Cybersecurity
From Zero to Hero

Mohammad Khreesha
Cybersecurity Manager

https://technawi.net

Whoami

- 13+ Years of IT & Infosec Experience.
- Cybersecurity Manager [at] Baaz Inc..
- Cybersecurity Trainer.
- OWASP Amman Chapter Leader.
- Youtuber, Blogger, & CTF Maker.
- CEH, CHFI, ECSA, LPT master, OSCP, CRTP, eCPPT, eCPTX, eWPT, eWPTX, eMAPT, ISO 27001 LI Certified.
- Top Arab Cybersecurity Social Media Influencer (2019, 2020, & 2021).

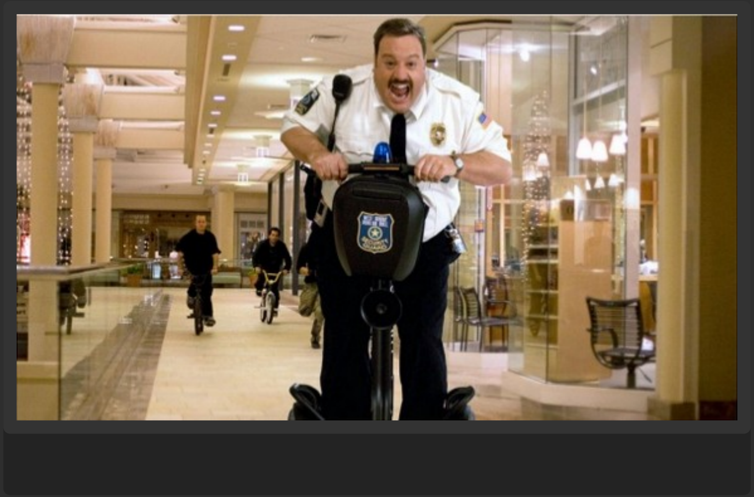


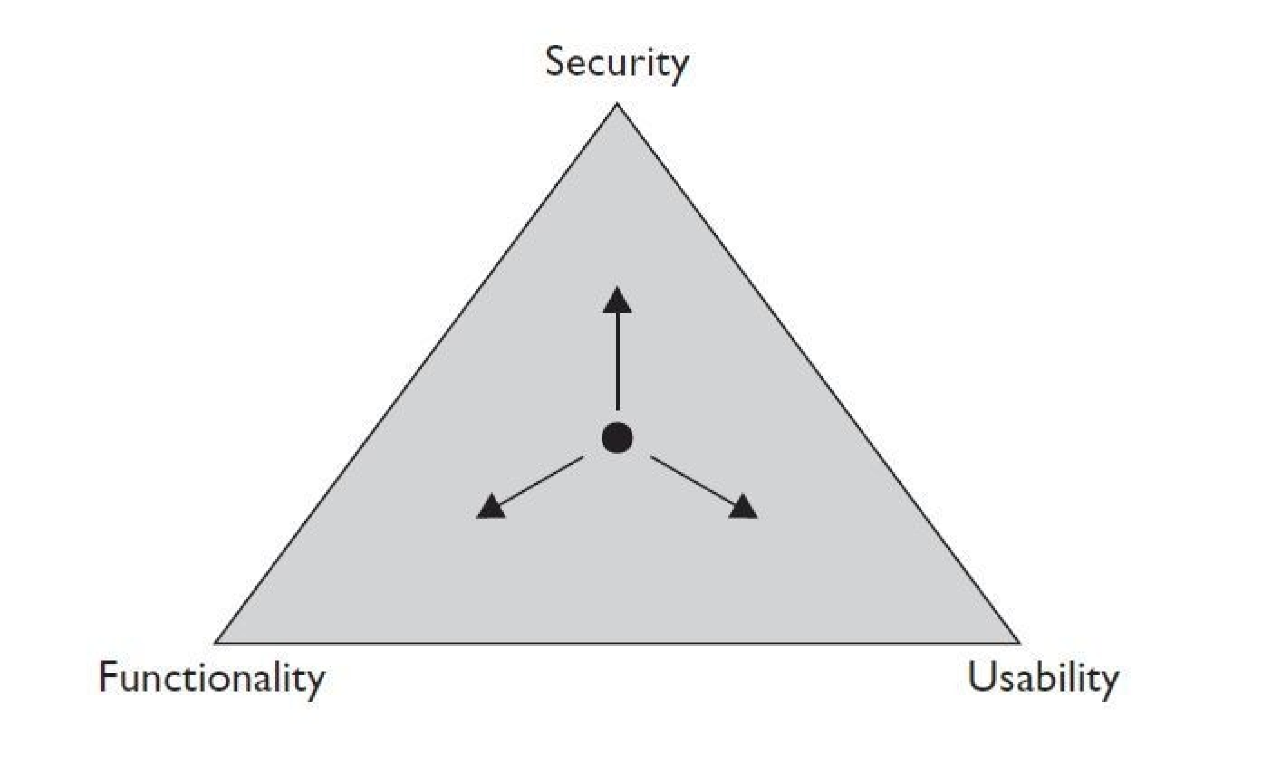
Table of Contents

- Introduction to Cybersecurity.
- Cybersecurity Paths.
- Cybersecurity Skills.
- Cybersecurity Certificates.
- Cybersecurity Resources.
- Q&A.

Introduction to Cybersecurity

- Cyber Security is the practice of protecting our electronic data by preventing, detecting, and responding to cyber attacks.
- Cyber Security effects on :
  - Political Systems
  - Countries Infrastructures ie. : Electric, Gas Stations, ... etc
  - Companies
  - You Privacy
  - … etc
- This means that it affects your life

Continue..



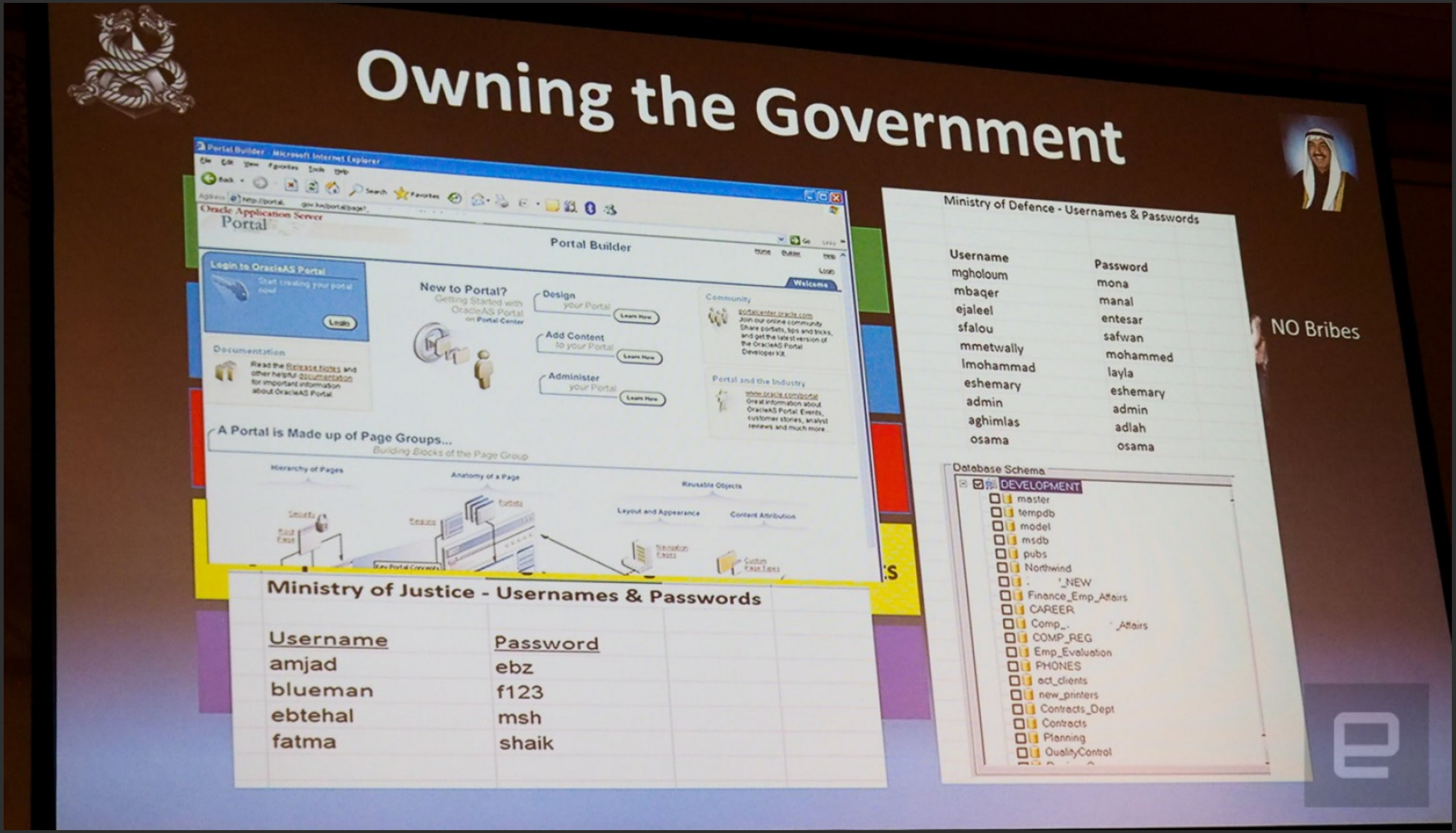
https://en.wikipedia.org/wiki/Bob_Quick_(police_officer)

https://www.businessinsider.com/biometric-fingerprint-password-hacking-2015-1

Directors
Seth Rogen >
Evan Goldberg >

Information
Studio Columbia Pictures
Genre Action & Adventure
Released 2014
Run Time 1:52:11
Size 3.71 GB (1080p HD), 3.73 GB (720p HD), 1.69 GB (SD)
Widescreen
Rated R for pervasive language, crude and sexual humor, nudity, some drug use and bloody

https://en.wikipedia.org/wiki/Sony_Pictures_hack



Owning the Government

Portal Builder - Microsoft Internet Explorer

Address http://portal. gov.kw/portal/page?

Oracle Application Server Portal

Portal Builder

Login to OracleAS Portal

Start creating your portal now!

Documentation

Read the Release Notes and other helpful documentation for important information about OracleAS Portal

New to Portal? Getting Started with OracleAS Portal on Portal Center

Design your Portal

Add Content to your Portal

Administer your Portal

Community

portalcenter.oracle.com Join our online community. Share portlets, tips and tricks, and get the latest version of the OracleAS Portal Developer Kit

Portal and the Industry

www.oracle.com/portal Great information about OracleAS Portal Events, customer stories, analyst reviews and much more

A Portal is Made up of Page Groups... Building Blocks of the Page Group

Ministry of Justice - Usernames & Passwords

Username	Password
amjad	ebz
blueman	f123
ebtehal	msh
fatma	shaik

Ministry of Defence - Usernames & Passwords

Username	Password
mgholoum	mona
mbaqer	manal
ejaleel	entesar
sfalou	safwan
mmetwally	mohammed
lmohammad	layla
eshemary	eshemary
admin	admin
aghimlas	adlah
osama	osama

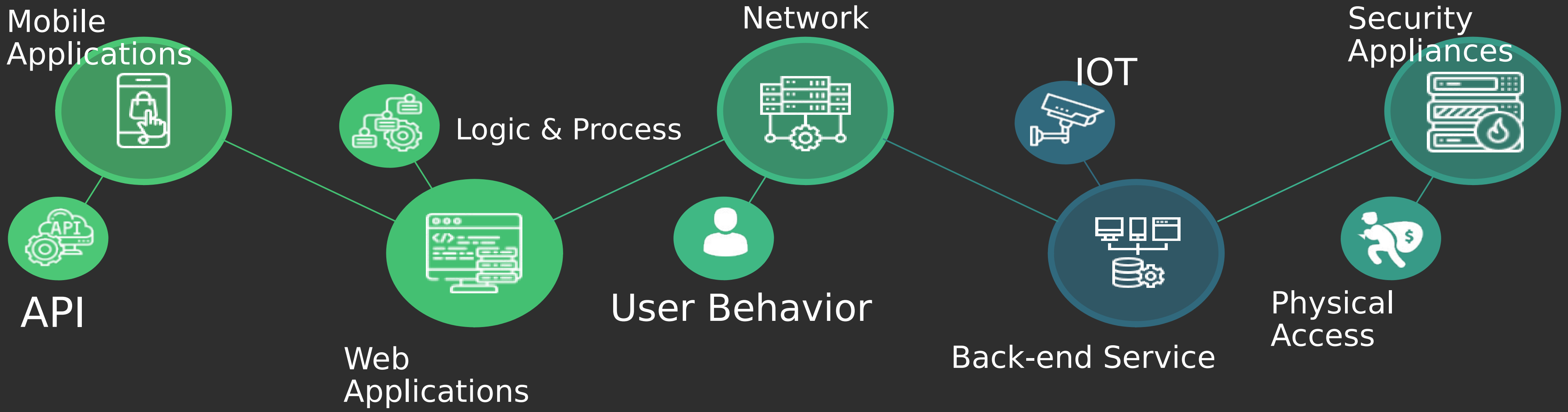
Database Schema

- ☑ DEVELOPMENT
  - □ master
  - □ tempdb
  - □ model
  - □ msdb
  - □ pubs
  - □ Northwind
  - □ . '_NEW
  - □ Finance_Emp_Affairs
  - □ CAREER
  - □ Comp_. 'Affairs
  - □ COMP_REG
  - □ Emp_Evaluation
  - □ PHONES
  - □ act_clients
  - □ new_printers
  - □ Contracts_Dept
  - □ Contracts
  - □ Planning
  - □ QualityControl

NO Bribes

https://www.youtube.com/watch?v=m1IhGqNCZIA

Complete Security



Cybersecurity Paths

- Defensive (Blue Teaming)
  - Security Operation Center
  - Security Architecture
  - DFIR
  - Threat Hunting
  - Threat Modeling
- Offensive (Red Teaming)
  - Pentesting
  - Source Code Review
  - Threat Emulation
- Governance & Management
  - Policies
  - Procedures
  - Compliance

Security Operation Center (SOC)

- Budget on Prevention vs on Detection
- While Prevention is Ideal, Detection is a MUST!
- Better Visibility
- SOC Analysts are those who :
  - Detect.
  - Analyze.
  - Respond to..
  - Report on..
  - And Prevent, cyber security incidents.

Continue..

- SOC Job Titles:
  - Intrusion Detection Analyst
  - SOC Analyst / Engineer
  - CERT Member
  - Cyber Threat Analyst

- SOC Jobs Certificates :
  - EC-Council Certifications (CEH, CSA, CTIA, ECIH)
  - CompTIA Certifications (Security+)
  - SANS GIAC Certifications (GSEC, GCIH, GCIA, GMON)
  - ISC2 Certifications (SSCP)

Incident Response

- Methodology:
  - Preparation, Identification, Containment, Eradication, Recovery, Lesson Learned.
- Certifications Related to IR Jobs:
  - EC Council Certifications (ECIH)
  - SANS GIAC Certifications (GCIH, GCIA, GCFA, GREM)

Digital Forensics

- Law and Order of Information Security
- Digital Evidences are extremely Volatile
- Chain of Custody (Continuity of Evidence)
  - Evidence has been (Gathered, Processed, handled and stored) without alteration.
- Job Titles :
  - Computer Crime Investigator
  - Insider Threat Analyst
  - Law Enforcement
  - Digital Investigation Analyst
- Certifications :
  - EC Council Certifications (CHFI)
  - SANS GIAC Certifications (GCFE, GCFA, GREM)
  - eLearnsecurity (eCDF)

Governance & Management

- Governance determines who is authorized to make decisions.
- Governance: doing the right thing
- Management: doing things right.
- Jobs : CISO, Security Manager, Security Director

Management	Governance
Implementation	Oversight
Authorized to make decisions	Authorizes decision rights
Enforce policy	Enact policy
Responsibility	Accountability
Project planning	Strategic planning
Resource utilization	Resource allocation

Risk Assessment

- It is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system.
- Security Risk Assessment can be implemented base on different standards and approach like: ISO 27005/ ISO 31000 / NIST / Cobit 5 for risk.
- Jobs : Risk Assessor, Risk Officer, Risk Manager

Security Audit

- It is a manual or systematic measurable technical assessment of a system or application.

- Usually the audit will be against standards, benchmarks, best practice and framework or process.

- Jobs : Auditor, Lead Auditor, Audit Manager

- Some of the standards in security the audit is happening against it:
  - ISO 27001 (ISMS – Information Security Management System)
  - PCI DSS (The Payment Card Industry Data Security Standard)
  - HIPAA (Health Insurance Portability and Accountability)
  - ISO 22301 business continuity management system (BCMS)

Pentesting

- Exploits security vulnerabilities in web-based applications, networks and systems.
- They use a series of penetration tools – some predetermined, some that they design themselves to simulate real-life attack.
- Responsibilities :
  - Perform formal penetration tests
  - Design and create new penetration tools
  - Web, Mobile, Network, IoT, SCADA, ...etc.
  - Help the customer fix the vulnerabilities.
  - Social Engineering.
  - PT is not about zero-days.

Continue..

- Skills :
  - Computer Skills
  - Networking Skills
  - OS Skills (both Windows & Linux)
  - Infosec knowledge
  - Programming Skills
  - CTF Competitions

Continue..

TM
C E H
Certified Ethical Hacker

eLearnSecurity Web application Penetration Tester eXtreme
eWPTX

eLearnSecurity Web application Penetration Tester
eWPT

eLearnSecurity Certified Penetration Tester eXtreme
eCPTX

eLearnSecurity Certified Professional Penetration Tester v2
eCPPT v2

TM
E C S A
EC-Council Certified Security Analyst

OFFENSIVE ®
security
OSWP

TM
L P T
Licensed Penetration Tester
MASTER

GIAC WEB APP PEN TESTER
GWAPT

GIAC CERTIFIED PENETRATION TESTER
GPEN

OFFENSIVE ®
security
OSCP

CERTIFIED
RED TEAM
PROFESSIONAL

Golden Rule

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

Any Questions, Comments or Concerns?

Thank you!

Website : https://www.technawi.net
Linkedin : https://www.linkedin.com/in/mohammad-khreesha-97b324a2/
Twitter: @banyrock
Facebook : http://www.fb.com/khreesha
Youtube : https://www.youtube.com/technawidotnet
Email: khreesha@technawi.com