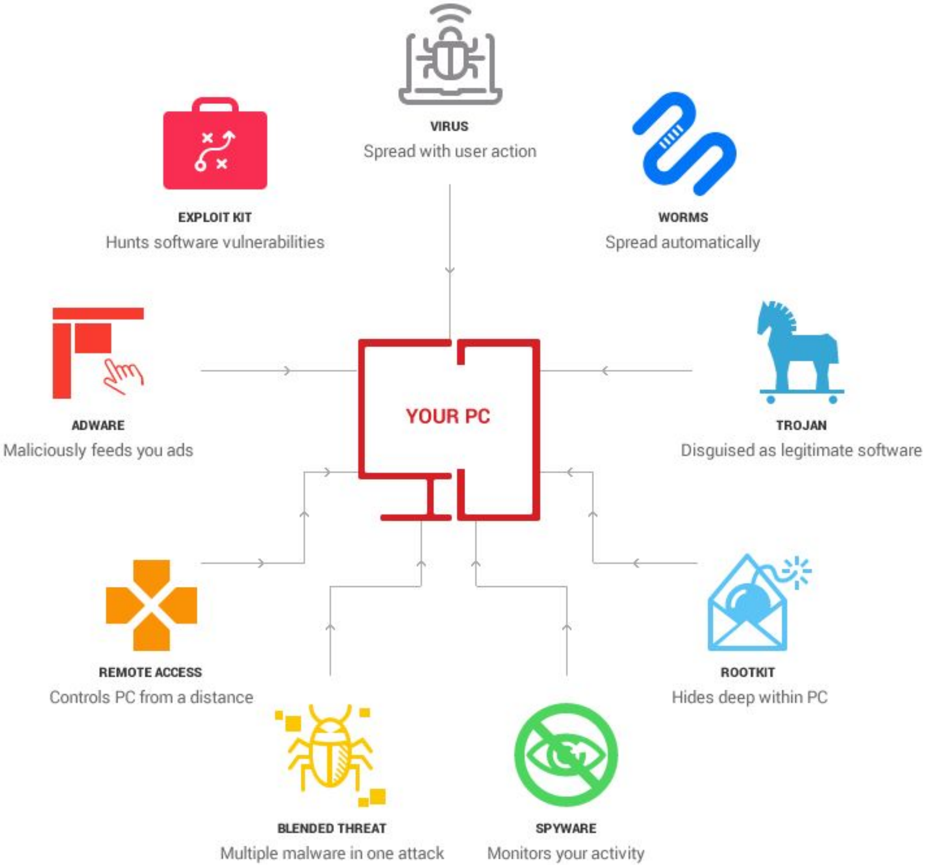


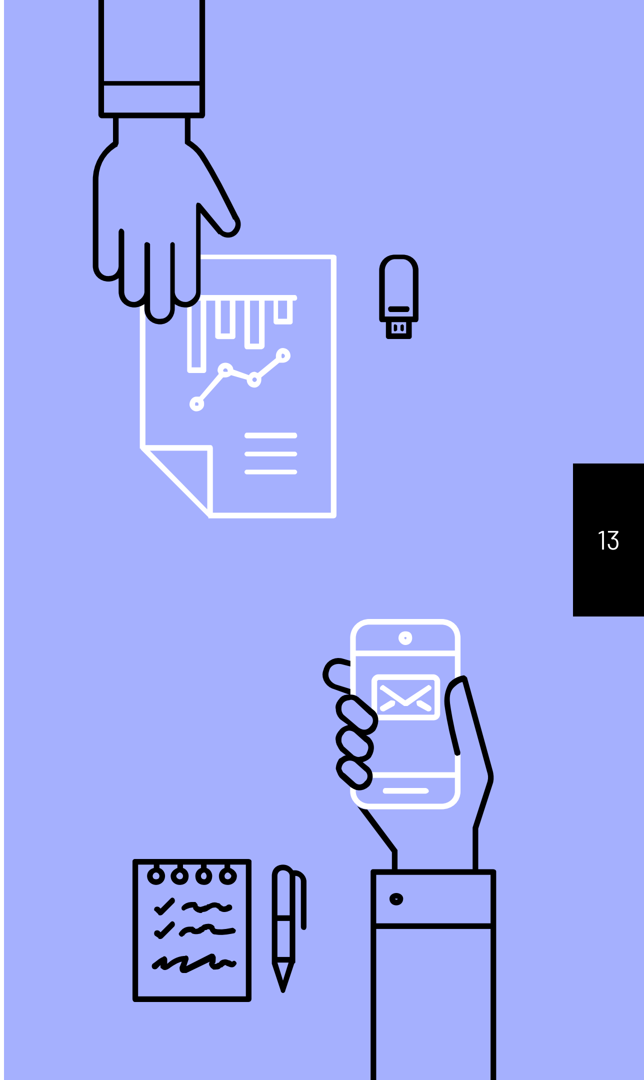


Types of Cyber Attacks



Types of Malwares

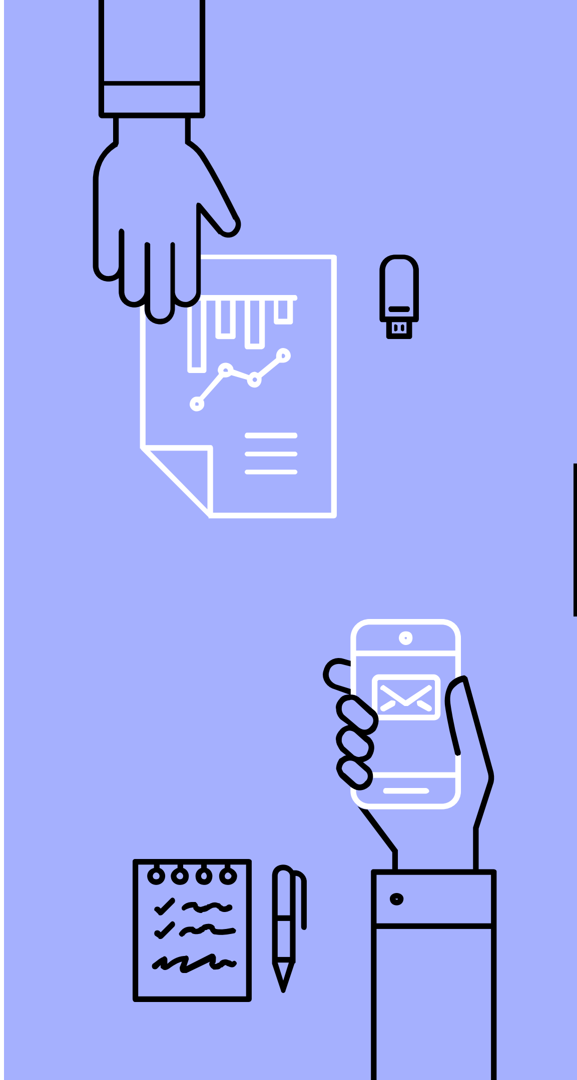




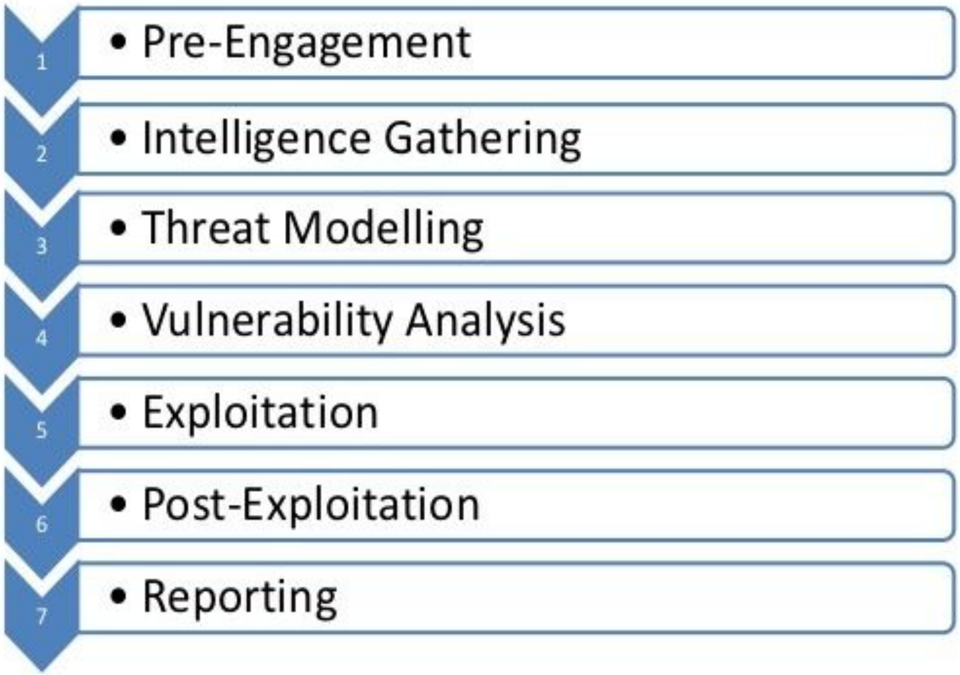
Hack in Different Styles

The initial step for VAPT referred as modes of testing are of three styles:

1. BlackBox Testing
2. Gray Box Testing
3. White Box Testing



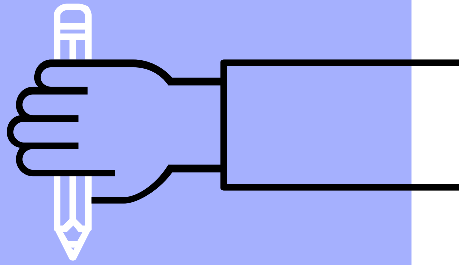
Process Flow of VAPT



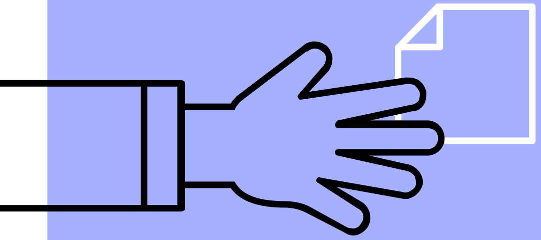
1. Pre-Engagement
2. Intelligence Gathering
3. Threat Modelling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

Understanding VAPT

Phase 1



Pre-Engagement

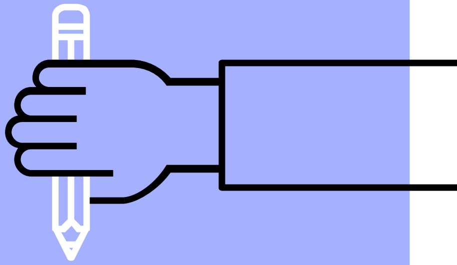


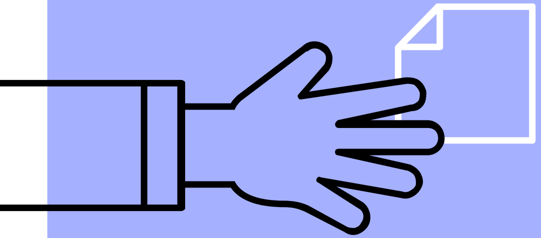
Pre-Engagement

- Introduction to Scope
- Metrics for Time Estimation
- Scoping Meeting
- Additional Support Based on Hourly Rate
- Questionnaires
- General Questions
  - Network Penetration Test
  - Web Application Penetration Test
  - Wireless Network Penetration Test
  - Physical Penetration Test
  - Social Engineering
  - Questions for Business Unit Managers
  - Questions for Systems Administrators

Phase 2

Intelligence Gathering





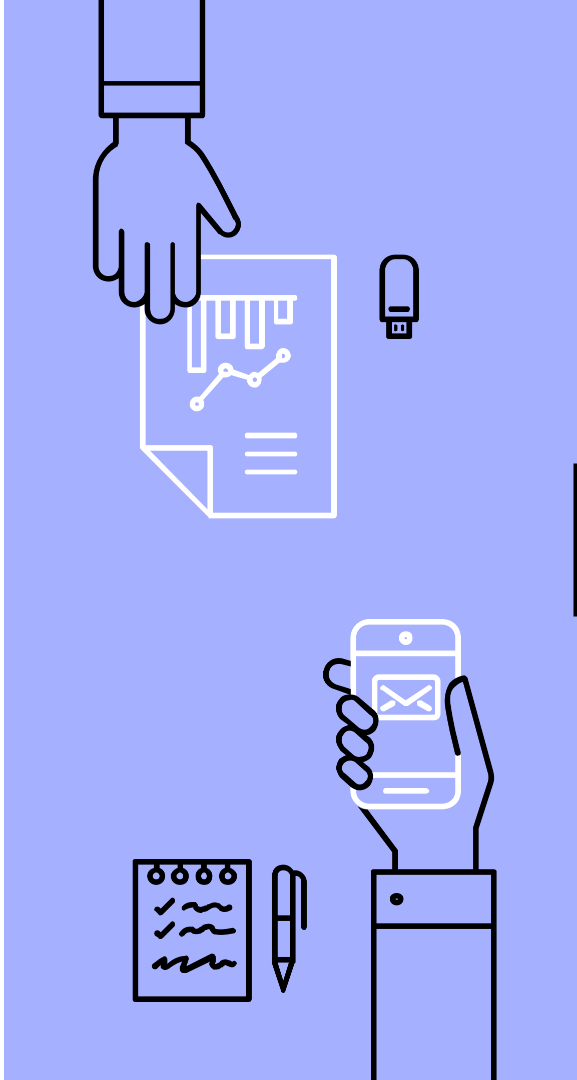
Intelligence Gathering

- Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible

- The information gathered can be utilized when penetrating the target during the vulnerability assessment and exploitation phases

- The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future

- VAPT always needs to begin with an extensive Information Gathering phase



Intelligence Gathering

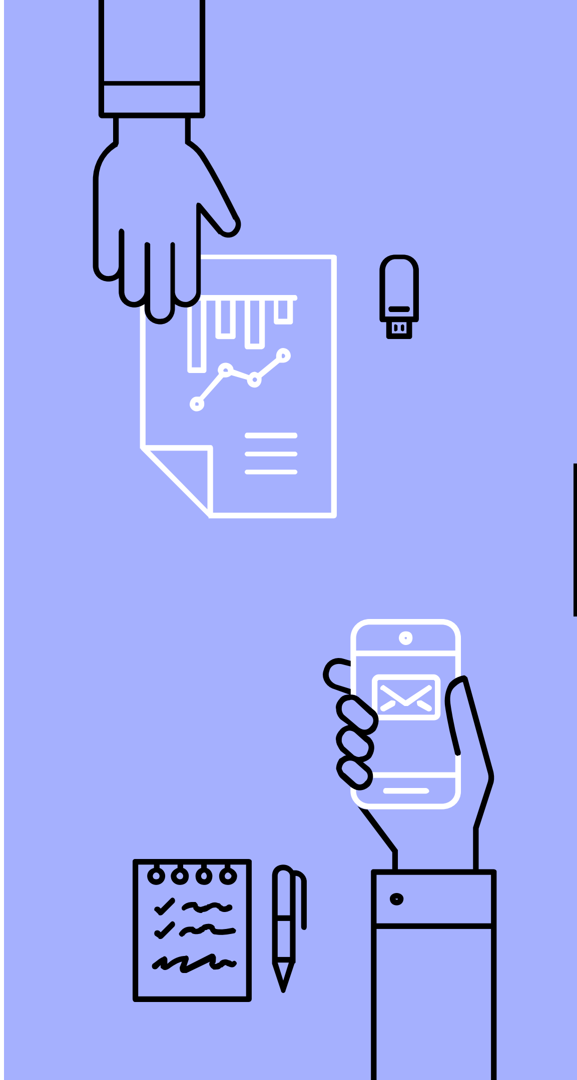
Two types:

- ❖ Active Intelligence Gathering

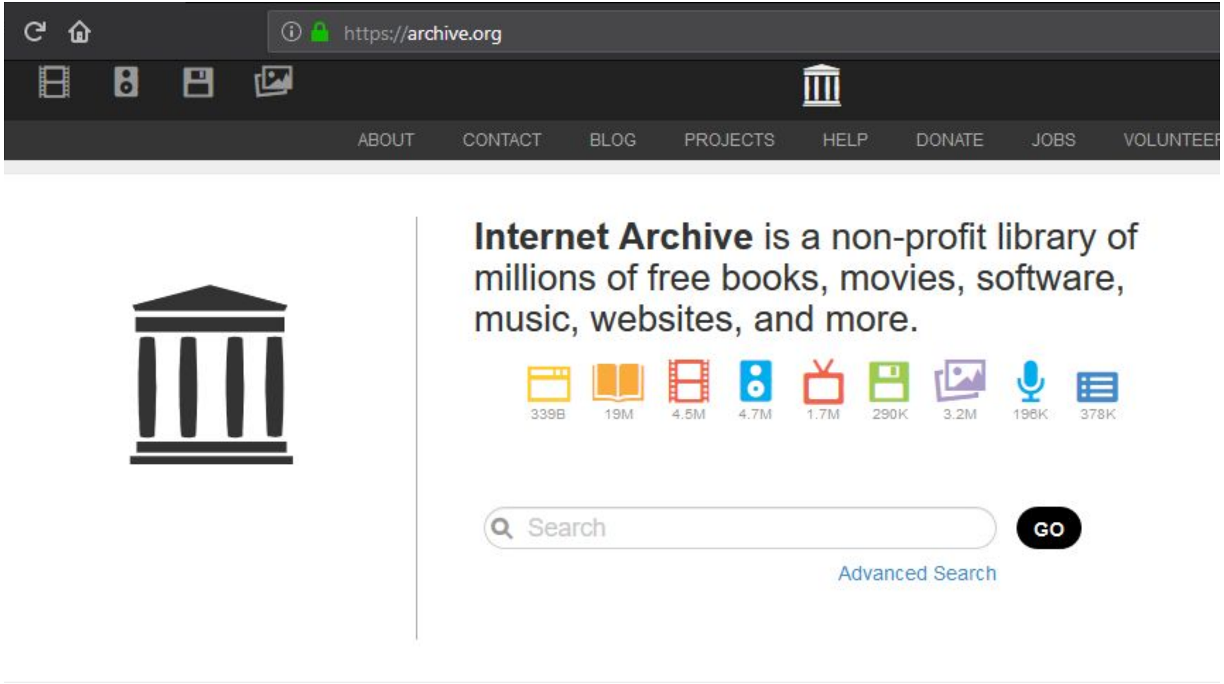
Type of computer attack in which an intruder engages with the targeted system to gather information about the target

- ❖ Passive Intelligence Gathering

Gathering as much information as possible without establishing contact with the target



Archive.org



Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

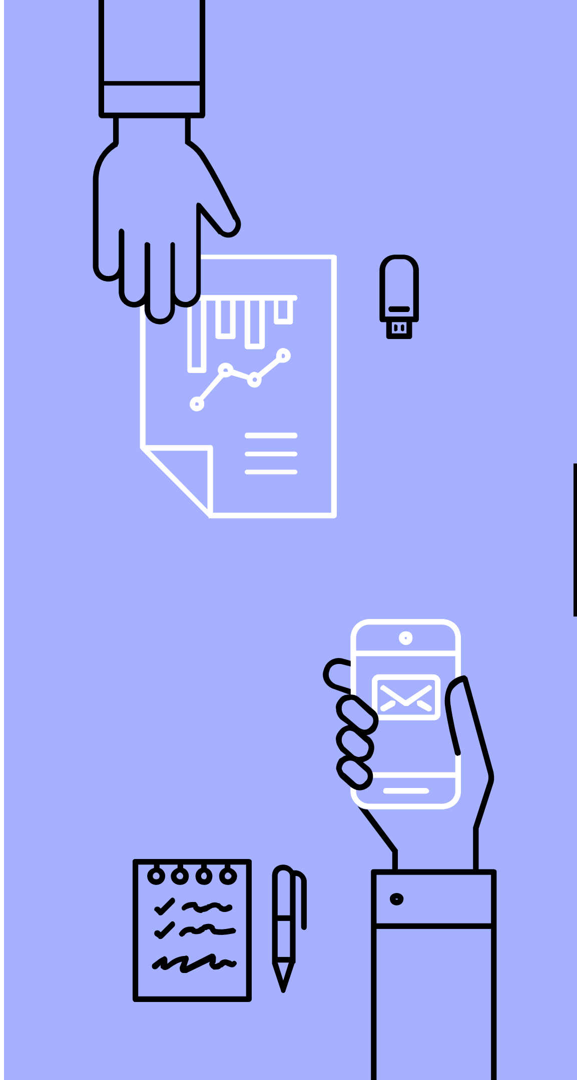
WHOIS - A Domain Tool

- A domain is tool consist of target information of gateway, email, phone number & lots more

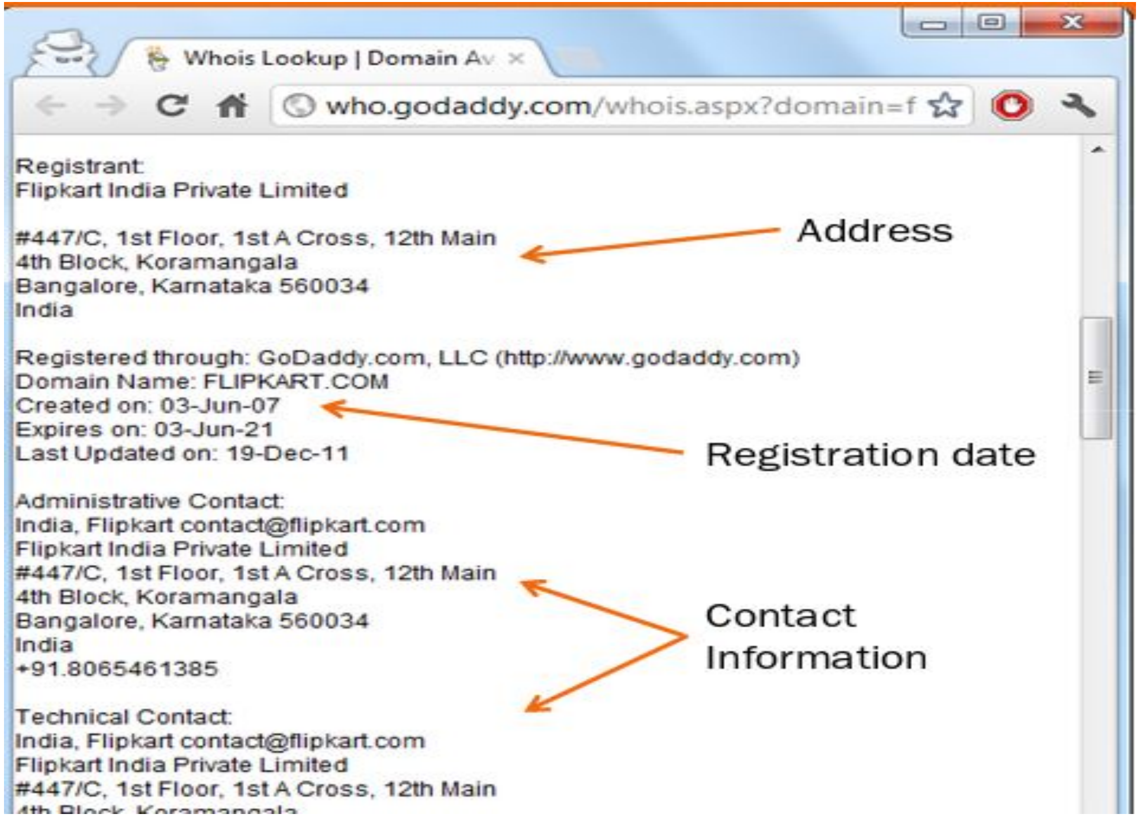
- This information is available publically. There are few examples for the same

- builtwith.com — Use BuiltWith to know the technology stack of any website. It helps you figure out the mail service provider of a domain, the advertising partners, the tracking widgets that are installed on a website and whether the site is using any CDN like Amazon S3 or Google Cloud

- ewhois.com — Ewhois, short for enhanced whois lookup, will help you determine other websites of someone. It looks the whois details, the AdSense publisher ID and the Google Analytics code of websites to figure out other web domain that may belong to the same owner



Examples



Registrant:
Flipkart India Private Limited

#447/C, 1st Floor, 1st A Cross, 12th Main
4th Block, Koramangala
Bangalore, Karnataka 560034
India

Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
Domain Name: FLIPKART.COM
Created on: 03-Jun-07
Expires on: 03-Jun-21
Last Updated on: 19-Dec-11

Administrative Contact:
India, Flipkart contact@flipkart.com
Flipkart India Private Limited
#447/C, 1st Floor, 1st A Cross, 12th Main
4th Block, Koramangala
Bangalore, Karnataka 560034
India
+91.8065461385

Technical Contact:
India, Flipkart contact@flipkart.com
Flipkart India Private Limited
#447/C, 1st Floor, 1st A Cross, 12th Main
4th Block, Koramangala

Intelligence Gathering

Social Engineering Attacks:

- It is a manipulation techniques that hackers use to trick their way into secured networks and systems

- **Attacks:**

  - Emails From Trusted Source
  - Phishing Scams
  - Baiting Scenarios
  - Pre-texting Scammers

Intelligence Gathering

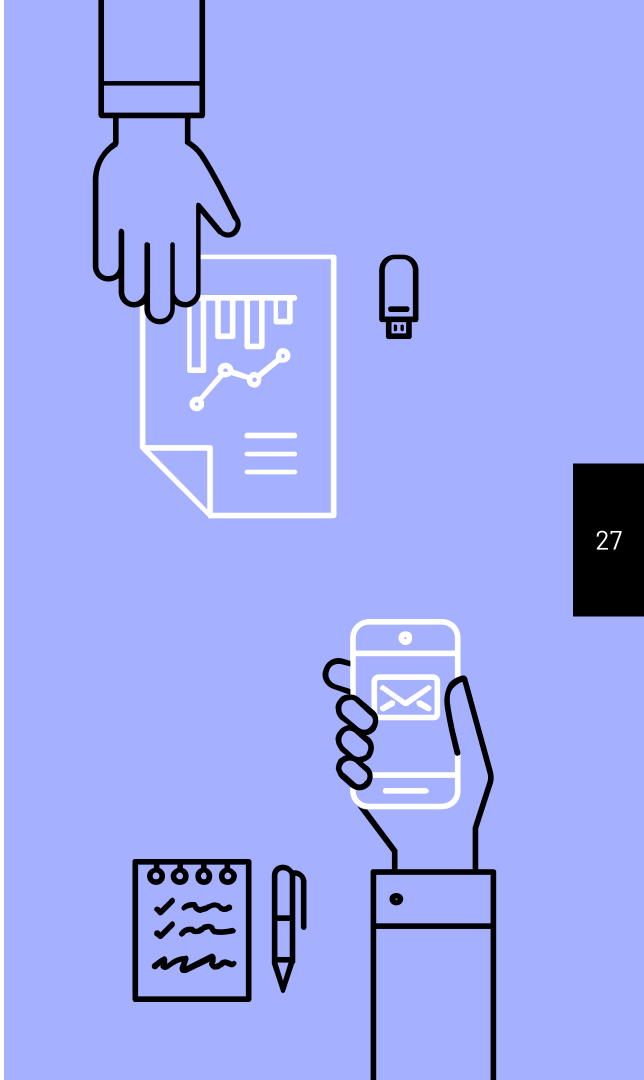
And I can't remember what email address
we used to log on to the account,
and the baby's crying-

Intelligence Gathering

OSINT

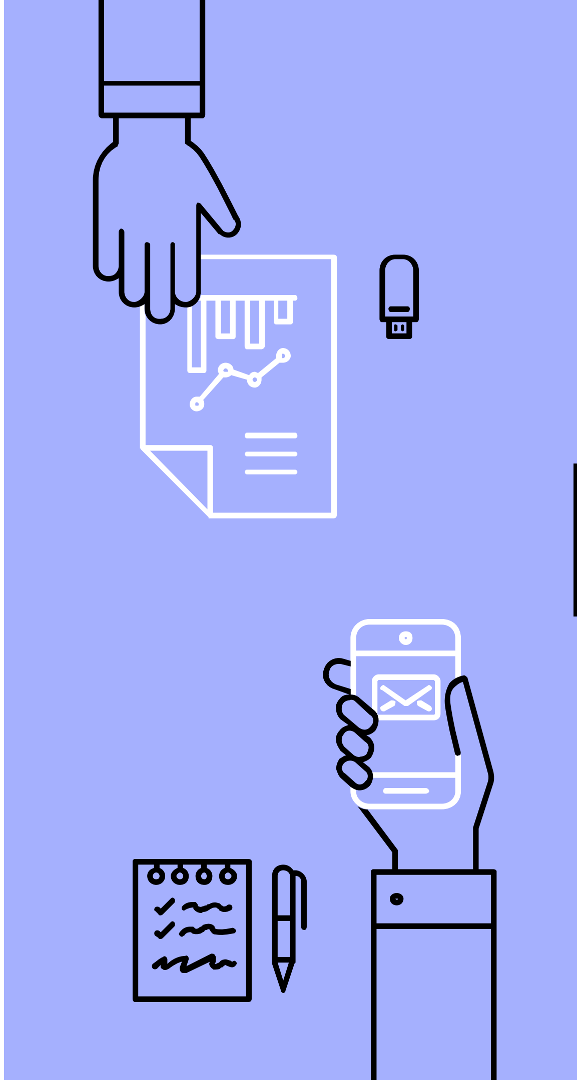
- Collection of data from public sources
- This type of information is often missed by link crawling search engines such as Google
- Top 5 tools:

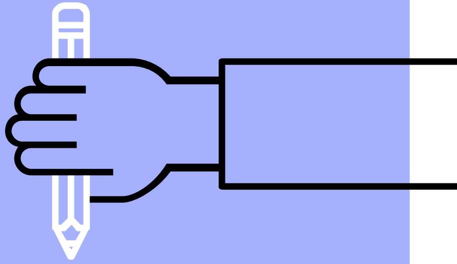
    - Maltego
    - Recon-ng
    - The Harvester
    - Shodan
    - Google Dorks



Social Engineering Toolkit

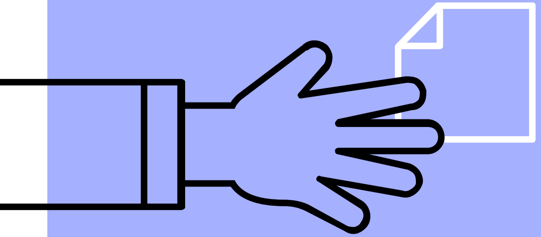
- Open source Python-based tool
- Aimed at penetration testing around Social Engineering
- SET has been discussed and presented at conferences including DerbyCon, Defcon, ShmooCon and Blackhat





Phase 3

Threat Modelling

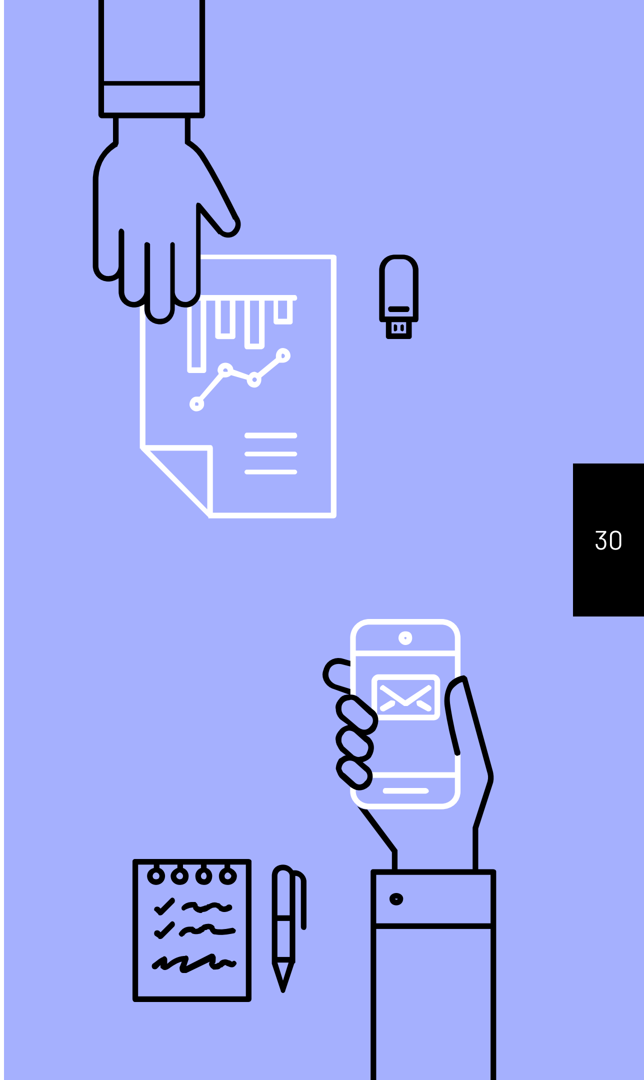


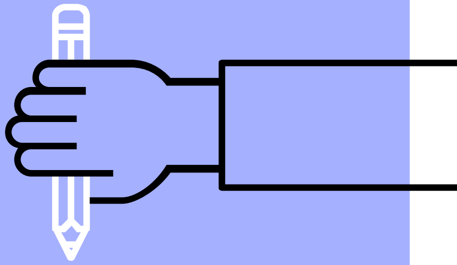
Threat Modelling

- A threat model is essentially a structured representation of all the information that affects the security of an application

- In essence, it is a view of the application and its environment through security glasses

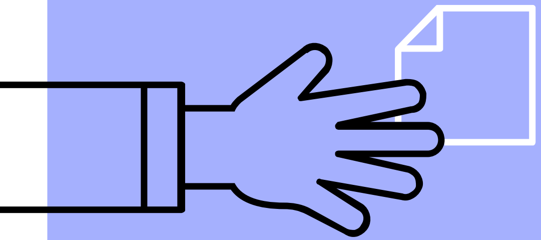
- Threat modeling is a process for capturing, organizing, and analyzing all of this information





Phase 4

Vulnerability Analysis

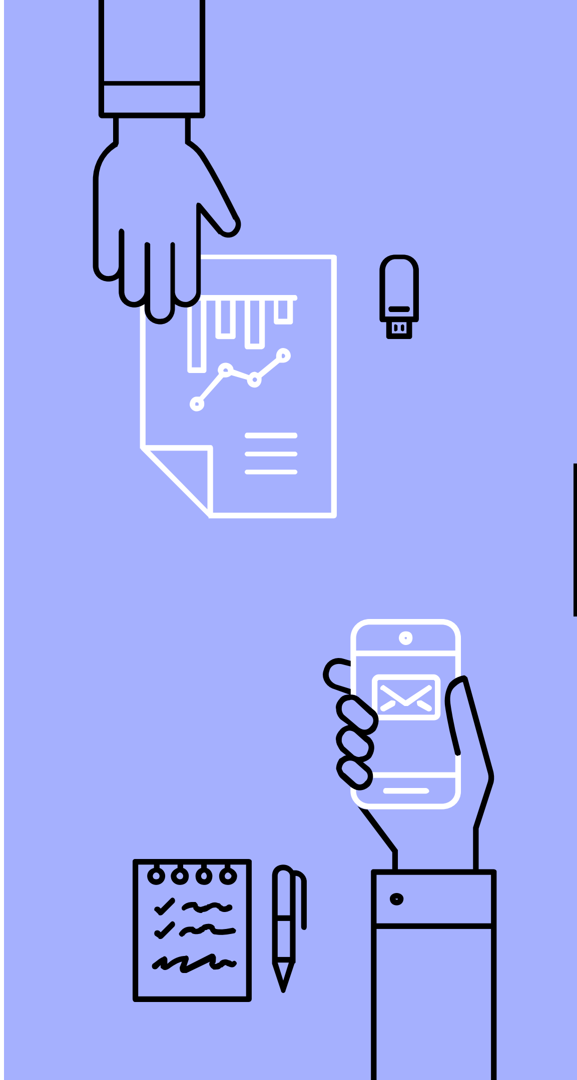


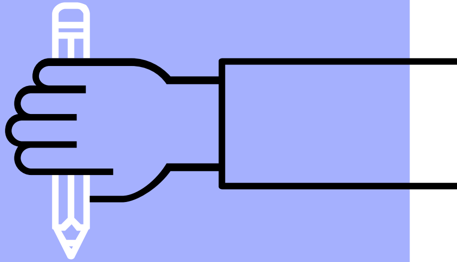
Vulnerability Analysis

- Vulnerability Analysis is also termed as Vulnerability Assessment

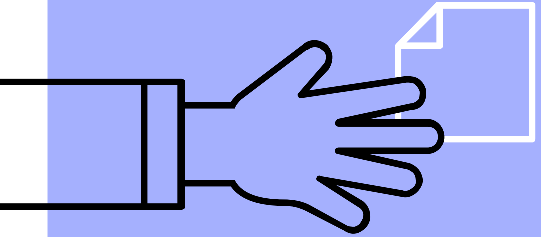
- The method of recognizing, categorizing and characterizing the security holes (called as vulnerabilities) among the network infrastructure, computers, hardware system and software etc is known as Vulnerability Analysis

- Example: misconfiguration of components, a defect or error in an operating system, any ambiguity in a marketable product etc



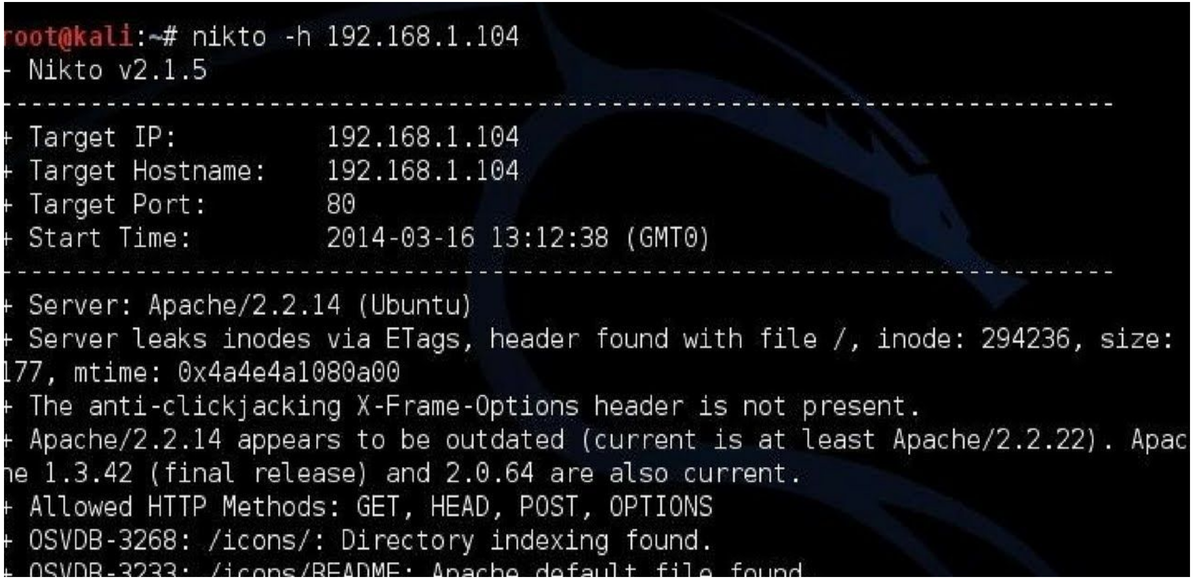


Demo



Nikto

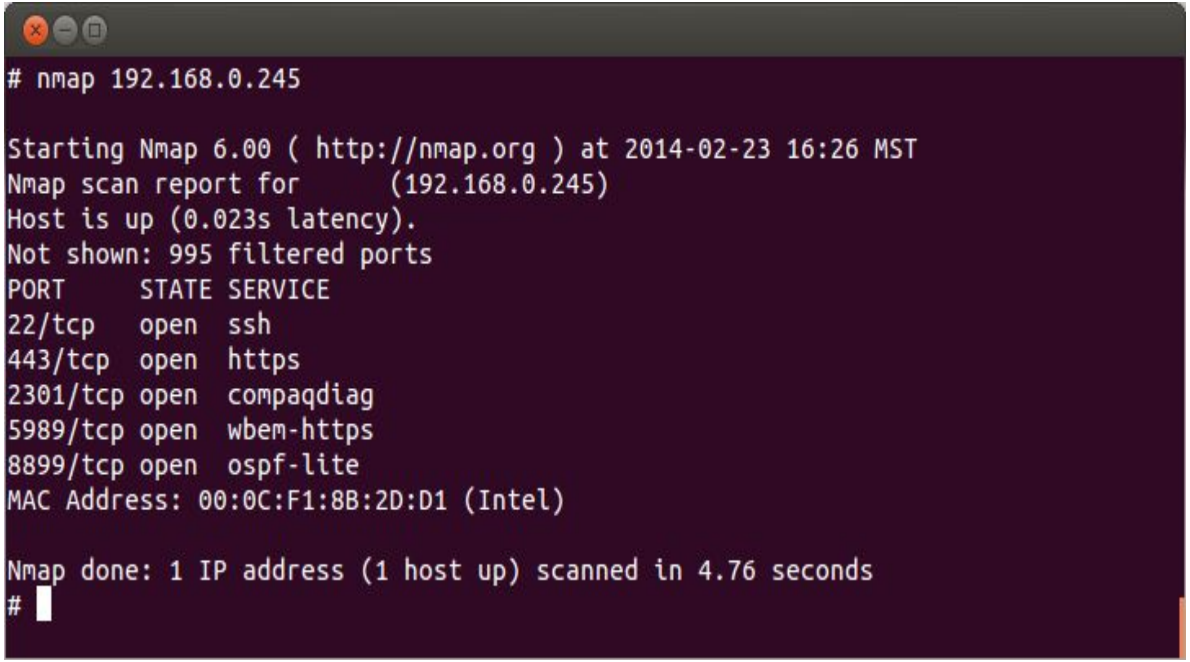
Nikto Web Scanner is a **Web server scanner** that tests web servers for dangerous files/CGIs, outdated server software and other problems



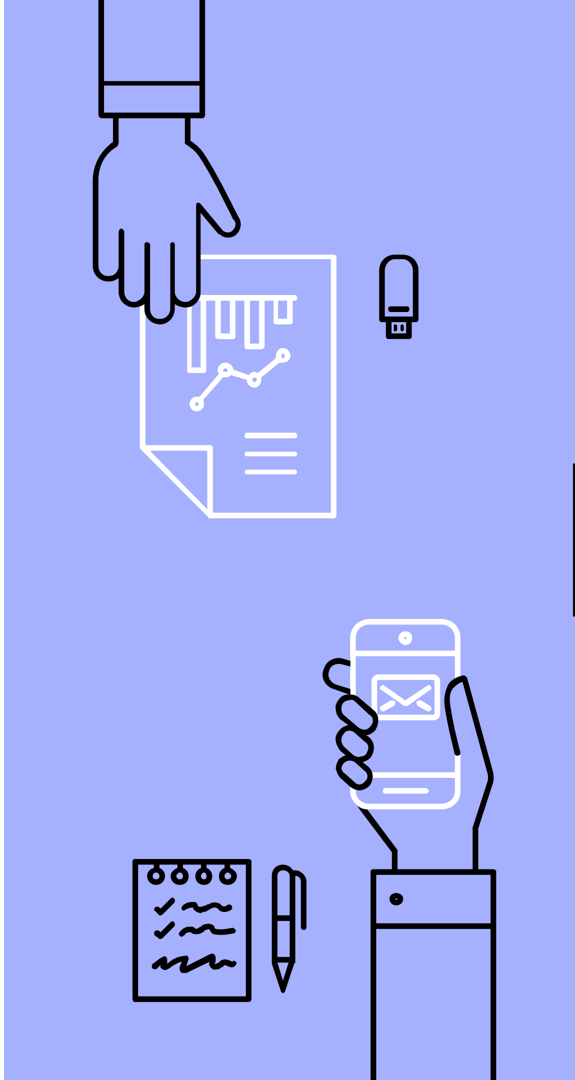
```
root@kali:~# nikto -h 192.168.1.104
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.104
+ Target Hostname:    192.168.1.104
+ Target Port:        80
+ Start Time:         2014-03-16 13:12:38 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 294236, size:
177, mtime: 0x4a4e4a1080a00
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.22). Apac
he 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
```

Nmap

Nmap (Network Mapper) is a free and open-source security scanner

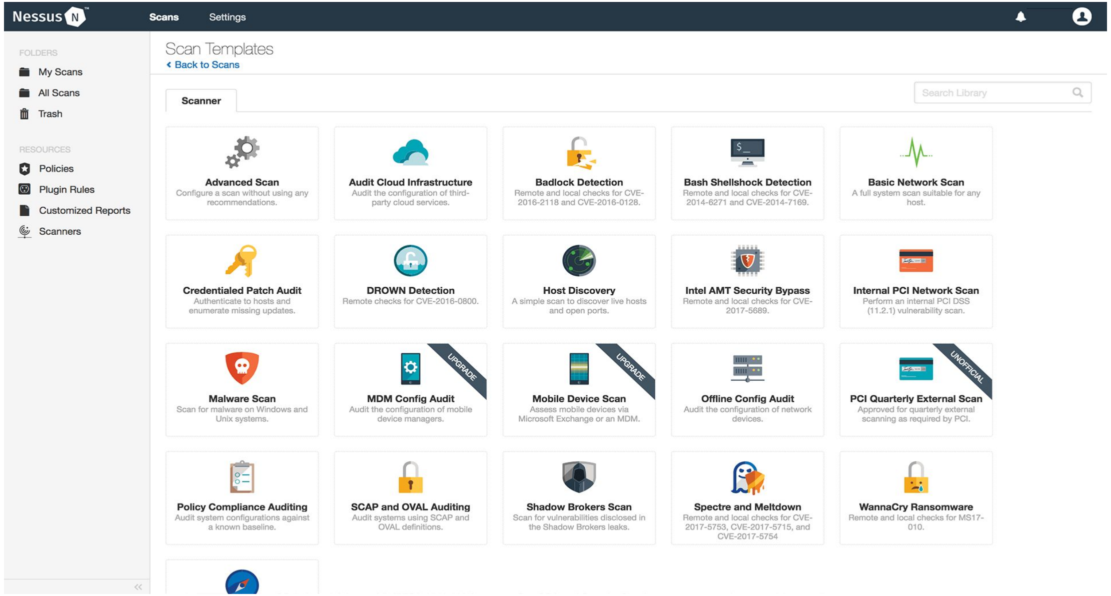


```
# nmap 192.168.0.245

Starting Nmap 6.00 ( http://nmap.org ) at 2014-02-23 16:26 MST
Nmap scan report for      (192.168.0.245)
Host is up (0.023s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
443/tcp  open  https
2301/tcp open  compaqdiag
5989/tcp open  wbem-https
8899/tcp open  ospf-lite
MAC Address: 00:0C:F1:8B:2D:D1 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
# 
```



Nessus

- Nessus is a proprietary vulnerability scanner developed by Tenable Network Security
- It is free of charge for personal use in a non-enterprise environment



Scan Templates

‹ Back to Scans

Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

MDM Config Audit
Audit the configuration of mobile device managers.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

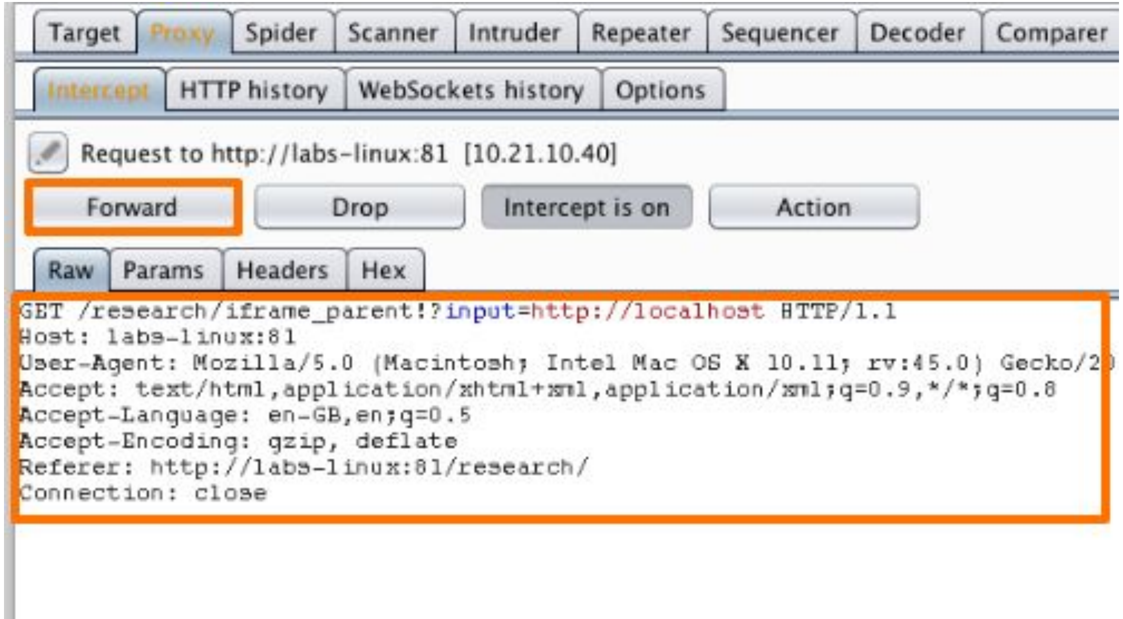
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Burp Suite

- Burp or Burp Suite is a graphical tool for testing Web application security
- We can intercept, tamper, scan web requests using Burp Suite and much more

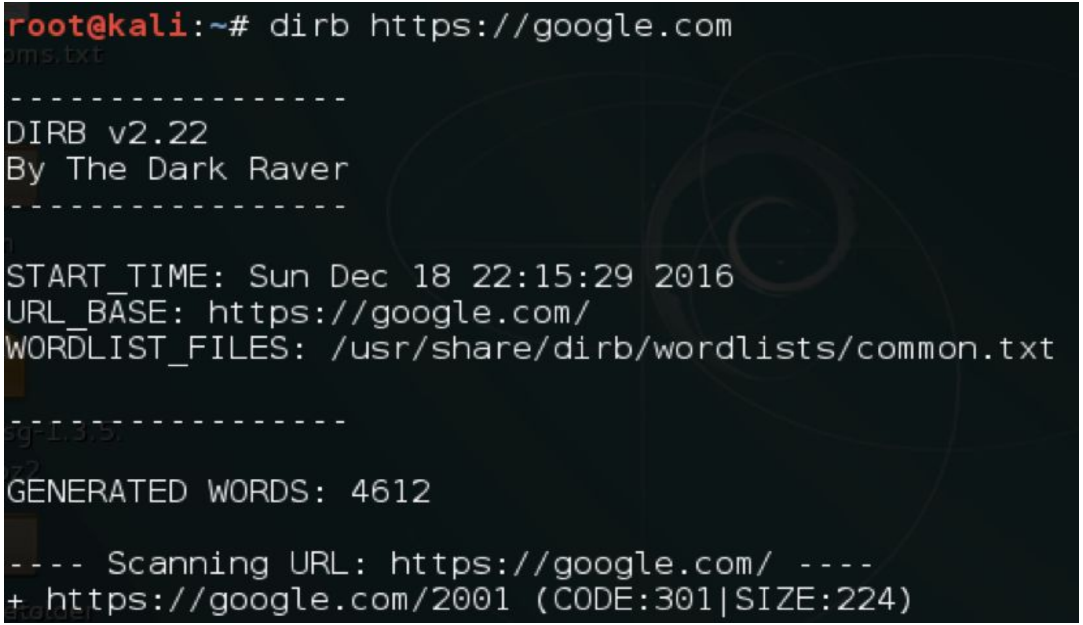


Request to http://labs-linux:81 [10.21.10.40]

```
GET /research/iframe_parent!?input=http://localhost HTTP/1.1
Host: labs-linux:81
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:45.0) Gecko/2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://labs-linux:81/research/
Connection: close
```

Dirb

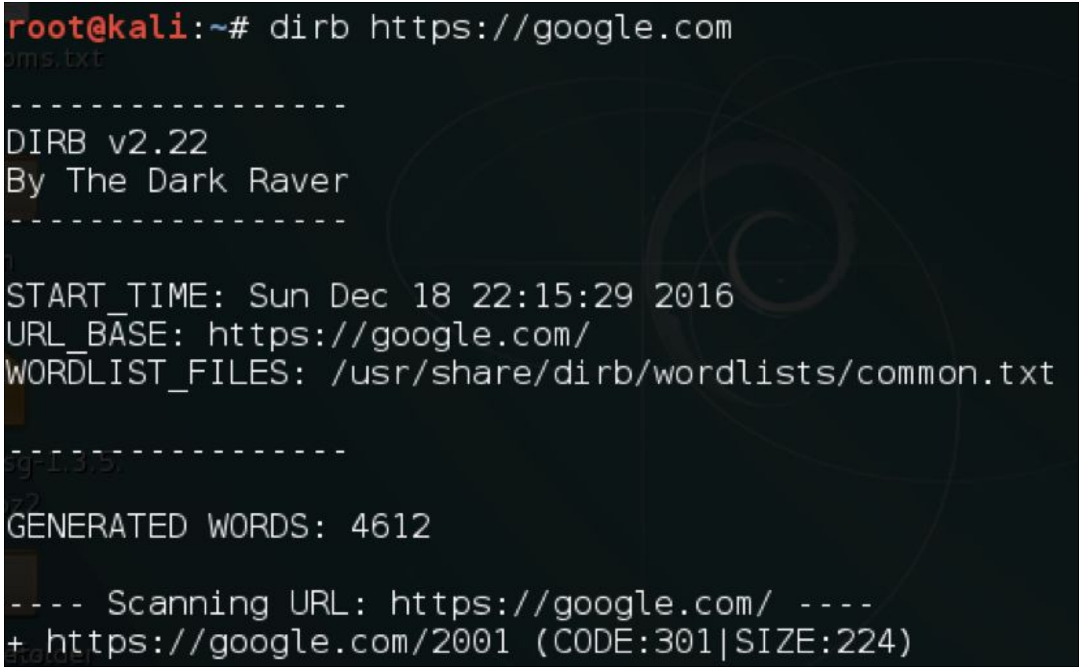
- DIRB is a Web Content Scanner. It looks for existing (and/or hidden) web objects
- It basically works by launching a dictionary based attack against a web server



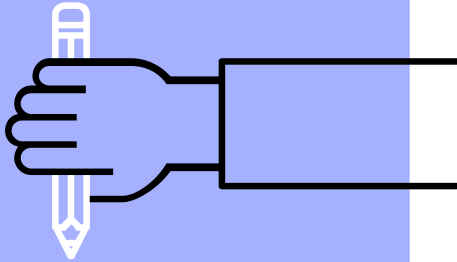
```
root@kali:~# dirb https://google.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 18 22:15:29 2016
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://google.com/ ----
+ https://google.com/2001 (CODE:301|SIZE:224)
```

Searchsploit

A command line search tool for Exploit-DB that also allows you to take a copy of Exploit Database

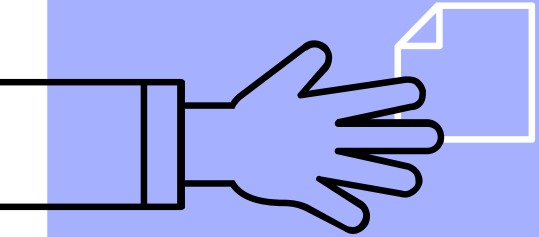


```
root@kali:~# dirb https://google.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 18 22:15:29 2016
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://google.com/ ----
+ https://google.com/2001 (CODE:301|SIZE:224)
```



Phase 5

Exploitation

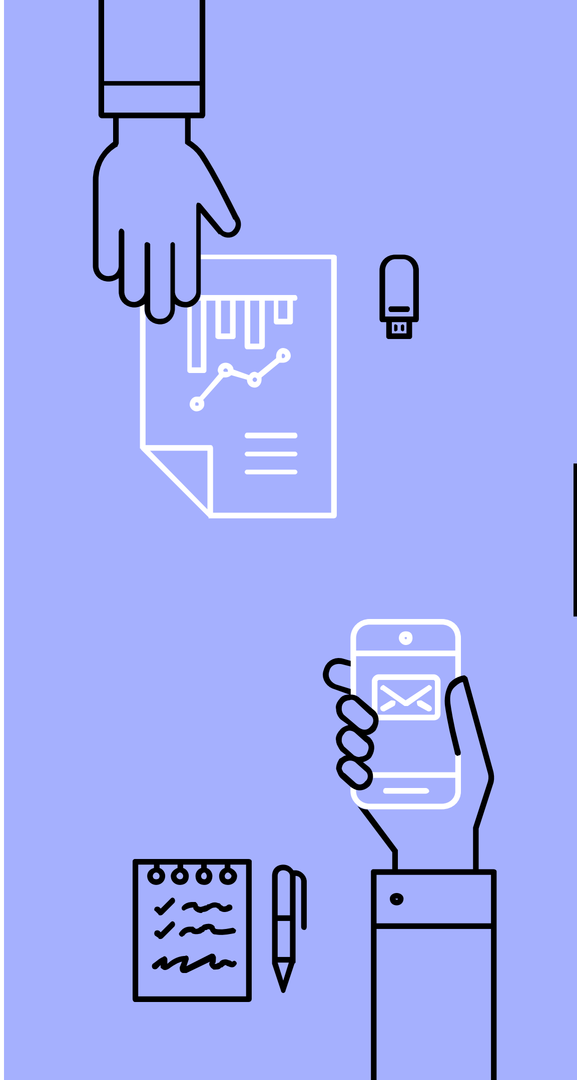


Exploitation

- Establishing access to a system or resource by bypassing security restrictions is known as exploitation

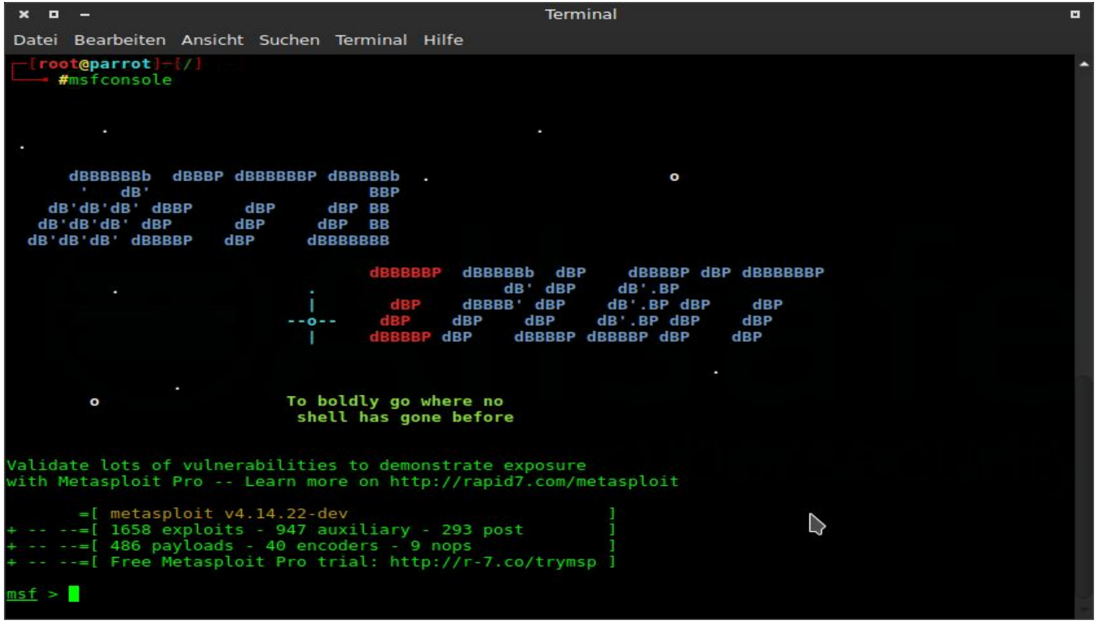
- If vulnerability analysis was performed properly, exploitation should be well planned and a precision strike

- The main focus is to identify the main entry point into the organization and to identify high value target assets

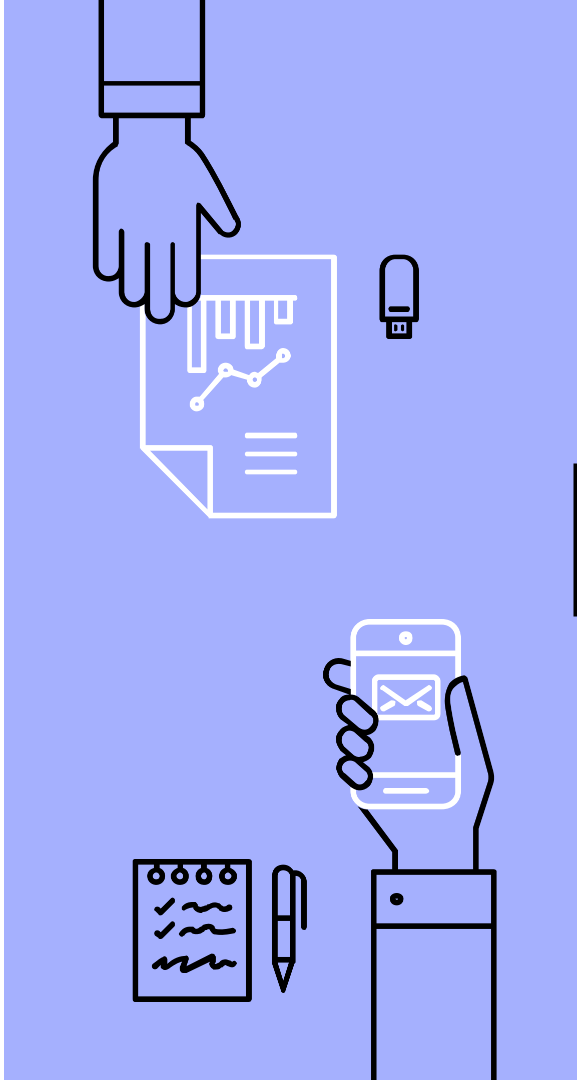


Metasploit

Metasploit can be used to test the vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems



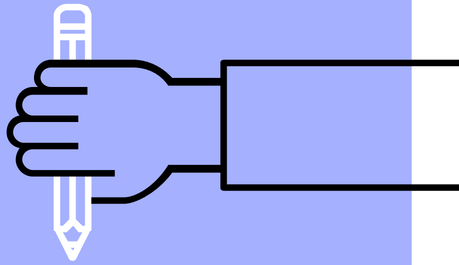
```
┌─[root@parrot]─[/]
└──╼ #msfconsole


         .                                          .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.14.22-dev                         ]
+ -- --=[ 1658 exploits - 947 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```



Metasploit

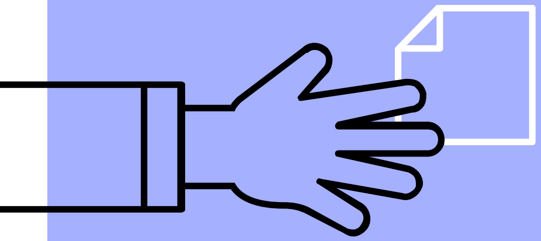
- It is a powerful tool used for penetration testing
- Basic steps to break into a system using metasploit after gathering some information about the target system:

  - Select a right exploit and then set the target
  - Verify the exploit options to determine whether the target system is vulnerable to the exploit
  - Select a payload
  - Execute the exploit



Phase 6

Post Exploitation

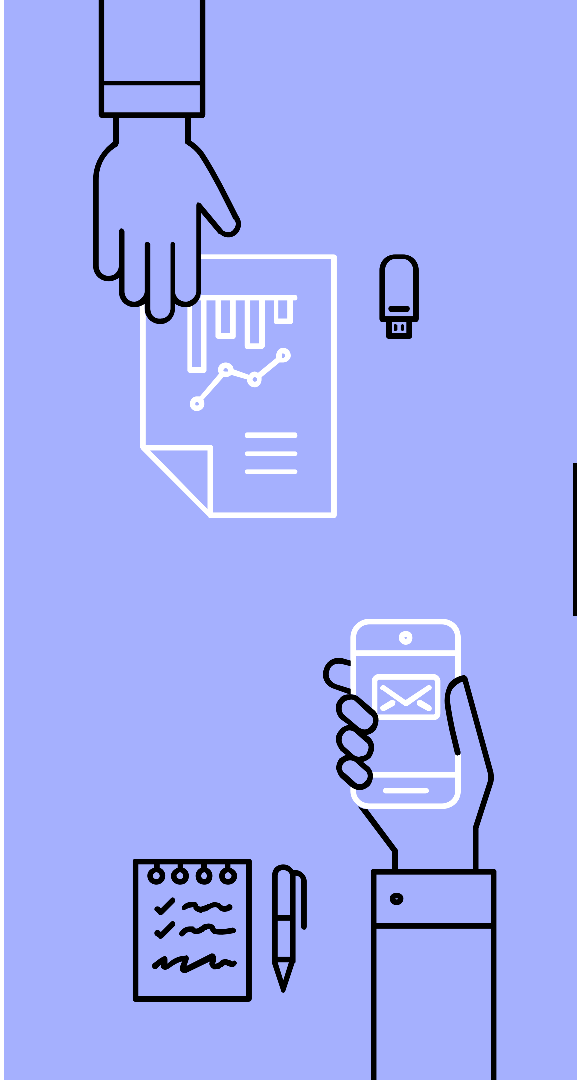


Post Exploitation

- This phase determines the value of the machine compromised and maintain control of the machine for later use.

- The value of the machine is determined by:
  - The sensitivity of the data stored on it
  - The machines usefulness in further compromising the network.

- Processes
  - Privilege Escalation
  - Opening Backdoors
  - Dumping Passwords
  - Data Exfiltration
  - Cleanup

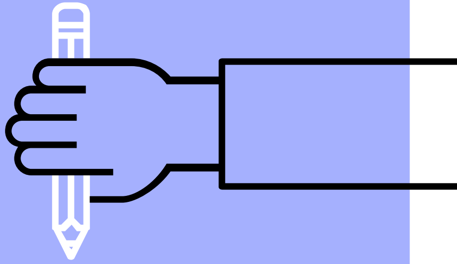


Privilege Escalation

- Privilege describes the rights of users a system have been granted to perform a particular action.

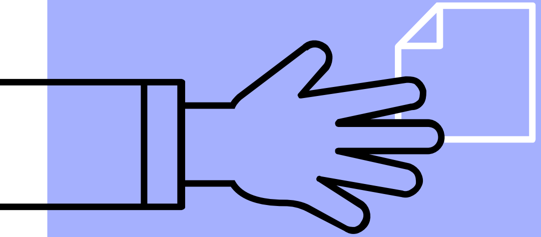
- Privilege escalation is using programming errors and weaknesses of the system to achieve a greater and higher level of access to the system.

- Tools:
  - SearchSploit
  - Metasploit Post Exploitation Module



Phase 7

Reporting



Reporting

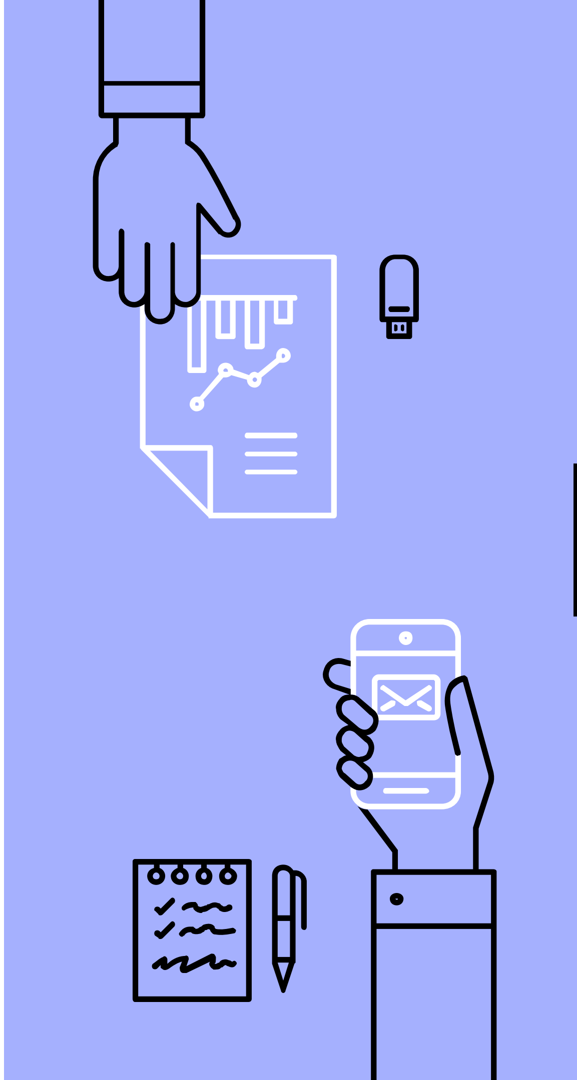
- ❖ **Report Structure**

The report is broken down into two (2) major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences

- ❖ **The Executive Summary**

The intended audience will be those who are in charge of the oversight and strategic vision of the security program

  - ■ Background
  - ■ Overall Posture
  - ■ Risk Ranking/Profile
  - ■ General Findings
  - ■ Recommendation Summary
  - ■ Strategic Roadmap



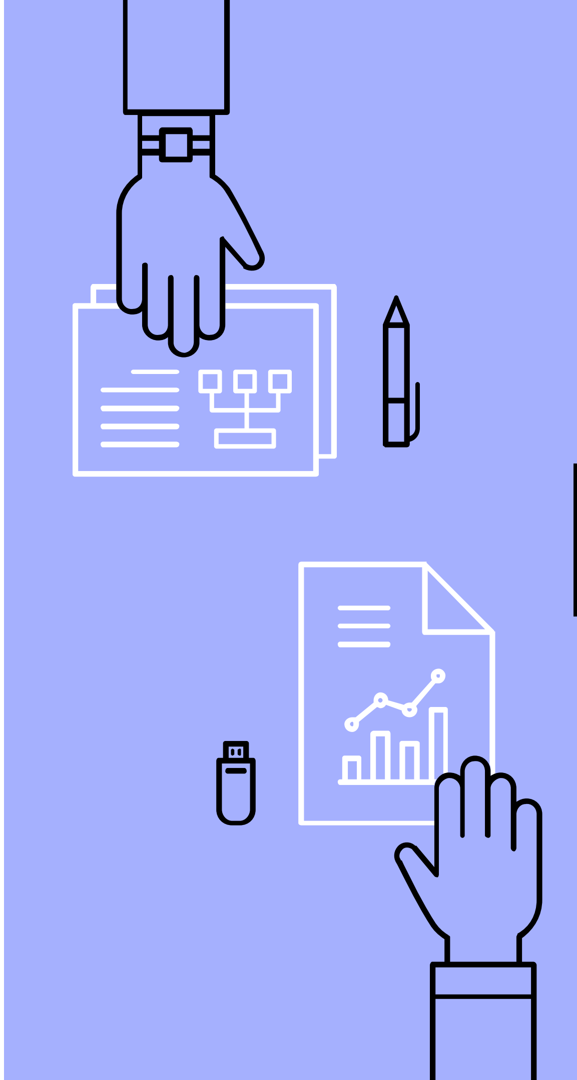
Reporting

- **Technical Report**

  The technical report section will describe in detail the scope, information, attack path, impact and remediation suggestions of the test

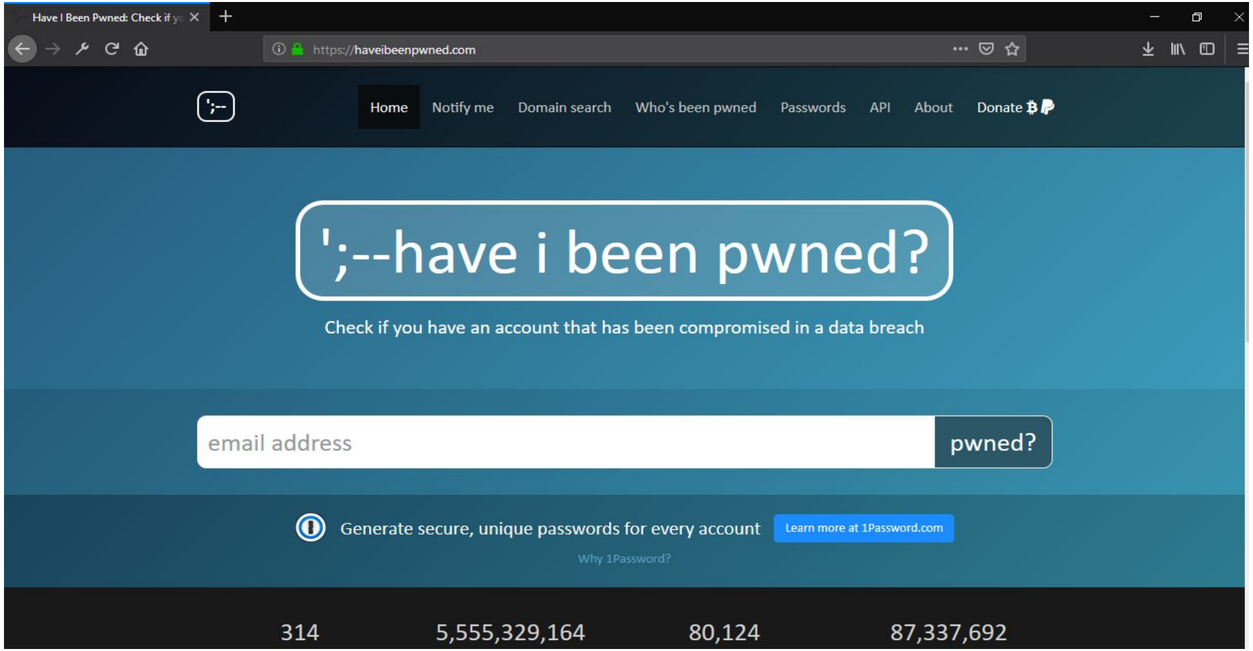
Cyber Security Best Practices

- Use a firewall
- Document your cybersecurity policies
- Plan for mobile devices
- Educate all employees
- Enforce safe password practices
- Regularly backup all data
- Install anti-malware software
- Use multifactor identification



Haveibeenpwned

A website that allows internet users to check if their personal data has been compromised by data breaches

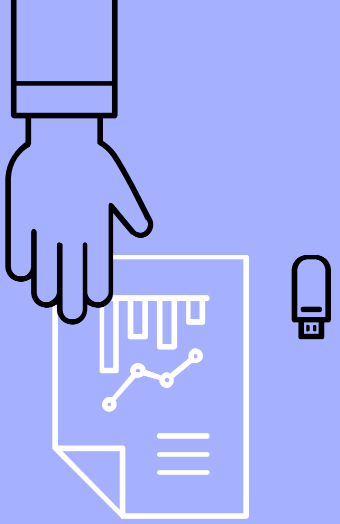


';--have i been pwned?

Check if you have an account that has been compromised in a data breach

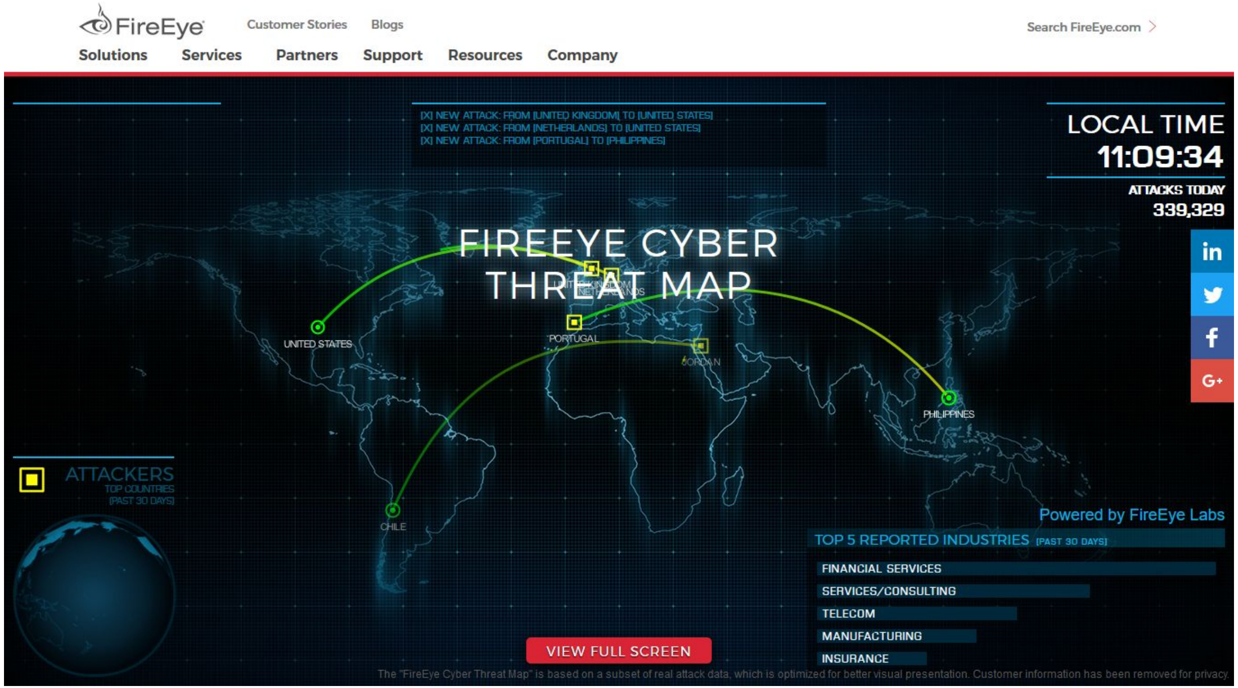
Generate secure, unique passwords for every account

314 5,555,329,164 80,124 87,337,692



Cyber Threat Map

A Cyber Threat Map gives information on major cyber attacks as they're discovered



[X] NEW ATTACK: FROM [UNITED KINGDOM] TO [UNITED STATES]
[X] NEW ATTACK: FROM [NETHERLANDS] TO [UNITED STATES]
[X] NEW ATTACK: FROM [PORTUGAL] TO [PHILIPPINES]

LOCAL TIME
11:09:34

ATTACKS TODAY
339,329

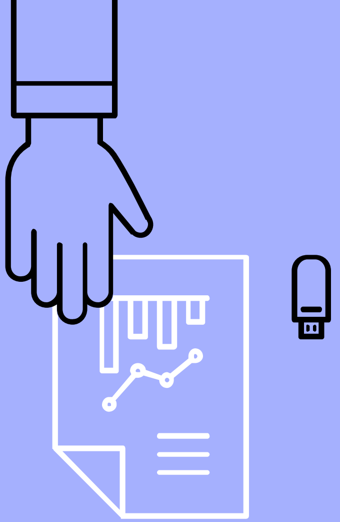
ATTACKERS
TOP COUNTRIES
[PAST 30 DAYS]

Powered by FireEye Labs

TOP 5 REPORTED INDUSTRIES [PAST 30 DAYS]

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

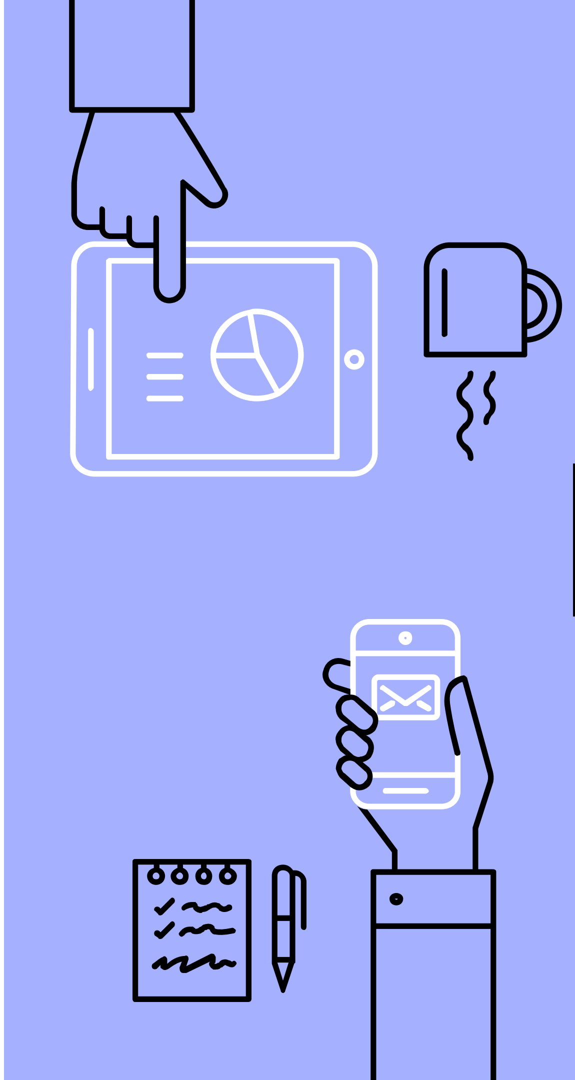


References

- SANS GPEN 560 notes

- Hack I.T, Security Through Penetration Testing Penetration Testing Penetration Testing Penetration Testing, by T.J Klevinksy

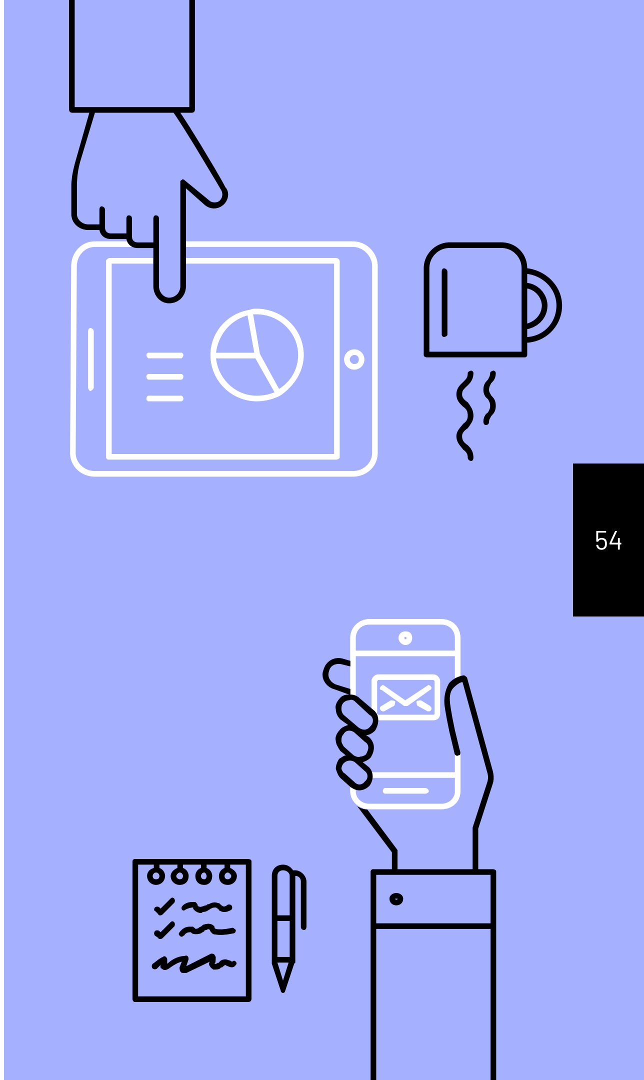
- http://www.pentest-standard.org/index.php/Main_Page



Thank You

Let us stay connected:

- **Twitter**: @kharbanda_manan
- **Email**: manan.k@lucideustech.com



Let’s Talk!