SURF Summer Undergraduate Research Fellowship

SURF Code: 2022036

PORTABLE PENTEST TOOL

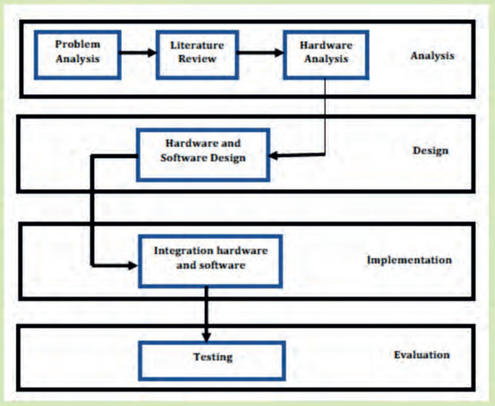
Supervisor: Dr. Gabriela Mogos
Authors: Enhua Kang, Jiaxuan Cai, Jie Ji, Zichao Cong, Zihan Wei
Department of Computing, School of Advanced Technology

ABSTRACT

This project addresses the critical issues of identifying and analyzing suspicious events that create exploitable paths for cyber-attackers. We consider these challenges as an opportunity to develop a portable security analysis tool able to collect and analyse evidence found in a compromised computer systems and networks to help in the prevention, detection, and mitigation of cyber attacks. The outcomes of this project will be a security testing tool designed to be simple, portable, inexpensive, robust, and easy to use and a beginner's *Guide of Basic Security Testing*.

METHODOLOGY

The research has to be carried out in various aspects, including technology and tool usage, in order to build the use cases.



PENTEST TOOL DESIGN

Kali Linux is one of the most popular penetration testing platforms used by security professionals, and researchers around the world for security and vulnerability assessment, attack research, and risk testing.

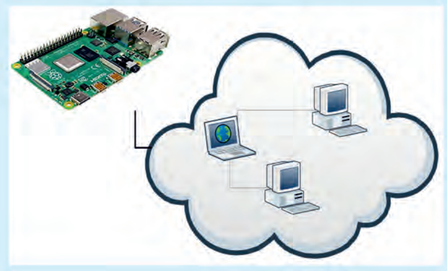
The Raspberry Pi is an extremely low-cost computer that plugs into a monitor using HDMI and uses USB keyboard and mouse.

The Kali Linux on a Raspberry Pi combination can provide us with a flexible, adaptable, low-profile and cost-effective penetration testing platform that can accomplish many test objectives larger platforms cannot.

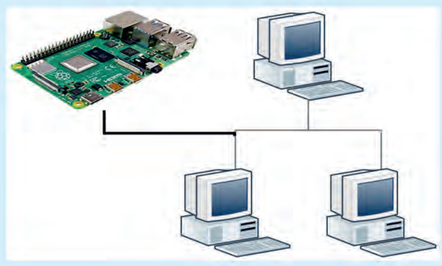
The pentest tool will be to investigate the vulnerabilities that may exist and could lead to a breach of the confidentiality, integrity, and availability of a data system.

EXPERIMENT SETUP

Outside the network: If we are starting outside, we are normally testing as if we are an external threat trying to gain access from the outside of the target network in.



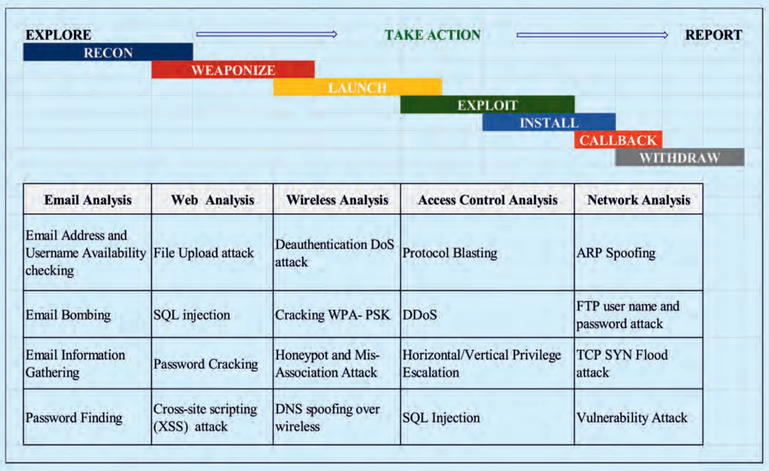
Inside the network: The placement here may be required in part of a white hat test, but black hat testing may depend on sustained presence here, and the challenge of getting our Raspberry Pi into a good vantage point without being detected can be substantial.



Kali Linux is a suite of tools built to help gather information and exploit weaknesses. Kali is a wonderful set of tools for our use, called *metapackages*, so we mapped those tools to the **Penetration test Chain** model to help get a better understanding of which tools to use where.

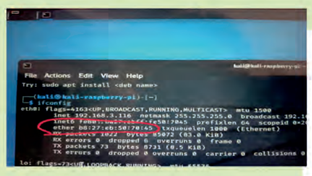
The portable system has been tested in the following scenarios: **Wireless analysis, Network analysis, Web security analysis, Port scanning, Access control analysis** and **Email Analysis**.

Each scenario covers the stages: **Information Gathering/Penetration Testing, Vulnerability Assessment, Exploiting Vulnerabilities,** and **Prevention and Mitigation Measures.**



Email Analysis	Web Analysis	Wireless Analysis	Access Control Analysis	Network Analysis
Email Address and Username Availability checking	File Upload attack	Deauthentication DoS attack	Protocol Blasting	ARP Spoofing
Email Bombing	SQL injection	Cracking WPA- PSK	DDoS	FTP user name and password attack
Email Information Gathering	Password Cracking	Honeypot and Mis-Association Attack	Horizontal/Vertical Privilege Escalation	TCP SYN Flood attack
Password Finding	Cross-site scripting (XSS) attack	DNS spoofing over wireless	SQL Injection	Vulnerability Attack

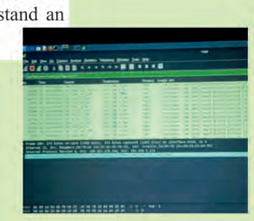
RESULTS & ANALYSIS



Emails use different protocols to send and receive emails depending on the method used for sending, receiving, and storing/accessing emails. The three protocols used are as follows:
• SMTP • POP3 • IMAP4

E-mail Analysis

Capturing and analyzing network traffic should be an essential part of our investigative process. Packet captures can be used to reveal artifacts that may help us to better understand an incident, point to its origin.



Web Security Analysis

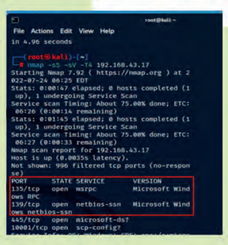
Web applications have always been a long-standing target for malicious adversaries to steal, manipulate, sabotage, and extort the corporate business.

Network Analysis

Using the *aircrack-ng* suite we can both disrupt and snoop on legitimate traffic, or even establish our own access to the network without explicit onboarding or access rights.

Access Control Analysis

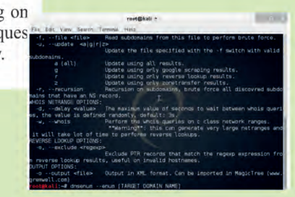
Access needs to have already been obtained before a local vulnerability can be exploited. The privilege escalation exploit is usually reserved for exploits that run locally, on a victim machine, exploiting a process or service with higher privileges.



Wireless Analysis

Password Analysis

If a service requires valid credentials to access it, we can simply attempt to guess, or brute force, these credentials until they are identified. Depending on the nature of the service, the techniques and tools for these attacks may vary.



CONCLUSION

The project taught us how to customize a Raspberry Pi running Kali Linux for penetration testing environments. One huge advantage of the Raspberry Pi is its size and mobility. We know that the Raspberry Pi will be slower than a normal computer based on the low memory and smaller hard drive size, so we are not expecting it to be as quick as one of the lab computers, but the hope is that it will work fast enough to be practical as a penetration testing platform.

ACKNOWLEDGEMENT

This work is supported by Summer Undergraduate Research Fellowship (SURF), Xi'an Jiaotong-Liverpool University. We would like to express our gratitude towards the supervisor, our families and friends for their support in carrying out this work successfully.

SELECTED REFERENCES

[1] B. Brennen. "Kali Linux on the Raspberry Pi with the PiTFT", Adafruit ®, 2015.
[2] C. Altheide, H. Carvey, "Digital Forensics with Open Source Tools", Syngress, 2011.
[3] O. Bowcott, "Justice system at 'breaking point' over digital evidence", 2018.
[4] S. V. N. Parasram, "Digital Forensics with Kali Linux", Packt Publishing, 2020.