Research Methodology

Pradeep Nagaraj

1140698

Date:

Research Methodology - COMP 5118

Research Journal

Date:

Table of contents

Date:

Date: 29/05/21

Cyber Security:

↳ is the protection of computer systems & networks from information disclosure, theft of or damage to their h/w, s/w or electronic data as well as from the disruption or misdirection of the service they provide.

Challenges:

-> N/w security - Protect unwanted users, attacks
-> Application security - app's need update to secure
-> Endpoint security - Remote access can be weak
-> Data security - Protecting information is a separate layer of security
-> identity management - understanding access of every individual in an organization

How cyber security different from Information security?

C.S -> Protect a computer system against unauthorized attacks or access

I.S -> To ensure business continuity & minimise damage by limiting the impact of security incidents. Preservation of confidentiality, integrity & availability of information.

Pg#: 1

Date:

Why cyber security intrested me?

↳ Nowadays everything is happening via internet from online banking, shopping transactions, including food & daily needs. same time many fraud's are happening online. Need to find how they are able to find loopholes to steal our personal record.

02/06/21 - Hacking

Process of identifying & exploiting weak links in computer systems or n/w's in order to obtain unauthorized access to data or modify the features of target computer or networks.

Methods / Steps

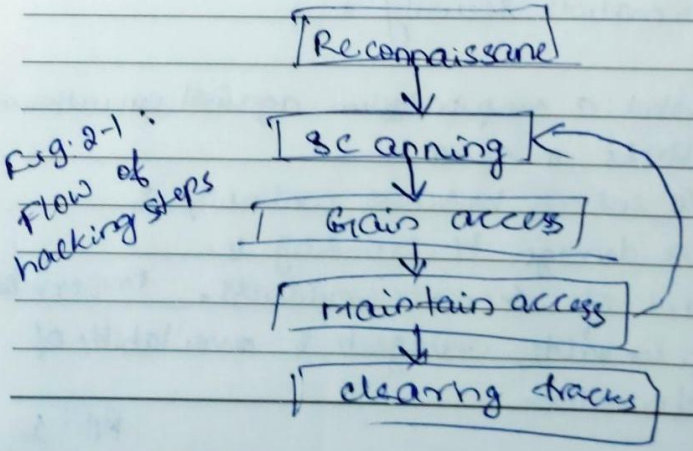


Fig: 2-1: Flow of hacking steps

Date:

⇒ Reconnaissance - gather requd information
⇒ Scanning - with collected data, make blue print to target the system
⇒ gain access - actual hacking step where hacker enters the system
⇒ Maintaining access: Tgd is important to maintain the access, also make some security changes to not get kicked out
⇒ clearing tracks - remove all sorts of finger print from being caught.

Types of hackers:

① Black hat - breaks into someone system without authorization with evil mind.

② White hat - "Good guy" - who breaks into & finds security vulnerabilities to fix them & improve security. They have certificates - CEC - certified ethical hacker.

③ Grey hat - Hybrid of above two. Have to be careful as they can change from white-hat to black hat anytime.

Date: 05-06-21

Ethical hacking:-

↳ a process of examining security flaws & identifying prospective security vulnerabilities for an Organisation in charge of I.T environment under attack.

↳ duplicating strategies of hackers.

↳ also called white hat hacking & penetration testing.

Q) When there are many ethical hackers, still why there is system hacks happening?

Q) What/how does ethical hackers help to keep system secure?

In 2017, database of zomato was hacked & accessed 5-key details - names, emails usernames, password, network user ID/ Mobile No. Ethical hacker was responsible for this breach, to draw company's attention to launch bug bounty programme.

↓

Vulnerability reward programme gets reward for reporting bugs.

Date: 06-06-21

What ethical hacker does?

Also known as penetration testing.

E.h / P.T helps to detect vulnerabilities, dangers & target environments in order to secure & take control of system.

Pentest ⇒ divided into 3 types

- White box test :-
  - ↳ tester will have complete information about system
  - ↳ less time consuming
- Grey box test :-
  - ↳ tester will have limited information
  - ↳ a bit time consuming than white box
- Black-box test :-
  - ↳ a tester will NO knowledge
  - ↳ More time consuming

08/06/21 Literature review

Topic 1: collaborative penetration testing & analysis toolkit (CPAT) [Jason, 2015]

- without pentest - network can fall victim to malicious mayhem
- team was able to perform pentest by utilizing existing network & tools.

Date:

- CAPT - means for security analysts to ensure a collaborative foundation for conducting pen testing.

Topic 2: A comprehensive tool [WR-3] that detects security flaws in network [Akash, 2010]

- discovers security issues in network
- solution is based on "N/W admin should try hacking their networks themselves before bad guys do."
- Big organisations do this but small companies can't afford, so WR-3 tool can be used to detect any possible network breach.

Topic 3: An automated approach to Vulnerability assessment & pen testing using Net-Nirikshak 1.0 [Shan, 2014]

- At IDRBT - a new automated VAPT testing named Net-Nirikshak 1.0 to detect vulnerabilities based on applications & services being used on target system.
- Also detects SQL injection vulnerabilities.

Date: 11-06-21

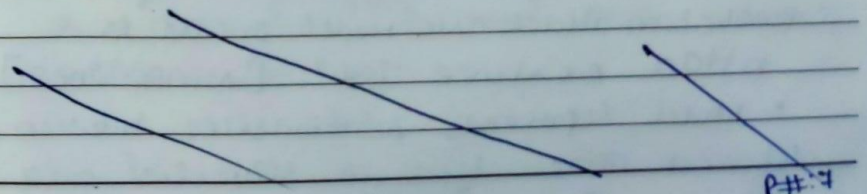
Topic 4: PENTOS [Visoothivich, 2017]

- Penetration testing tool for Internet of Things devices"
- helps to identify any vulnerabilities & risks associated with IoT devices.
- Authors couldn't finish as the hardware used "ZigBee" for pen-testing is expensive & require specialised person.

What is ZigBee?
↳ wireless sensor device used in IoT

Topic 5: Neural Networks based choice of tools for penetration testing of web applications [Tekerkyi, 2018]

- Web app pen-testing based on the use of Neural network based.
- Neural Networ will produce decision tool which will assist pen-testers.
- Easy to use & its versatility
- disadvantage: large requirements to meet the needs.



Date: 12-06-21

Topic 6: "An analysis system for computer Forensic education, Training, & awareness. [Zhou, 2012]

- ASCFETA → Primary goal - ensure system Analysis, to assist best possible plan for organization
- developers & managers with the ability to recognize & address any deficiencies in forensic field.

Topic 7: Ensemble based approach to increase vulnerability assessment & Penetration testing accuracy [Goel, 2016]

- Primary goal - improve the accuracy of VAPT tools.
- "VEnsemble 1.0" - runs of variety of VAPT tools & can detect various Vulnerability kinds by combining several open source VAPT tools.

Topic 8: "Design & Application of Penetration attack Tree Model oriented to Attack Resistance Test" [Ning, 2008]

- Model represents relationships between different attack types in sequential order of executed assets

Pg:8

Date:

- can track per asset as well as attack execution
- Helpful in intrusion detection areas.

Topic 9: Automated penetration testing based on threat model [Wells, 2016]

- Model to assess the resistance of tested systems to malicious attacks.
- Model built for human reading instead of system reading
- Model can be used to implement security measures to mitigate the effects of sensitive data exposures.

Topic 10: Assessment of website security by Penetration using Wireshark [Sandhya, 2017]

- Wireshark - tool to monitor routing packets
- Wireshark do execute information gathering
- this method to determine if a website was secure or not.
- the evaluated website, Presented in this paper has flaw in its own security mechanism

Pg:9

Date: 14-06-21

Topic 11: Evaluating Self-Adaptive Authorisation Infrastructures through Gamification [Bailey, 2018]

- A technique based on an ethical hacking game, secured by authorisation that observes user action pre/post adaption to prior methods.
- This experiment found the capacity to handle harmful behaviour of genuine & intelligent users while also gathering user responses to new adaption.

Topic 12: Despriptive Analytics: Examining expert hackers in web forums. [Abbasi, 2014]

- Hackers forum content - identify experienced hackers based on their specialities using a generalised framework.
- Social media used to get hackers specialities
- All interactions between hackers was extracted.

Date: 16/06/21

Research Proposal:

Topic: What is hacking?

Hacking is someone who explores methods of breaching defenses & exploiting weakness in a computer system or network.

RQ*: What is ethical hacking
Identify & exploit vulnerabilities using the same methods as criminal hackers

RQ*: Why do we need ethical hacker?
Every business/organisations are prone do attacks, to safe gaurd their environments they should secure the environments by finding all the gap's in their system & to fix it. So every organisation must hire ethical hackers to find the vulnerabilities & fix them.

RQ: can ethical hackers really fix the system vulnerabilits?

RQ = Research Question

Date: 20/06/21

RQ: How security provided by ethical hackers are different from traditional security?

Traditional security	Ethical hackers
→ Reactive	→ proactive
→ catch criminal who hacks the system	→ hack the system before the attack to find any weak links
→ Tools & softwares are used like "antivirus" to protect the system.	→ hired by their company to identify loop holes

RQ: Does ethical hackers poses risk to client?

→ Criminal hacker monitoring the transmissions of ethical hacker could drop the information.

RQ: Assessing the tools & techniques used by ethical hackers.

Date:

RQ: How ethical hackers approach towards finding intruders?

→ Ethical hackers looks for answers to these basic questions. How intruder can gain access to the target system? Are they any weak link in the security system? On target system, what can an intruder see? What can an intruder see?

RQ: Is ethical hacking "ethical"?

Many people considers that hacking is unethical. With the rise of cyber-crime, it is clear that businesses & governments must ensure their cybersecurity is flawless

25/06/21

Hacking Methodology.

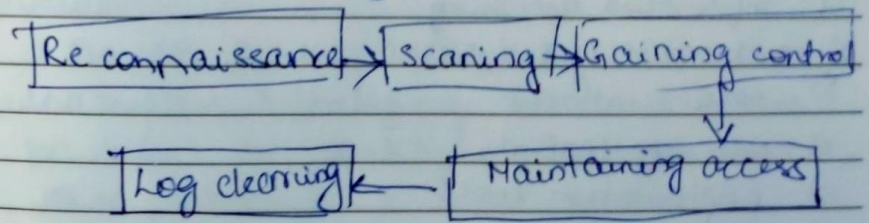


Fig 1: Flow of hacking methodology.

Date: 02/07/24

Tools need to perform ethical hacking:

* Kali Linux - Linux distribution O.S mainly used for penetration testing & security auditing. Kali Linux contains tools for computer forensics, penetration testing, reverse engineering etc.
Kali linux developed by "offensive security"

* Kali Linux is popular because it has over 600 tools for penetration testing & security analysis.

* Kali follows an open-source model & all the code is available on Git & allowed for tracking.

Major utilities of Kali Linux
1) Information Gathering
2) vulnerability Analysis
3) Wireless Attacks
4) Web application
5) Exploitation tools
6) Stress Testing
7) Forensic tools

Date:

8) Sniffing & spoofing
9) Password Attack
10) Maintaining Access
11) Reverse Engineering
12) Reporting Tools
13) Hardware hacking.

04/07/24

Kali applications:

NMAP: Network mapper, open-source utility used for network discovery & vulnerability scanning.
* NMap also can reveal the services & ports each host is serving, exposing a potential security risk.

ex: nmap IP_ADDR.

Metasploit:
Provides public resource for researching vulnerabilities & developing code that allows pen tester's the ability to infiltrate their given network.

ex: db_nmap -V -sV 10.0.1.1/24
(db_nmap: database; -V: verbose mode; -sV: service version)

Date: 09/07/21

Ethical hacking terminologies:

* Adware - s/w to force pre-chosen ads to display
* Backdoor - hidden entry to computing device
* Bot - Program that automates an action
* DDOS - Distributed denial of service attack.
* Logic bomb - A virus secreted into a system that trigger a malicious action when certain conditions are met.
* Rootkit - type of software to hide the existance of certain types.
* Phising - e-mail fraud method.
* Social engineering - deceiving someone with the purpose of acquiring sensitive & personal information
* SQL Injection - SQL code injection technique
* Trojan - A malicious program disguised to look like a valid program.
* Zombie - drone - Hi-jacked computer that is being used anonymously as a soldier or drone for malicious activity.

Date: 14/07/21

Ethical hacking tools (Continued..)

* Burp Suite
  - used for performing security testing of web applications.
  - provides full control to combine advanced manual techniques

* Angry IP scanner:
  - light weight cross-platform IP address & port scanner.
  - multithread approach is used to increase scanning speed.

* Cain & Abel
  - Password recovery tool for microsoft OS.

* Super scan
  - powerful tool for n/w adimistrators to scan TCP ports & resolve hostnames.

* Network Stumbler:
  - WiFi scanner & monitoring tool for windows. It helps to find non-broadcasting wireless networks.

Date:

* ToneLoc :-

- Stands for Tone Locator
- Popular computer program written for MS-DOS in early 90's.
- Scans list of telephone numbers, usually dialing every number in a local area code.

14/Oct/21

Ethical Hacking Process

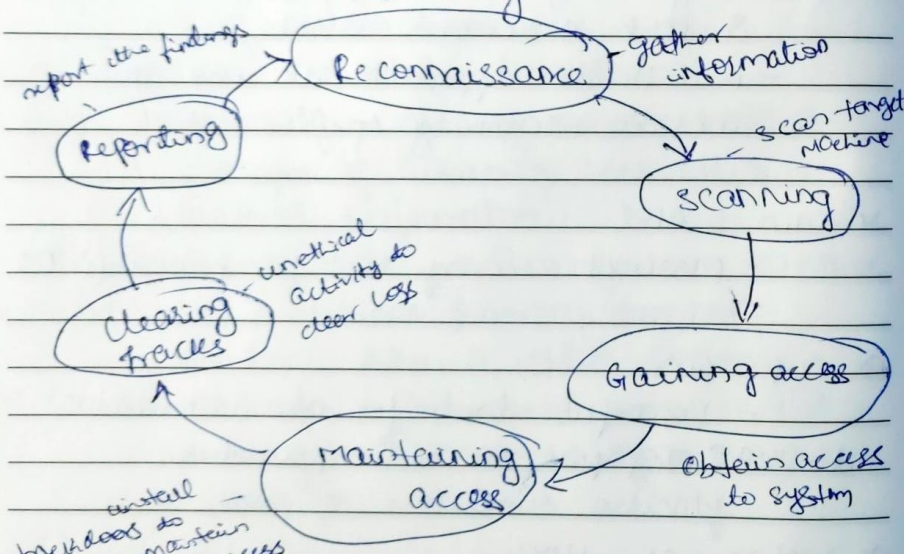


Fig 2: Ethical hacking flow chart

Date: 22/Oct/21

Penetration testing :-

* Always mandatory to have agreement that will explicitly mention
  1) time of pen test
  2) IP source of the attack
  3) Penetration fields of the system.

Types of penetration testing :-

1) Blackbox - doesn't have any information regarding the infrastructure or organisation

2) Grey box - have partial knowledge of infrastructure

3) White box - have necessary information about the infrastructure.

4) Internal Pentesting - hacker is inside the n/w of company when performing test

5) External pen testing - ~~hacker~~ ethical hacker tries the attack using public networks through the internet.

Date: 25/07/21

Ethics in ethical Hacking:

Ethical hacking code of ethics or behaviour focuses on the duties, responsibilities & limitations when performing his duty.

- → Not collect, give, sell or transfer any personal information to a third party without client prior consent.
- → protect the intellectual property of others by relying on your own innovations & efforts
- → Never knowingly use software or process that is obtained or retained either legally or unethically
- → Never engage in deceptive financial partices such as bribery or other improper financial practices.
- → Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- → Ensure all penetration testing activities are authorized & within legal limits.

Date: 29/07/21

What ethical hackers check & what answers they are asking for?

- → How intruder can gain access to target sys?
- → On the target systems, what can intruder see?
- → What could an intruder do with the target?
- → Is anyone at the target paying attention to intruder's efforts or success.

02/08/21

Does ethical hacking have a future?

- The industry will witness a 35% growth by 2021.
- Technical hackers can look for top companies like Dell, Google, Wipro, Reliance, infosys & IBM. to land the highest-paid ethical jobs.
- Experts predict global penetration testing market value will reach US$ 4.1 billion by 2024.
- Every organisation must have pen-testers to find the vulnerabilities & prevent network from hackers

Date: 09/08/21

Latest news on ethical hacking.

> ~~How~~ How do you become an ethical hackers?" - by connor Jones

> The proliferation of hacking as a service is giving cybersecurity experts nightmares
- by Economic times

> Apple pays ethical hackers $288k for finding 55 vulnerabilities
- by Sabina Weston.

> Mobile banking apps are exposing user data to attackers
- by Sarah Lennan

> India's ethical hackers rewarded abroad, Ignored at Home - by NDTV

> Decade-old Arcadyan Firmware Vulnerability risks million of routers Attribution link
- by Trendingglow news blog.

Pg#:22

Date: