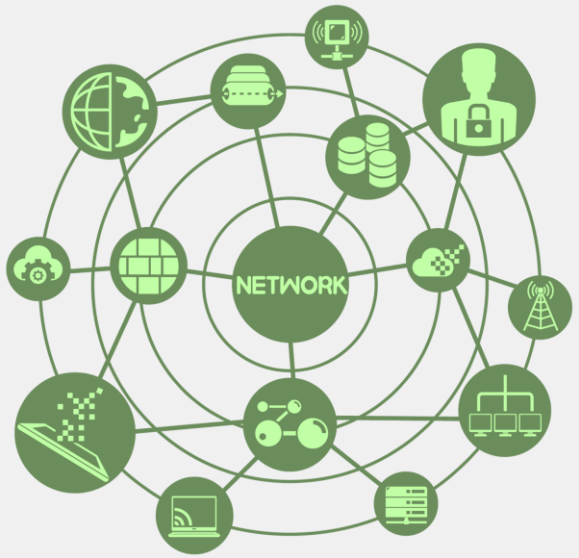
Vulnerability Assessment & Penetration Testing Using Raspberry Pi Remotely

Rizwan Syed

Department of IT, Theem College of Engineering, Mumbai University

Vulnerability Assessment & Penetration Testing (VAPT)

- Every organization is a potential target for hackers.
- The best practice for any organization is to conduct VAPT Audit time to time to secure their network from various hacking attacks.



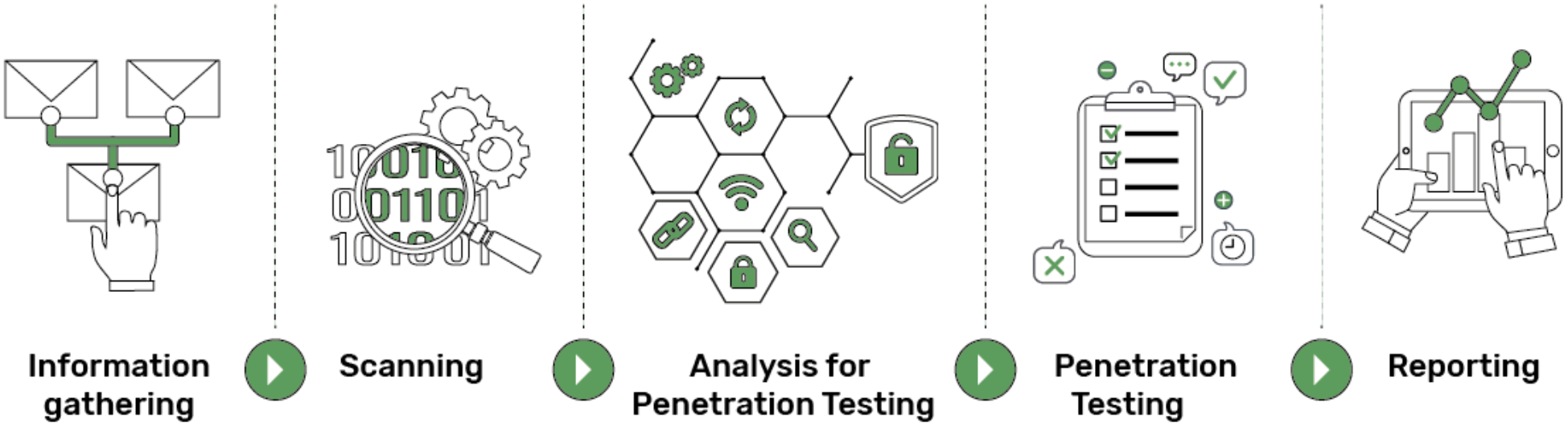
Vulnerability Assessment & Penetration Testing

- VAPT Audit is the way to detect security vulnerabilities in the system or network with various malicious techniques.
- VAPT, uses same techniques as that of a real-life evil hacker.
- Focus on identifying vulnerabilities in the network, server and system infrastructure.
- VA & PT is the two different tasks, usually with different results, within the same areas of focus.

Vulnerability Assessment & Penetration Testing

- IT network VAPT, is an important task to be carried out by IT administrators.
- This is because of the rise in hacking attempts irrespective of the industry type.
- Attacks can happen from internally or externally.

Vulnerability Assessment & Penetration Testing Process



- Penetration Testing (PT) – Exploitation of security flaws and vulnerabilities simulating real-life attack, analyse and provide the business impact of the attack performed

External & Internal Network Pen testing

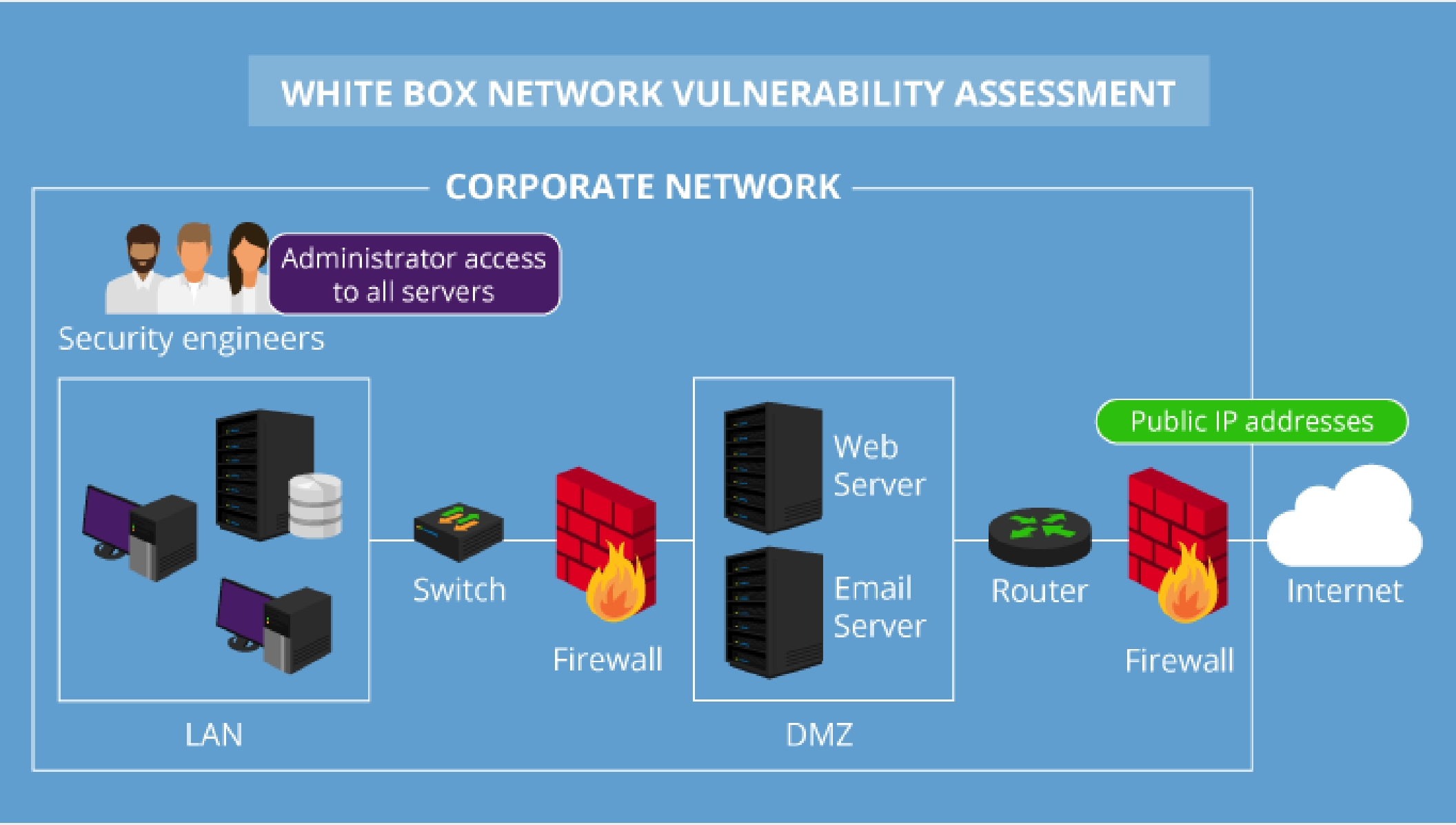
❖ External Network Pen testing

An external network pen test is designed to test the effectiveness of perimeter security controls as well as identify weaknesses affecting all other external-facing systems, such as web, mail and FTP servers.

❖ Internal Network Pen testing

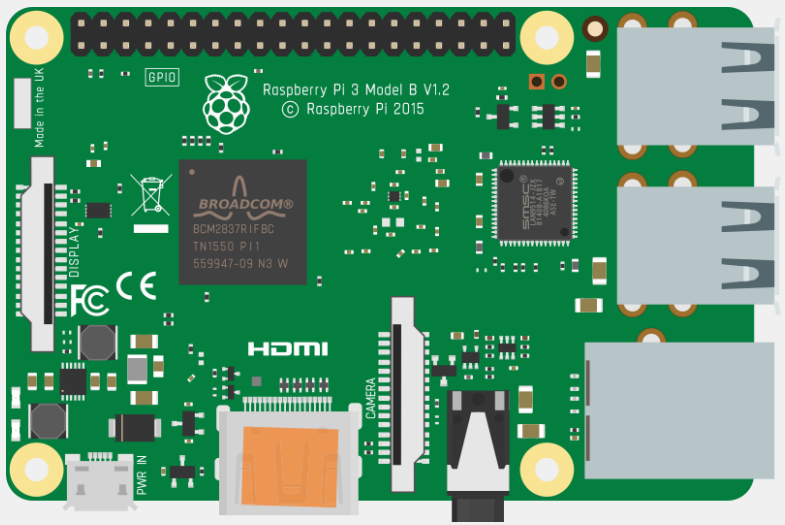
- An internal network pen test is performed inside a network with controlled exploits to identify weaknesses in existing network, so you know organization's security posture.
- Internal penetration testing evaluates what an insider attack could achieve.

Internal Network Penetration Testing



Penetration Testing With Raspberry Pi

- Raspberry Pi is a low-cost credit-card sized computing system that may be custom-made for almost about anything including penetration testing
- The Raspberry Pi can be configured to run Kali Linux and most security tools and applications.
- With right devices and setup, Raspberry Pi is an incredible wireless analysis and network pen test tool.



Penetration Testing With Raspberry Pi Operating System

- Kali Linux is a penetration testing / security auditing Linux distribution.

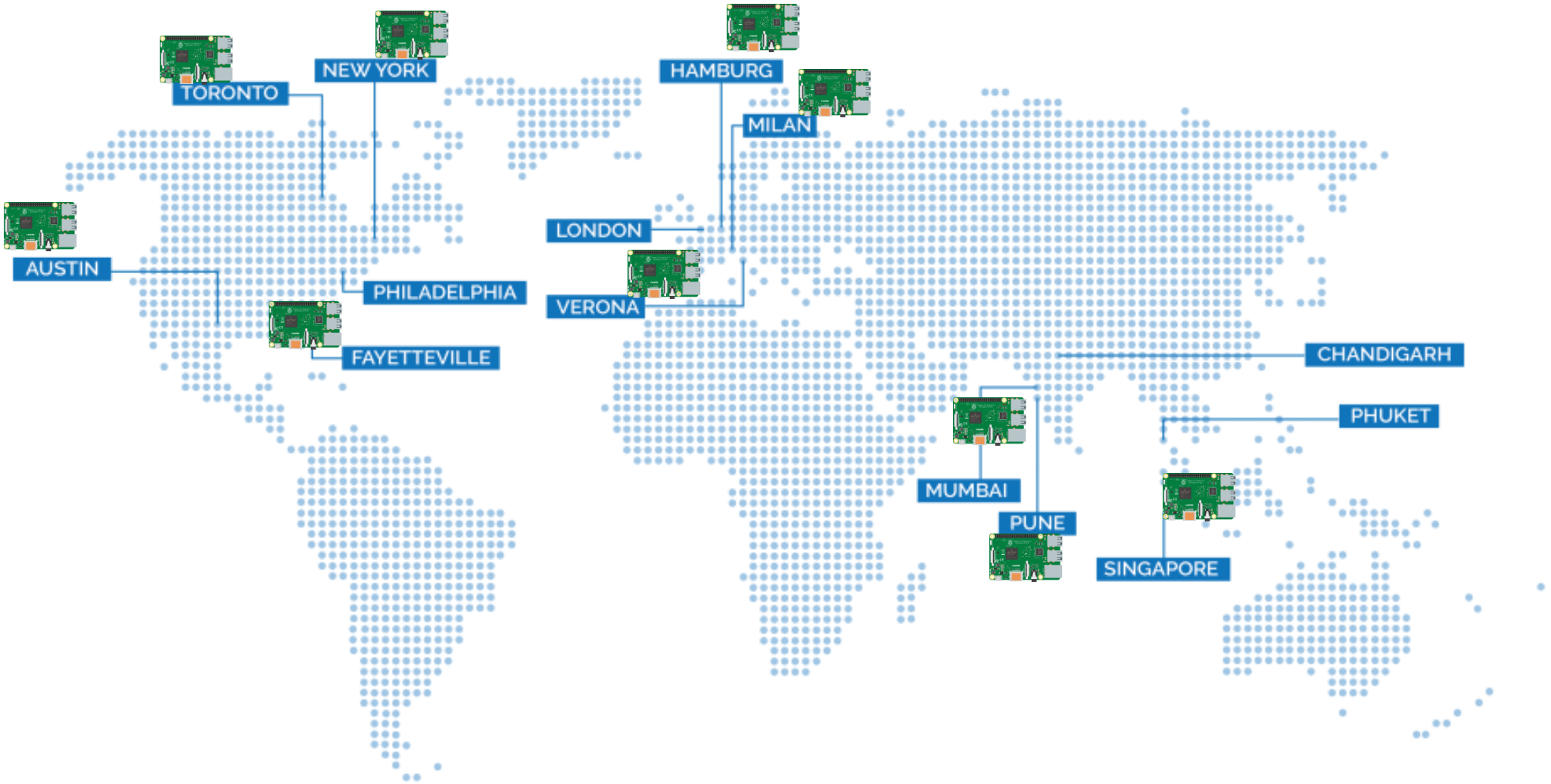
- Kali Linux has numerous penetration-testing programs, together with
  - Nmap (a port scanner),
  - Aircrack-ng (Wireless Pentesting Suite),
  - Wireshark (a packet analyzer),
  - John the Ripper (a password cracker),
  - Burp suite and
  - OWASP ZAP (both web application security scanners)
  - and far a lot of.

Penetration Testing With Raspberry Pi Use Cases

- Use a Raspberry Pi for penetration tests such as breaking wireless security.
- Scanning vulnerabilities in networks, and capturing sensitive data.
- Turn a Raspberry Pi into a honeypot to capture sensitive information (Rogue Wireless Honeypot AP).
- Compromise wireless vulnerable keyboards and mouse.

Scenario

Scenario


TORONTO
NEW YORK
HAMBURG
MILAN
AUSTIN
LONDON
PHILADELPHIA
VERONA
FAYETTEVILLE
CHANDIGARH
PHUKET
MUMBAI
PUNE
SINGAPORE

Scenario

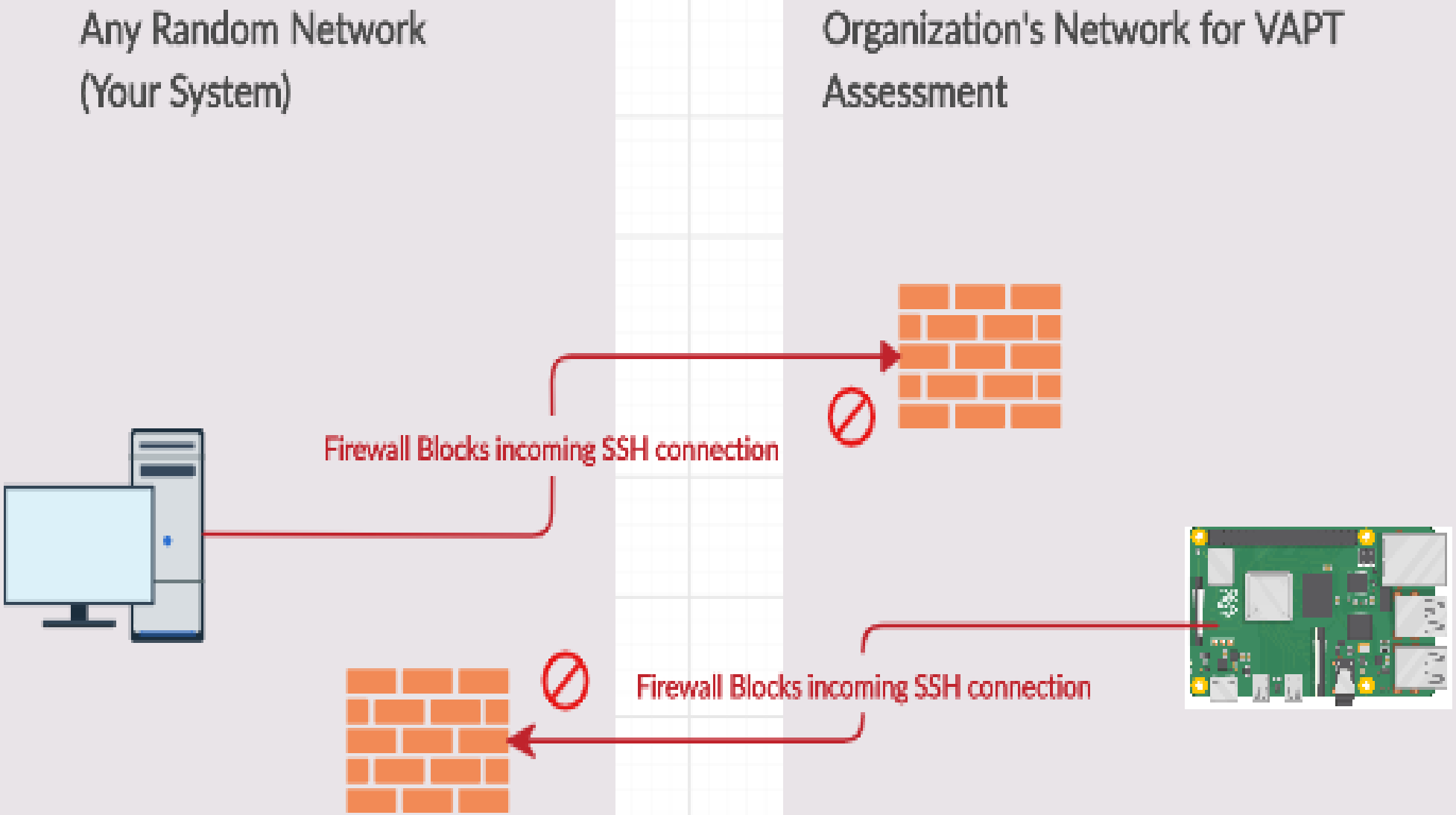
Scenario

- Since Kali Linux is a fully featured Linux OS, you'll control the whole environment through SSH
- However, your incoming SSH connections may be blocked by firewalls or other security solutions

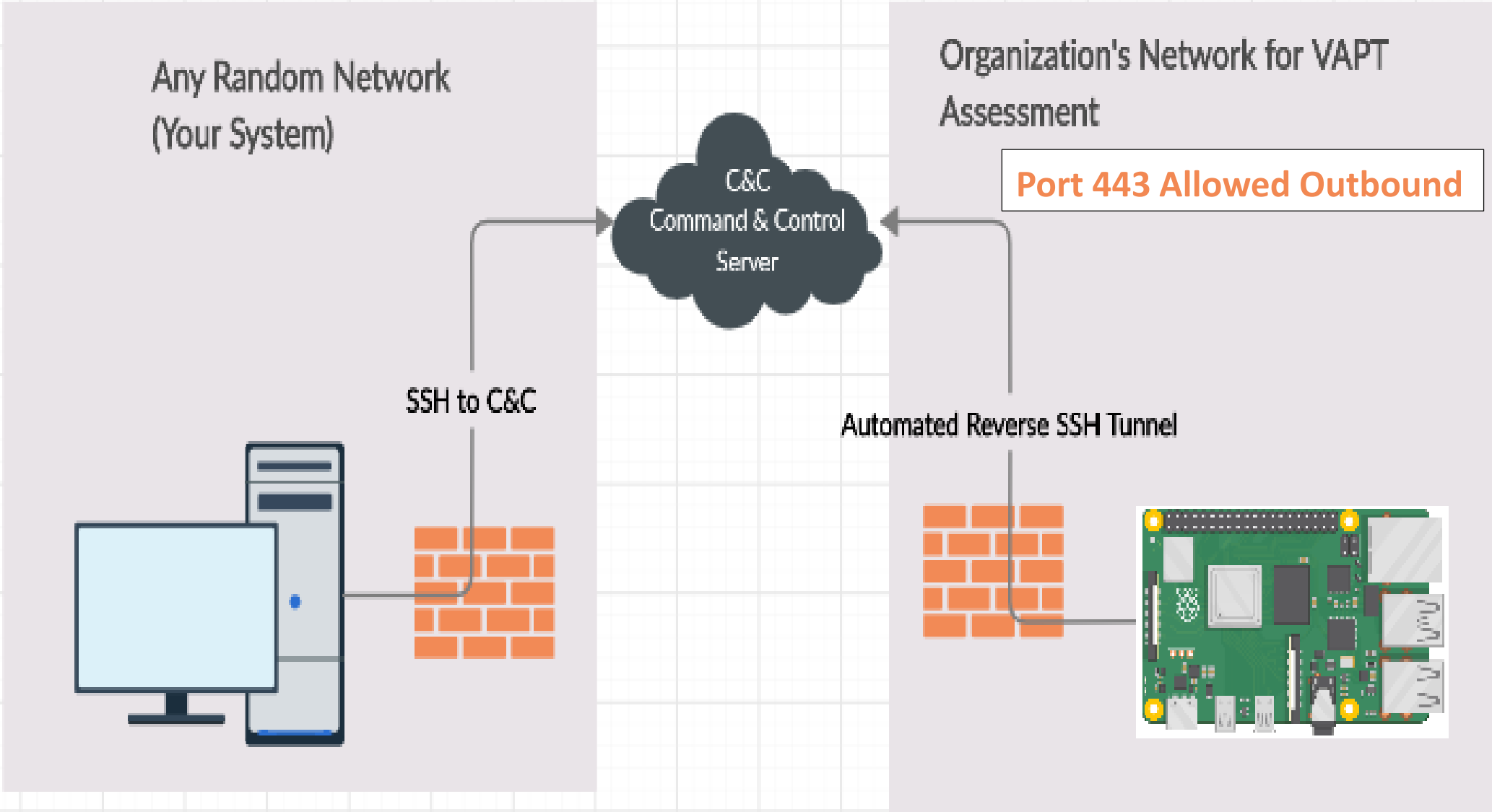
Scenario

- Many organizations have security measures in place to block incoming connections with the goal of preventing backdoors into their network.
- In a white-box assessment, you'll be explicitly ready to open up a firewall port to allow SSH to your Raspberry Pi.
- The bad news is even though this is often possible from a policy standpoint, it's going to be difficult to accomplish when handling multiple sites under multiple administrative controls.

Scenario


Any Random Network
(Your System)
Organization's Network for VAPT
Assessment
Firewall Blocks incoming SSH connection
Firewall Blocks incoming SSH connection

Reverse SSH Tunnel to C&C Server



Conclusion

- Reducing Hardware Cost.
- Saving Time and Space.
- Increase productivity of Security Engineers.
- No need to explicitly open up firewall port.
- Able to conduct VAPT remotely.
- Central Command and Control (C&C) Server.

Conclusion

- The Raspberry Pi would work perfectly for Red Team Engagement where we can place our Raspberry Pi Dropbox anywhere in client network without need to worry about company's firewall policy.

- In a reverse SSH connection, the Raspberry Pi connects and initiates the connection to the C&C server instead of security engineer connecting to the Raspberry Pi directly.

- **Reverse SSH to C&C Server** is a good alternative to manage a Raspberry Pi running Kali Linux at various location.

Vulnerability Assessment & Penetration Testing Using Raspberry Pi Remotely

THANK YOU

Any Questions ?

Rizwan Syed
Department of IT, Theem College of Engineering, Mumbai University