
CYESEC TECH
CYBER SECURITY & ESOLUTIONS

Mr. Emmanuel Okoi

Lead Faculty/CEO

CYESEC TECHNOLOGIES

Red & Blue Team

Multi-Certified in Offensive & Defensive Cybersecurity

HND || BSC || MSC|| CCNA || CEH || CCSA || CPENT || CDFA || ISO/IEC 27003

(PhD In-view)

Cybersecurity & Forensic Analyst

PROACTIVE CYBERSECURITY TOOLS FOR ATTACK PREVENTION AND DETECTION: USING MILITARY INTELLIGENCE APPROACHES

01

Business of learning who the enemy is

02

How the enemy operates

03

What are his objectives

04

Using the proactive tools and Approaches for countermeasures

RED TEAM VS BLUE TEAM

TWO DIFFERENT ROLES IN HACKING

follow @thehardsecurity

Which team you'll join? Comment!

RED TEAM

- Offensive Approach
- Exploit vulnerabilities
- Do Social Engineering
- Performs Pentesting
- Ethical Hacking
- Web App Hacking

BLUE TEAM

- Defensive Approach
- Damage Control
- Threat protection
- Incident Response
- Infrastructure security
- Digital Forensics

INTRODUCTION

Proactive cybersecurity entails hunting for threats and identifying gaps in your security posture before an incident or breach takes place.

Examples of a proactive approach to security include:

1. Threat Hunting

2. Penetration Testing

3. Security Awareness Training.

WHY YOU NEED TO TAKE A PROACTIVE APPROACH TO CYBERSECURITY

Threat Hunting is the process of proactively searching for and identifying threats in your environment — long before your endpoint detection and response (EDR) solution or antivirus catches them. Threat hunting gives you the opportunity to identify weak spots in your existing security measures. And even better, proactive threat hunting helps you find and stop threats that dwell in your environment without your knowledge.

Threat Hunting is particularly effective at finding quiet, hidden threats in your environment. While some threat actors still favor loud and overt attack tactics (such as ransomware), others prefer to be stealthy, gaining access to your environment and quietly sitting there, plotting their next move.

Penetration Testing

Sometimes, the best way to learn to fix things is to break them. And that's the general goal of penetration testing, or pentesting.

Pentesting is an exercise that requires a person or team to try their best to hack your system. But unlike shady threat actors who do this, pentesters are ethical hackers who are kind enough to offer specific, tangible takeaways to help you strengthen your cybersecurity defenses. After conducting their exercises, pentesters analyze what went well and what didn't, giving you a list of improvements to make in your environment.

Penetration testing is the ultimate test (see what we did there?) for your proactive cybersecurity defenses. These tests can be performed internally or outsourced to a trusted third party.

Security Awareness Training

An organization is only as strong as its weakest link. And if Jerry in accounting just can't pass up an opportunity to click a link in an email, it's imperative to help him understand why this is a bad practice. And that happens through cybersecurity training.

Security awareness training is the key to helping your end users understand the risks associated with poor cyber practices. And this training works — 67% of IT professionals claim their organization's phishing failure rates went down with the incorporation of security awareness training. But it's important to note that while training is an exceptional start, simulations and exercises up the ante and help your employees retain the knowledge they learn.

How the enemy operates

1. **Masqueraded links**
2. **Social medial handles**
3. **Open ports**

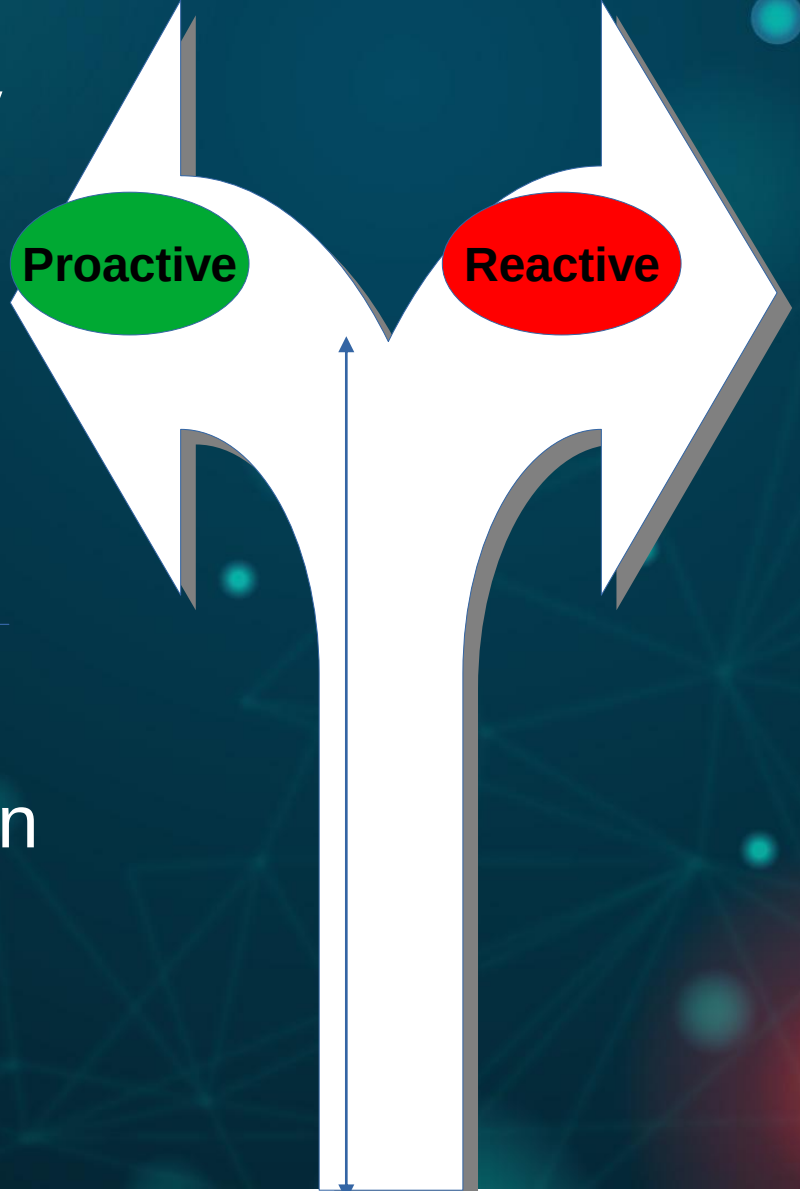
A proactive approach to cybersecurity defensive measure is the best approach to make sure there is little to no room for attackers to exploit your devices, systems and network.

What are his objectives

1. Money **(Ransomware)**
2. Power
3. Control
4. Publicity
5. Revenge
6. Protection
7. Learning & Exposure
8. Penetration testing
9. Just for fun!

The majority of today's cybersecurity practices are **reactive.** Most organizations are not adequately prepared against cybersecurity incidents until it is too late; they wait for cybersecurity incident to happen before they take action.

However, having a **proactive** approach to security rather than reacting to every new threat can be time-saving and cost- effective.



USING EXPERT TOOLKITS FOR PROACTIVE APPROACH

STEP 1: Launch your parrot os browser

STEP2:Type on your Browser https://github.com/skavngr/rapidscan.git

STEP 3: Find code zip and click to download ZIP files and save on your desktop

STEP 4: Find the download file on your desktop and locate the rapidscan ZIP file and right click on extract file possibly save it on your desktop

STEP 5: Launch your parrot terminal

Step 6: type cd Desktop

STEP 6: Type ls

STEP 7: Copy rapidscan-master

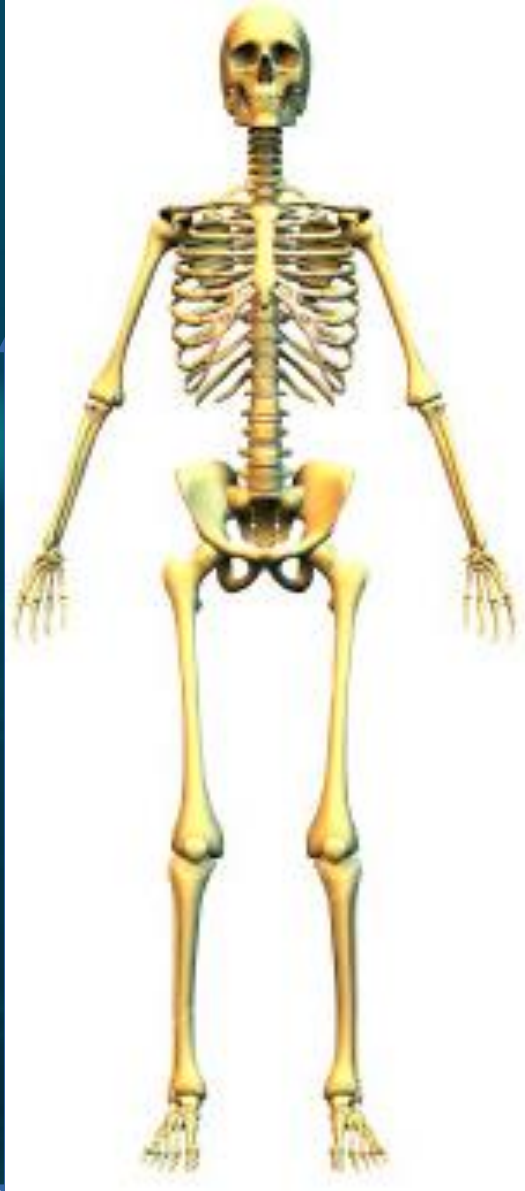
STEP 8: Type cd rapidscan

STEP 9: Press ls

STEP 10: Copy rapidscan.py

STEP 11: Type: sudo ./rapidscan.py and enter

STEP 12: Type: ./rapidscan.py example.com: The process is to begin Vulnerability Assessment using the target URL or Ip address



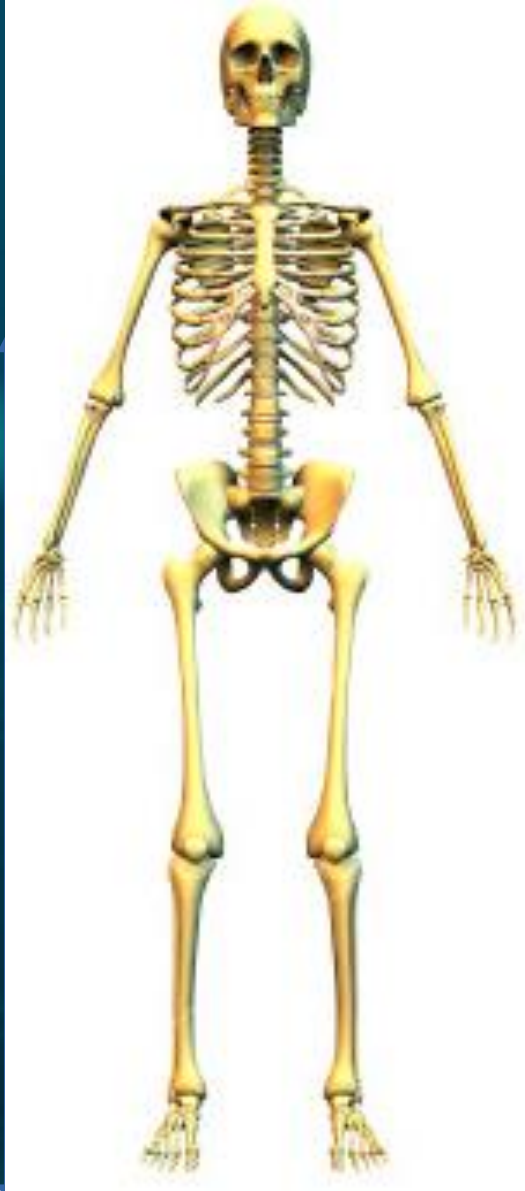
THE NECESSITY OF A PROACTIVE APPROACH TO CYBERSECURITY

Even though businesses are taking a more proactive approach to cybersecurity, they are still far behind in cybersecurity preparedness.

An IBM study revealed that 78 percent of surveyed IT security practitioners reported a data breach that resulted in the loss or theft of more than 7,000 records that contained sensitive and confidential information.

The reactive approach may save an organization's data initially, but eventually, it will increase costs and ultimately result in a damaged reputation. The cost of responding to a single public vulnerability is almost always more than being originally prepared for one. Furthermore, harsher regulatory penalties are being doled out for not properly securing third-party data and digital information.

On the other hand, a proactive approach will help organizations define a baseline level of cybersecurity; this will engage the organization's security team with threats notification to enable them to take action in real-time.



National Cybersecurity Policy and Strategy 2021

In all it chapters, chapter 9 ASSURANCE MONITORING AND EVALUATION

9.1 Standard and Good Practices

9.2 Quality Control and Security Processes

FROM DEFENCE-IN-DEPTH TO DEFENCE-IN-CONCERT.

Defence-in-depth is no longer fit for purpose. A new approach of defence-in-concert is your best chance to stop threats.

HOW

The Defence-in-Depth approach (DiD) refers to an information security approach in which series of security mechanisms and controls are thoughtfully laid throughout a computer network to protect the confidentiality, integrity and availability of data within an organization.

An effective DiD strategy may include these (and other) security best practices, tools and policies:

1.Network Segmentation,
2. Endpoint detection and Response(EDR)
3. Patch Management
4. Intrusion Prevention or Detection System (IDS/IPS)
5. Firewall and Password

WHY DOES IT MATTER?

There is no silver bullet in cybersecurity, however, a DiD strategy ensures network security is redundant, preventing any single point of failure.

DiD strategy significantly increases the time and complexity required to successfully compromise a network, which further drains the resources of engaged cyber threat actors and increases the chances that an active attack is identified and mitigated before completion.

A DiD approach is routinely practised in physical security when trying to protect valuable equipment or other material assets. For example, election offices often have a chain of custody logs, security cameras, and locks within the physical elections environment to protect elections equipment and associated infrastructure. In the banking world, security cameras, ballistic glass, and vaults are used to protect assets and personnel.

N/B: The question now is who cares about those staff members who are sacked or dismissed from service because of one mistake or the other?

WHAT YOU CAN DO!

The idea behind defence in depth is to manage risk with diverse defensive strategies, so that if one layer of defence turns out to be inadequate, another layer of defence will hopefully prevent a full breach. This principle is well known, even beyond the security community; for example, it is a famous principle for programming language design.

Defence in Depth has a series of defence concert approach that if an error isn't caught by one, it will probably be caught by another.

Proactive Cybersecurity tools for attack prevention and detection: using military intelligence approaches will help expose internal and external threats, leading to hidden vulnerabilities, while building an expert team to always respond to system and network failure remotely at any time.

Most significantly, the risk of system infections will reduce realistically. Team leads, unit heads and departments are to deploy effective response procedures to contain malware incident to prevent data loss and safely mitigate attacks using core practitioners.

FINALLY

The aim of proactive cybersecurity tools for attack prevention and detection: using military intelligence approaches is to guide cybersecurity practitioners deploy countermeasures to protect clients critical infrastructure by showcasing an expert methodology for industry best practices. As cybersecurity experts the ethics and standard is to improve upon stimulating **Offensive** & **Defensive** operation against systems and network disruption.

THANKS

Questions?

www.cyesec.com.ng