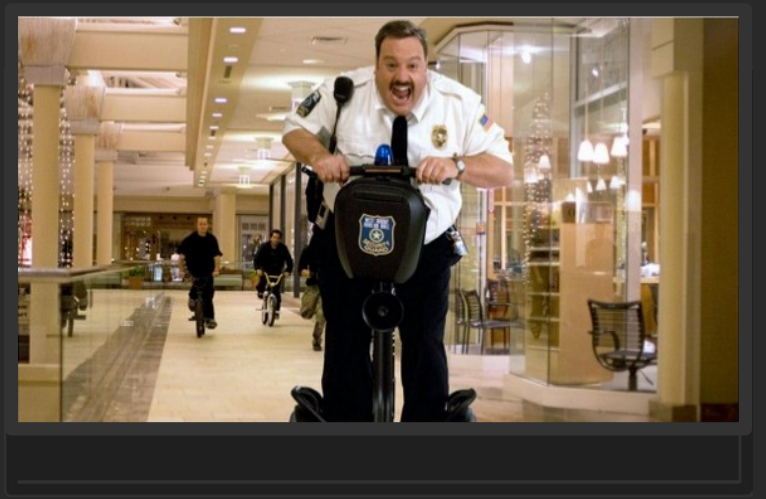
How to Become a Pentester?

Career Secret Roadmap

Mohammad Khreesha
Senior Cybersecurity Director

Whoami



- 13+ Years of IT & Infosec Experience.
- Cybersecurity Director & Trainer.
- ex-OWASP Amman Chapter Leader.
- Youtuber & Blogger.
- CEH, CHFI, ECSA, LPT master, OSCP, CRTP, eCPPT, eCPTX, eWPT, eWPTX, eMAPT, eCIR, eCTHP, eCMAP, eCDFP, & ISO 27001 LI.
- Top Arab Cybersecurity Social Media Influencer (2019, 2020, 2021, 2022, & 2023).

Table of Contents

Pen-testing vs Red-teaming

- **Pen testing** is a security exercise where a Cybersecurity expert attempts to find and exploit vulnerabilities in a defined scope.
- **Red teaming** is a multi-layered, full scope cyber-attack simulation schemed to test the effectiveness of enterprise security controls. The process encloses networks, applications, physical safeguards, and employees.

Penetration Test		Red Teaming
Gain oversight of vulnerabilities	**Goal**	Test the resilience against realistic attacks
Predefined subset	**Scope**	Realistic access paths
Focus on preventive controls	**Tested controls**	Focus on detection and response
Focus on efficiency	**Test method**	Focus on realistic simulation
Mapping, scanning and exploiting	**Test techniques**	Tactics, Techniques and Procedures (TTPs)
Very limited	**Post-exploitation**	Extensive focus on critical assets/functions
Parts of development lifecycle	**Recurrence**	Periodical exercise

The Road-map : Prerequisites

IT Fundamentals

Windows

Linux

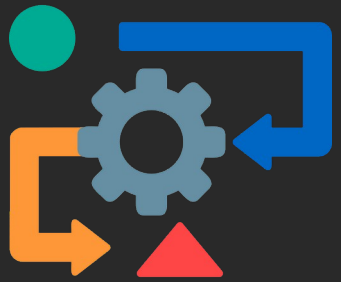
Networking

Scripting

Database

Cybersecurity

The Road-map : Main Skills



Pen-testing Methodologies & Frameworks

Building Home lab

Pen-testing Stages

Play CTFs

Bug Hunting Platforms

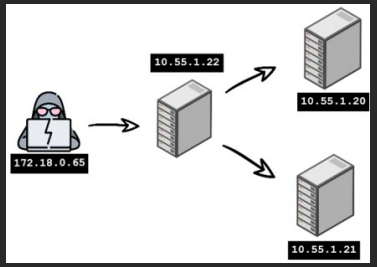
The Road-map : Advanced Skills

AV/EDR Bypass Techniques

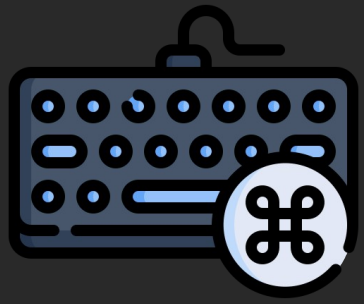
Active Directory Pen-testing

MITRE ATT&CK™

Red-teaming TTPs



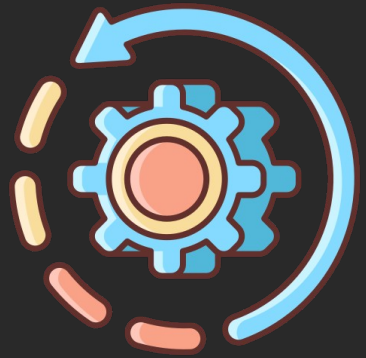
Port Forwarding & Pivoting



C2 Frameworks

Phishing

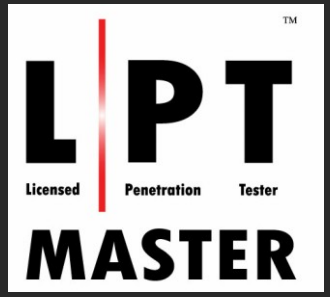
Blue-team/SOC Mindset



Reverse Engineering

Exploit Development

The Road-map : Certificates



Golden Rule

“The best way to learn new things in your field is to teach them to others”

Learning Resources

CYBRARY.IT

www.Free4arab.com

Any Questions, Comments or Concerns?

Thank you!

Website : https://www.technawi.net
Linkedin : https://www.linkedin.com/in/khreesha
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha
Youtube : https://www.youtube.com/technawidotcom