25-Sep-2019

Information security:
Agents, Attacks, and Tools

Joseph Bugeja

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

Doktorander I Lärande

KK-stiftelsen

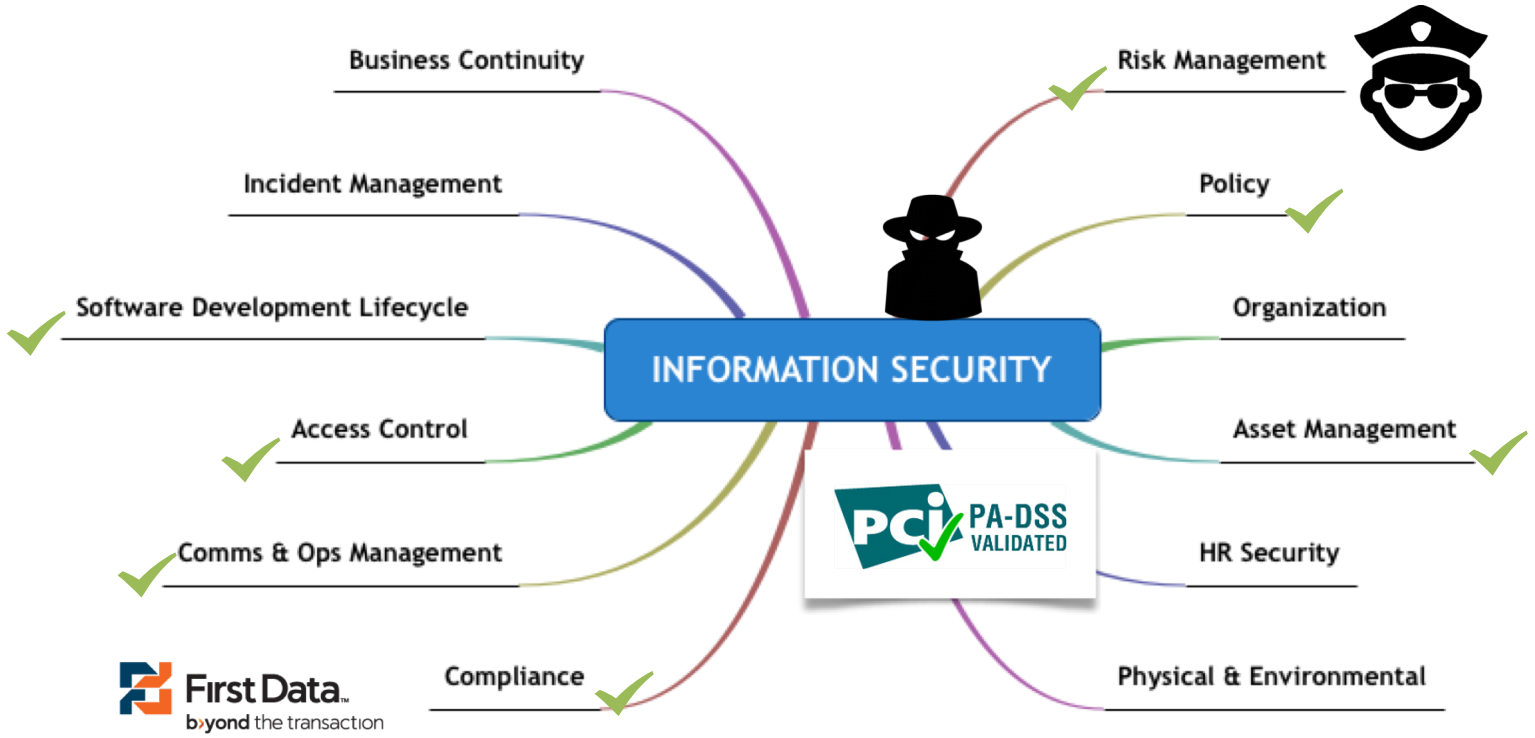
ABOUT ME

- ✓ Lic in Computer Science, MSc in Information Security
- ✓ 14 years working in the software industry

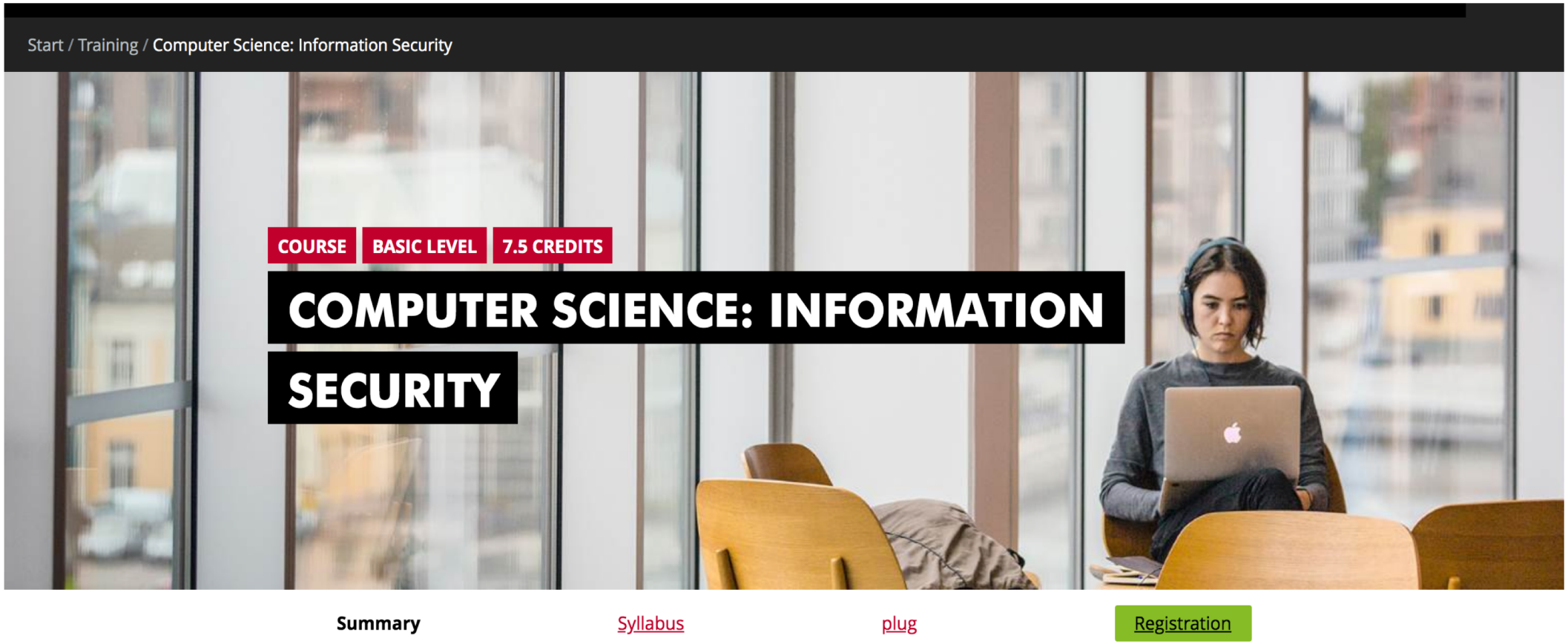
- ✓ Phd student in Computer Science
- ✓ Main research themes: security, privacy, and Internet of Things

PROFESSIONAL INFORMATION SECURITY DUTIES

✓ **Information Security Management Duties**

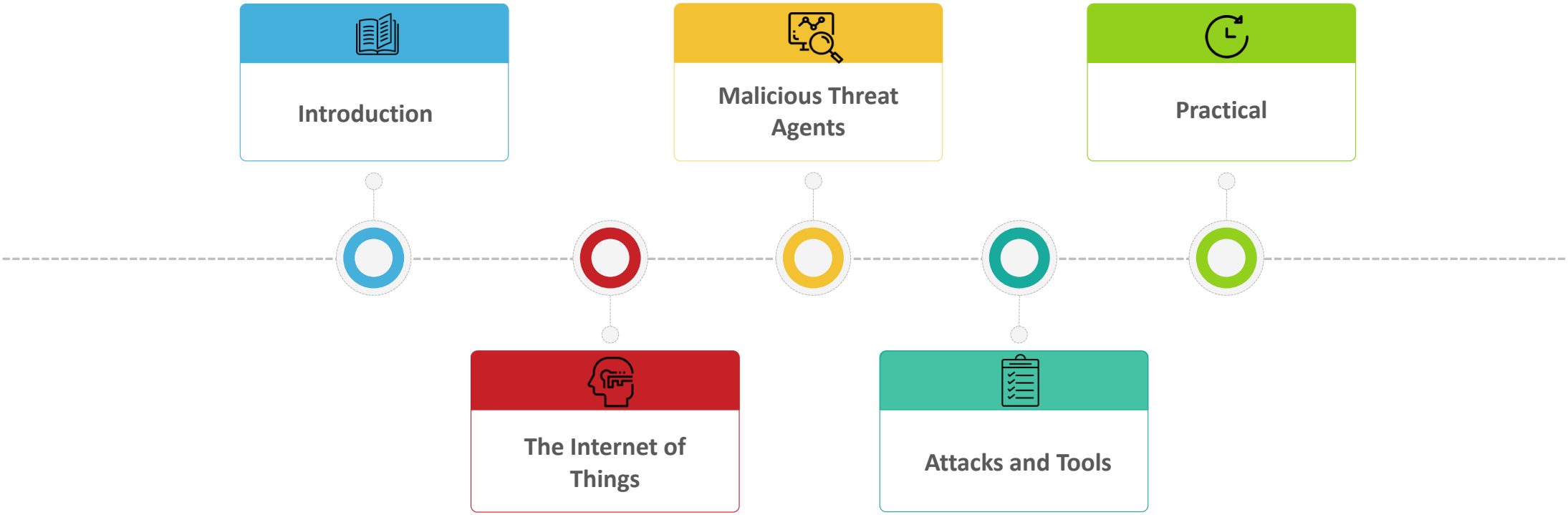


TEACHING RESPONSIBILITIES AT MALMÖ UNIVERSITY



Source: https://edu.mah.se/sv/Course/DA351A

AGENDA

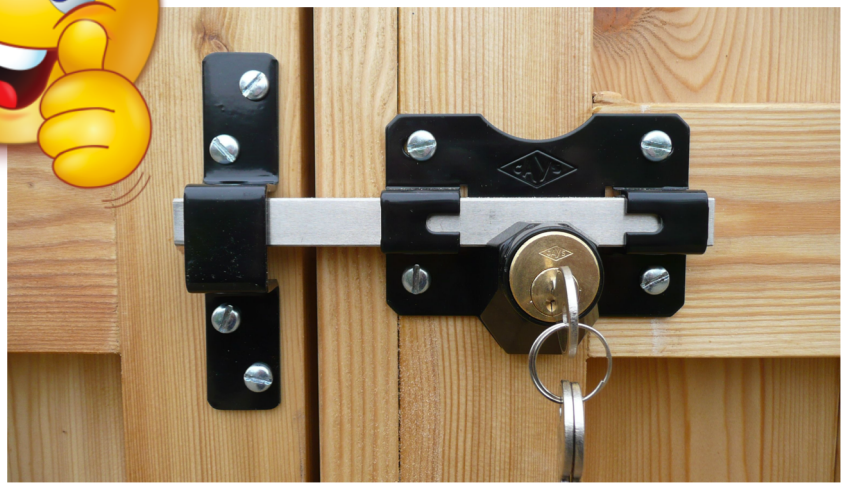

Introduction
The Internet of Things
Malicious Threat Agents
Attacks and Tools
Practical

INTRODUCTION

A WHILE AGO AND STILL

Fences

Seals



Locks

Signatures

Do you think this is enough to be secure nowadays?

THE SITUATION NOWADAYS

How can we ‘lock’ these things?

Smart speakers

Wearables

Drones

Smart toys

SECURITY THINKING

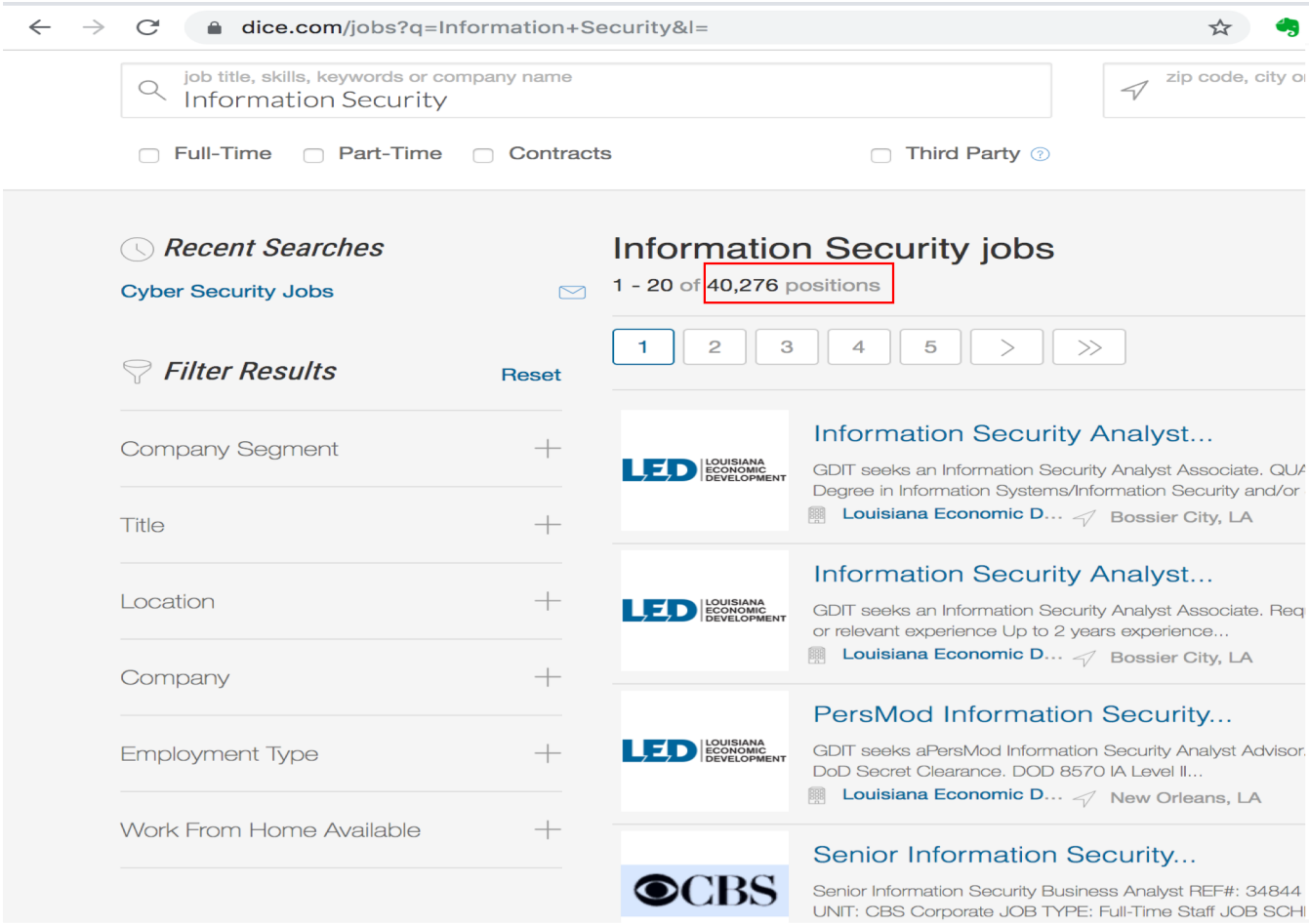
Physical

Informational

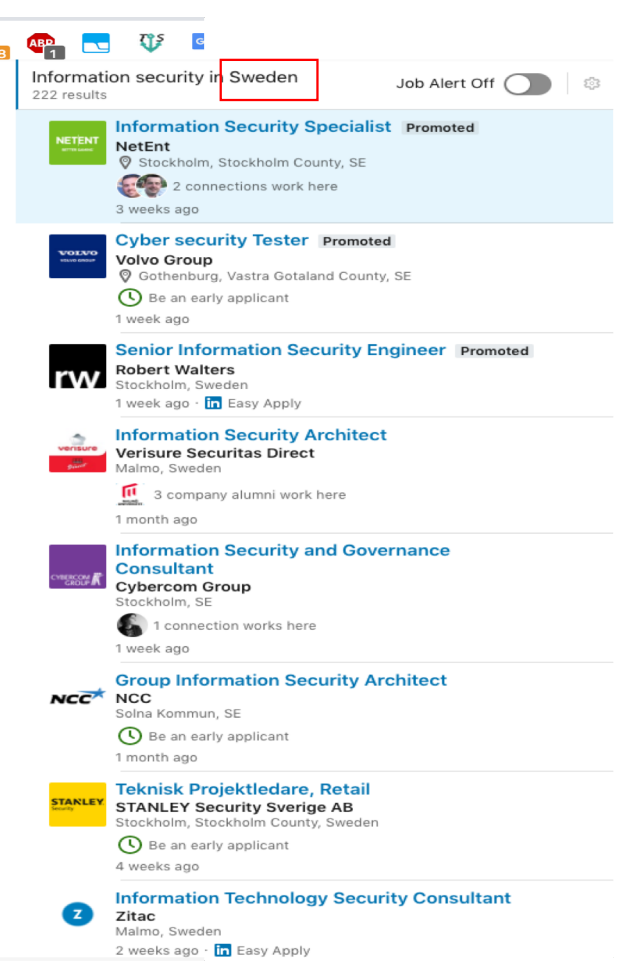
+

People

INFORMATION SECURITY JOBS



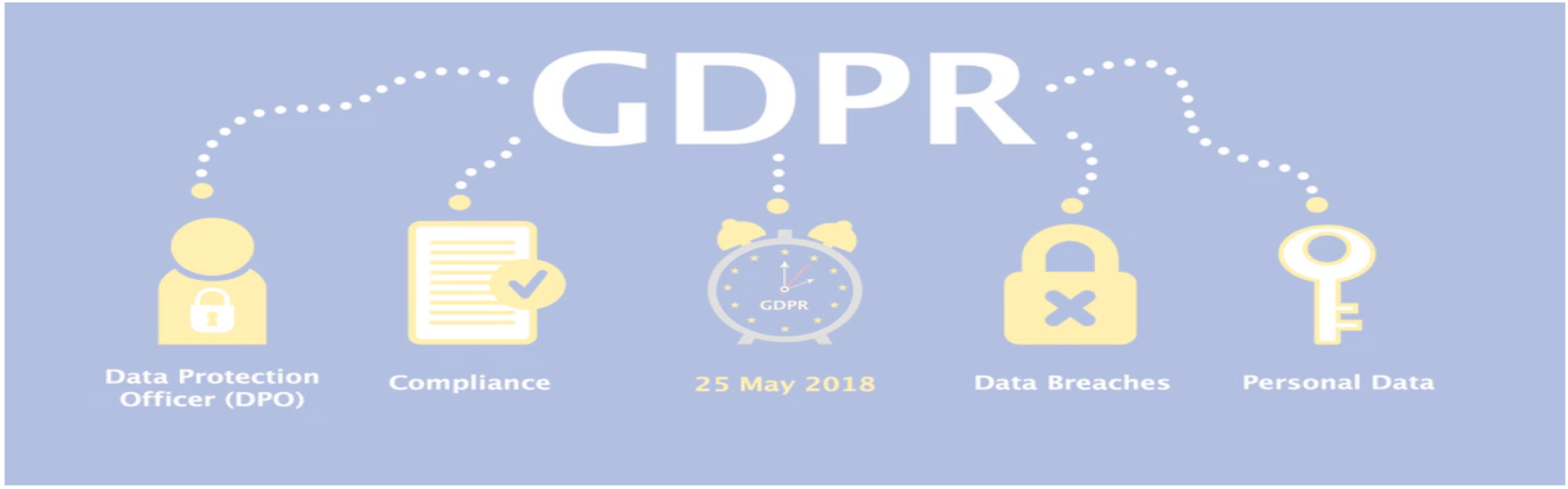
Source: Dice



Source:LinkedIn

GDPR introduces a new job position: The data protection officer

IAPP says that as many as 75,000 DPOs may be required worldwide to comply with the regulation.



SECURITY AND PRIVACY OF CITIZENS IS AT RISK

- ✓ 73,000 private video cameras leaking live footage (2014)

SECURITY AND PRIVACY OF CITIZENS IS AT RISK

✓ Smart devices may jeopardize your security and privacy

"Hackers could steal personal information and turn the microphone of the doll into a surveillance device"

"A hacker could crank up the temperature of a smart thermostat to a sweltering 99 degrees"

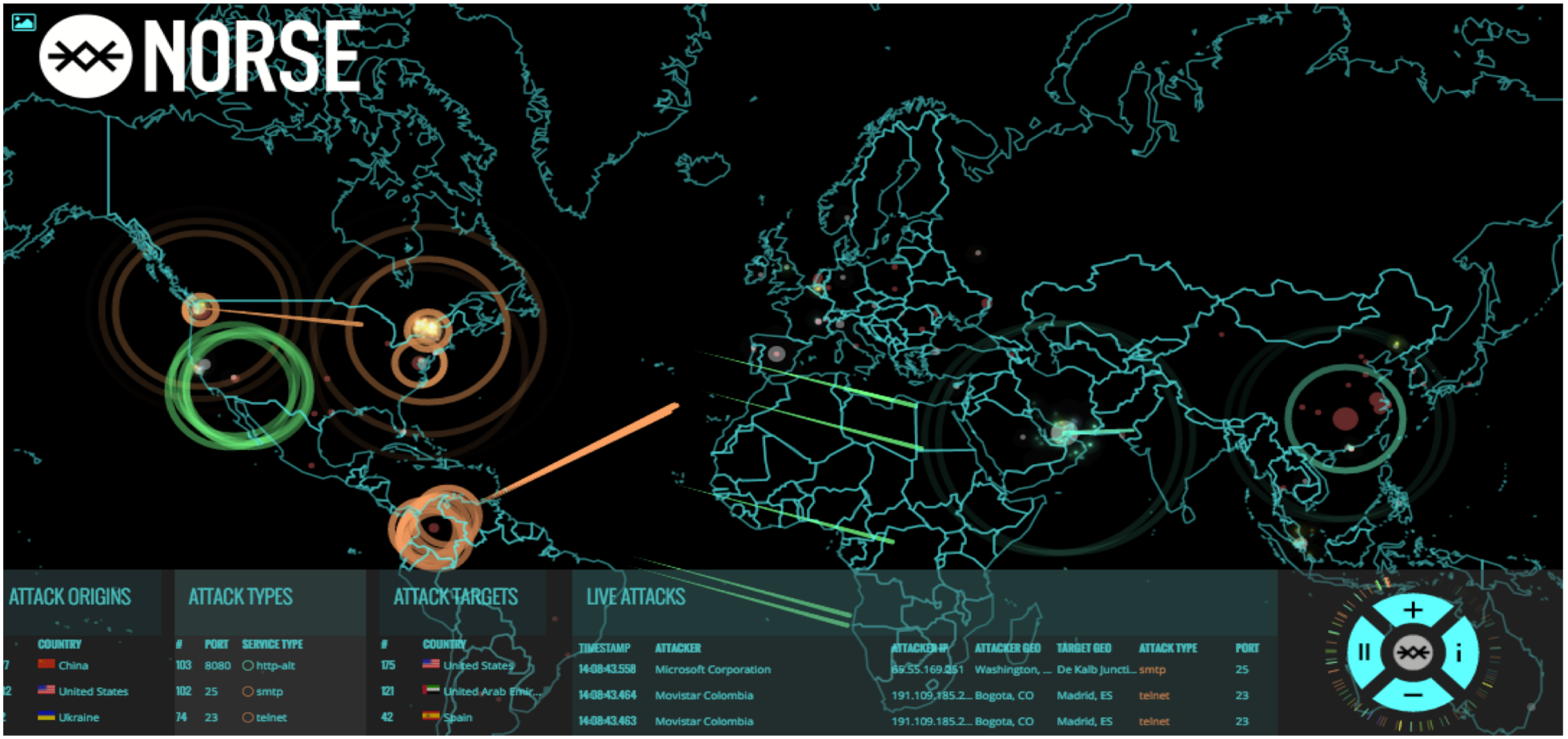
Ransomware PoC FTW!

#Defcon24 #wargames @IoTvillage

Hackers demonstrated first ransomware for IoT thermostats at DEF CON

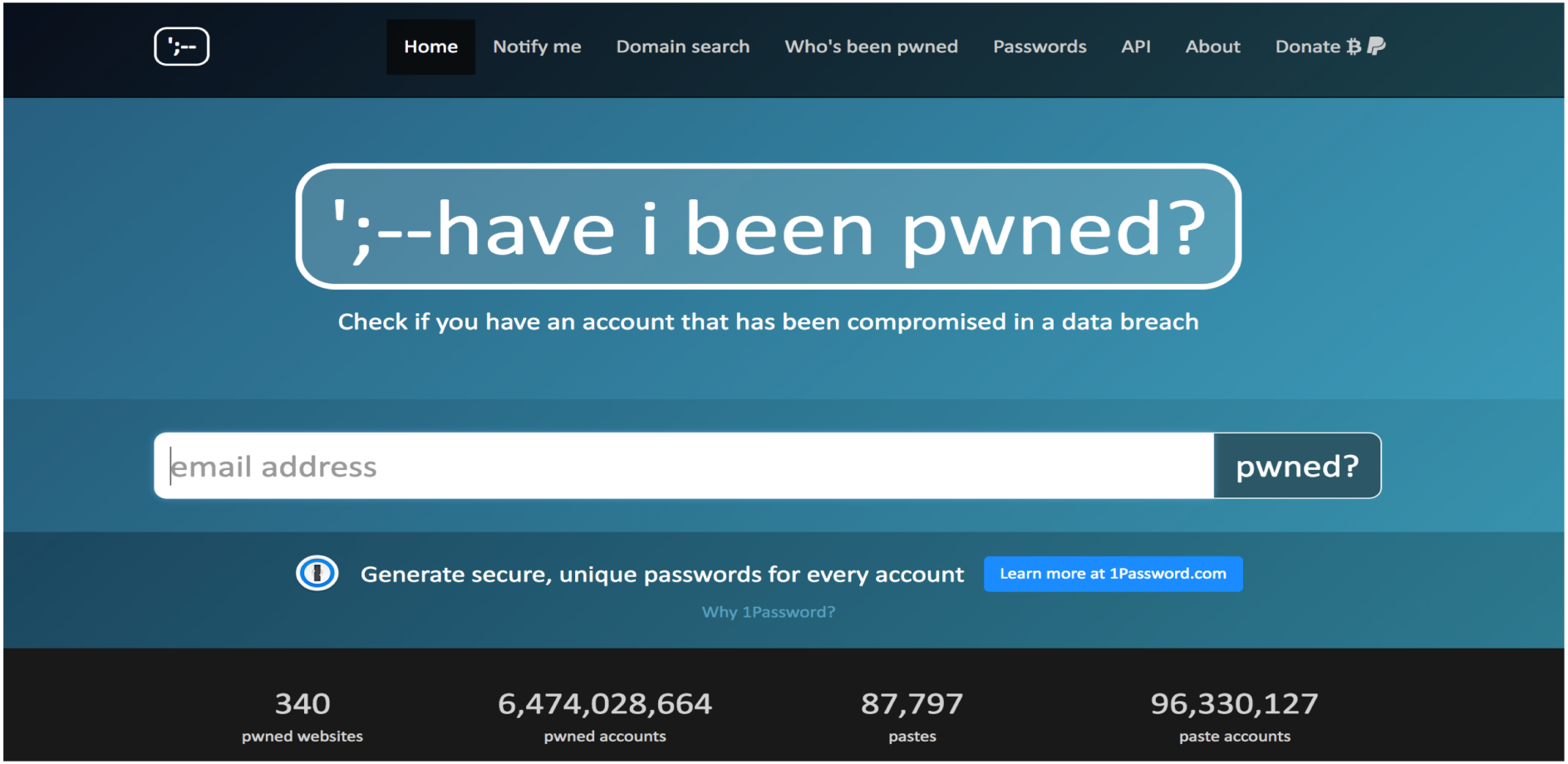
"After hearing the anchor's comment, their own devices also tried to order pricey dollhouses"

EXAMPLES OF LIVE ATTACKS



http://map.norsecorp.com/#/

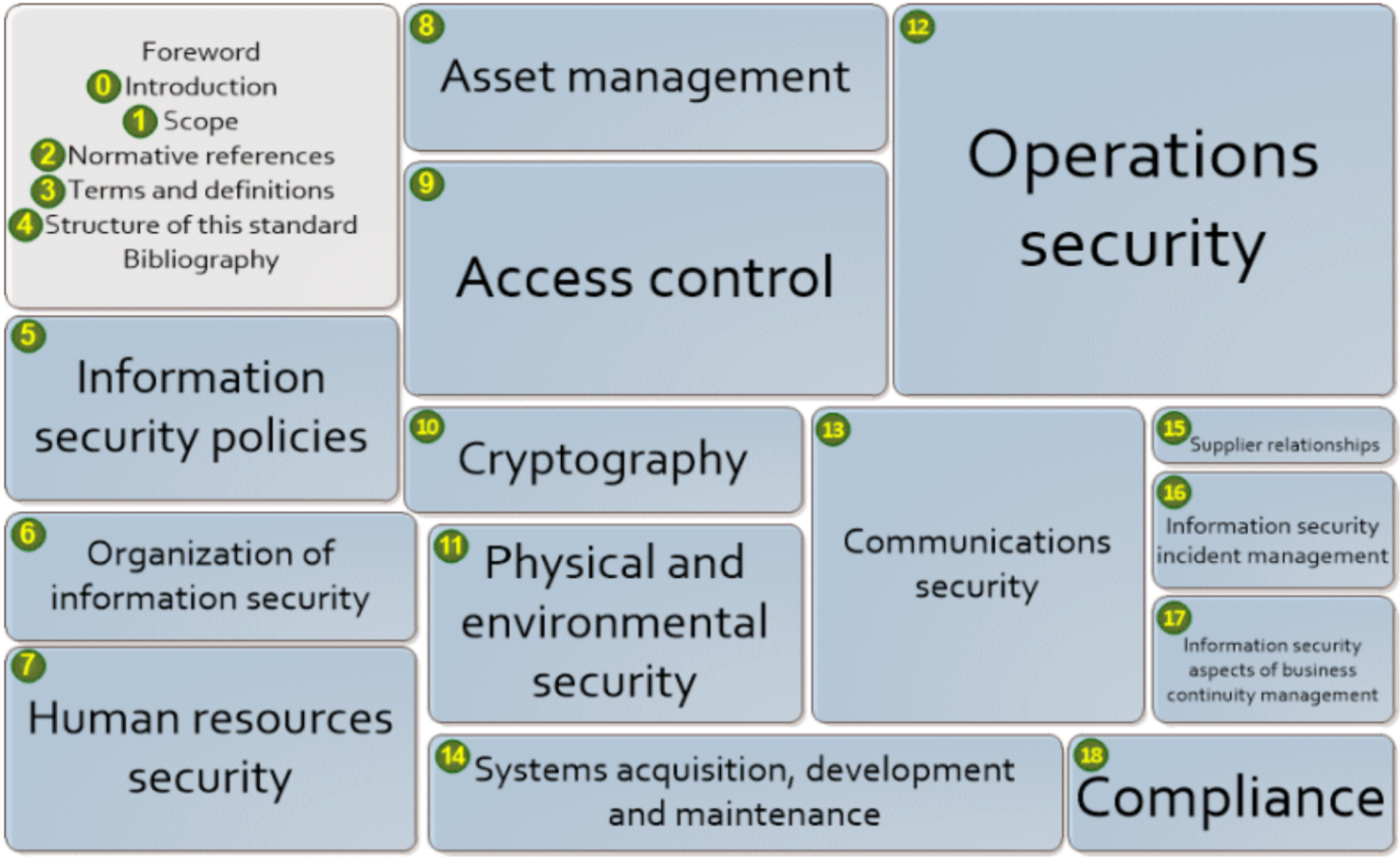
HAVE YOU BEEN HACKED!?



Source:https://haveibeenpwned.com/

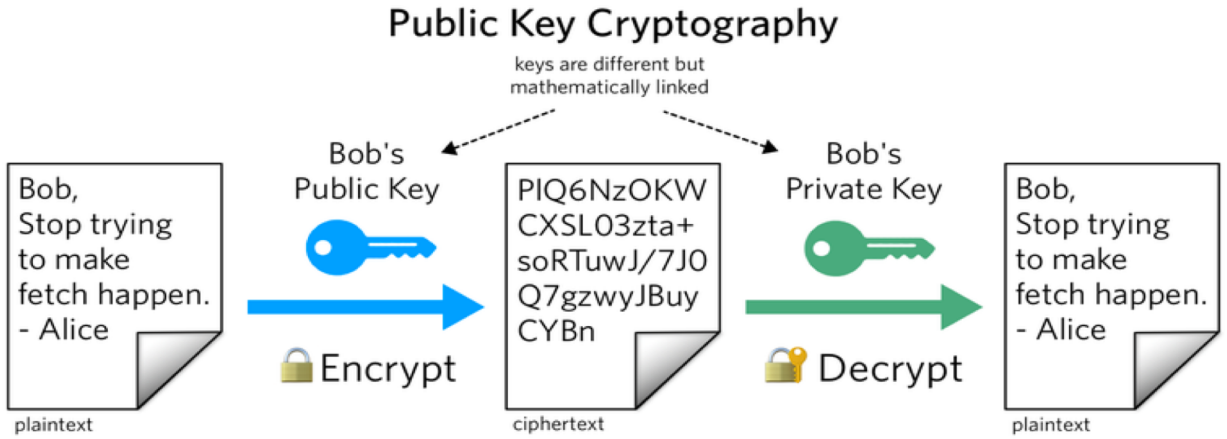
WHAT YOU MAY THINK IS INFORMATION SECURITY

THE DIFFERENT DIMENSIONS OF INFORMATION SECURITY



SECURITY INCORPORATES A WIDE SPECTRUM OF SKILLS

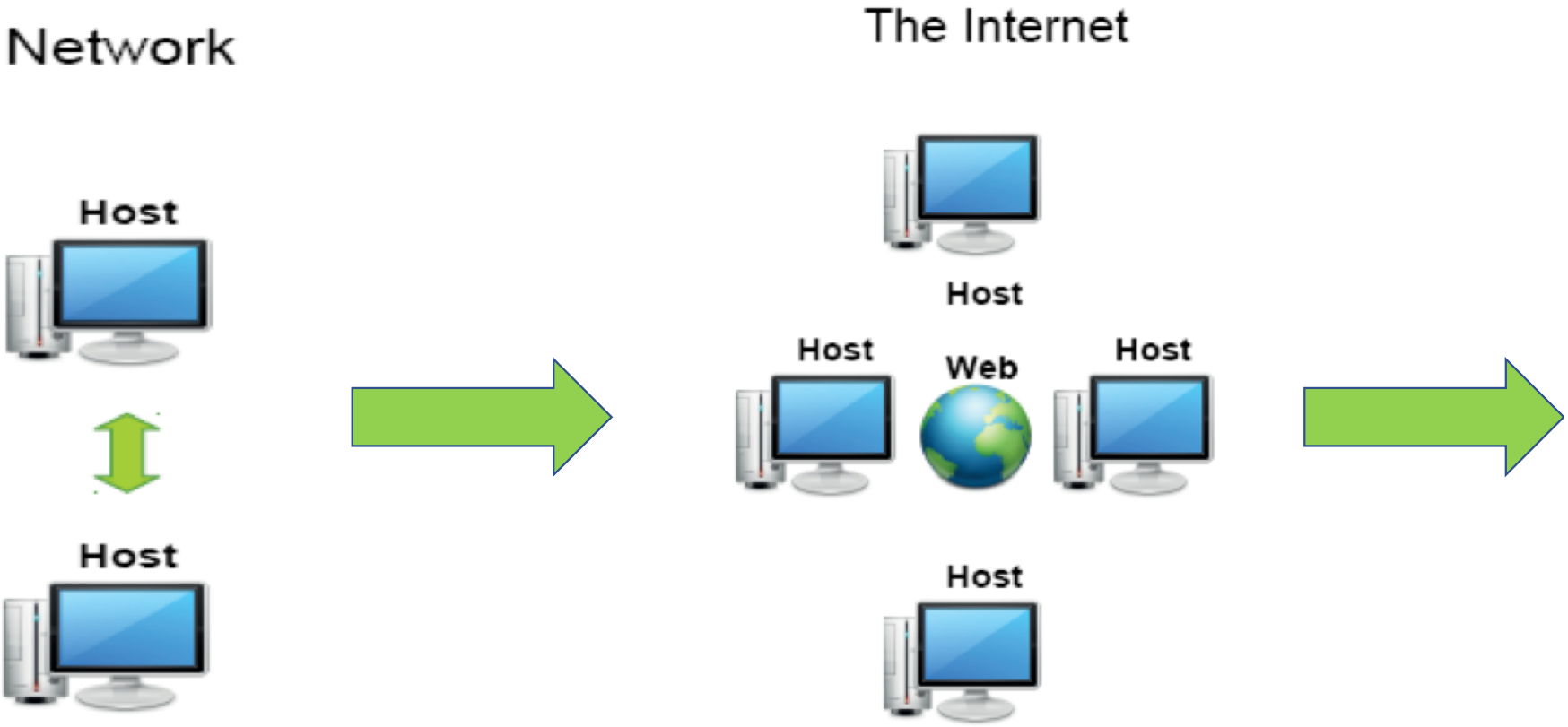
MATHEMATICAL



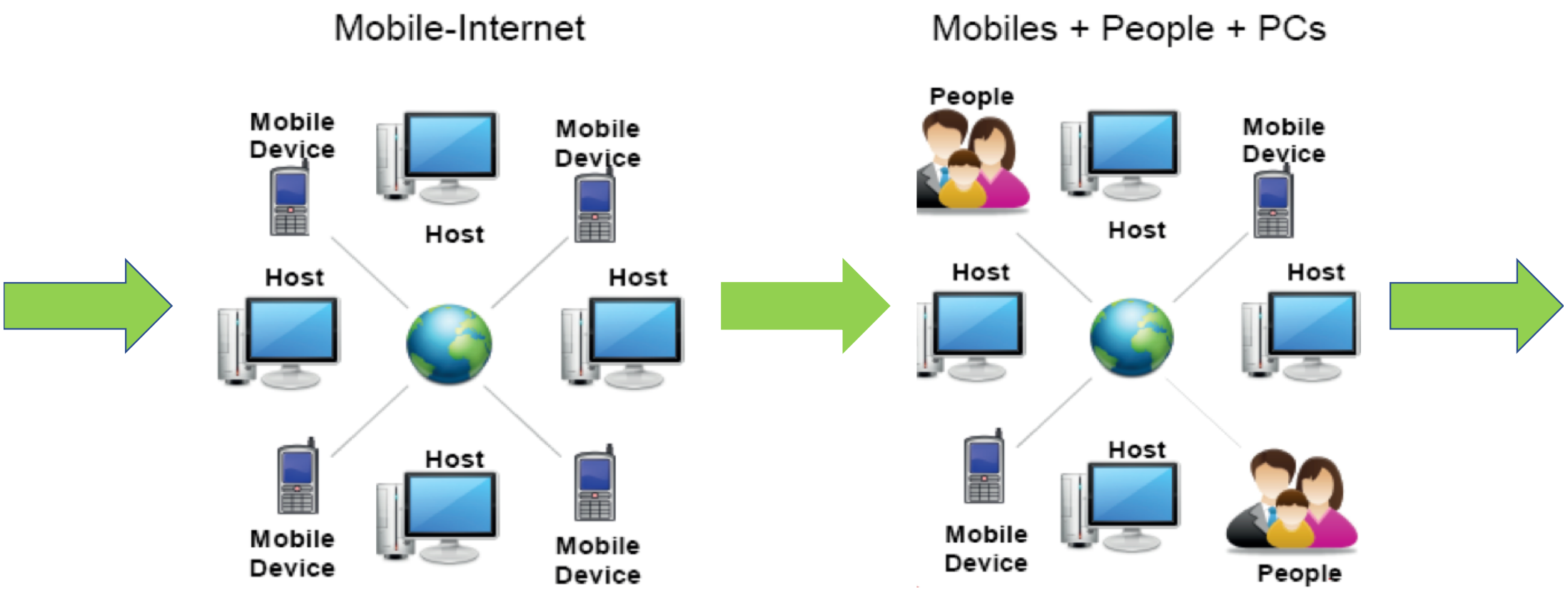
MANAGERIAL

The Internet of Things

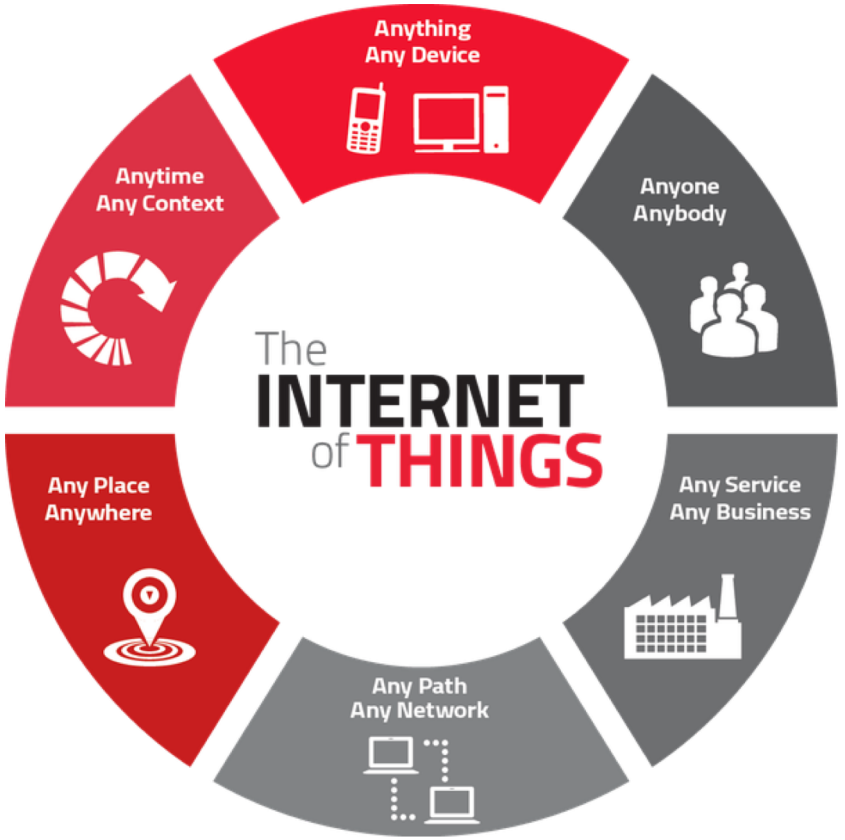
THE EVOLUTION OF NETWORKING



THE EVOLUTION OF NETWORKING



THE INTERNET OF THINGS



THE INTERNET OF THINGS

- Smart Home
- Wearables
- Smart City
- Smart grid
- Industrial internet
- Connected car
- Connected Health
- Smart retail
- Smart supply chain
- Smart farming

THE INTERNET OF THINGS

- ✓**Over 20 billion** Internet of Things (IoT) devices by 2020
- ✓Internet-connected devices will **outnumber people** at least 2:1
- ✓Global **market size of about $457B** by 2020

THE TRADITIONAL HOME

- ✓ Well-defined (solid) perimeter
- ✓ Mostly, uses wired technologies
- ✓ Human persons accessing the home

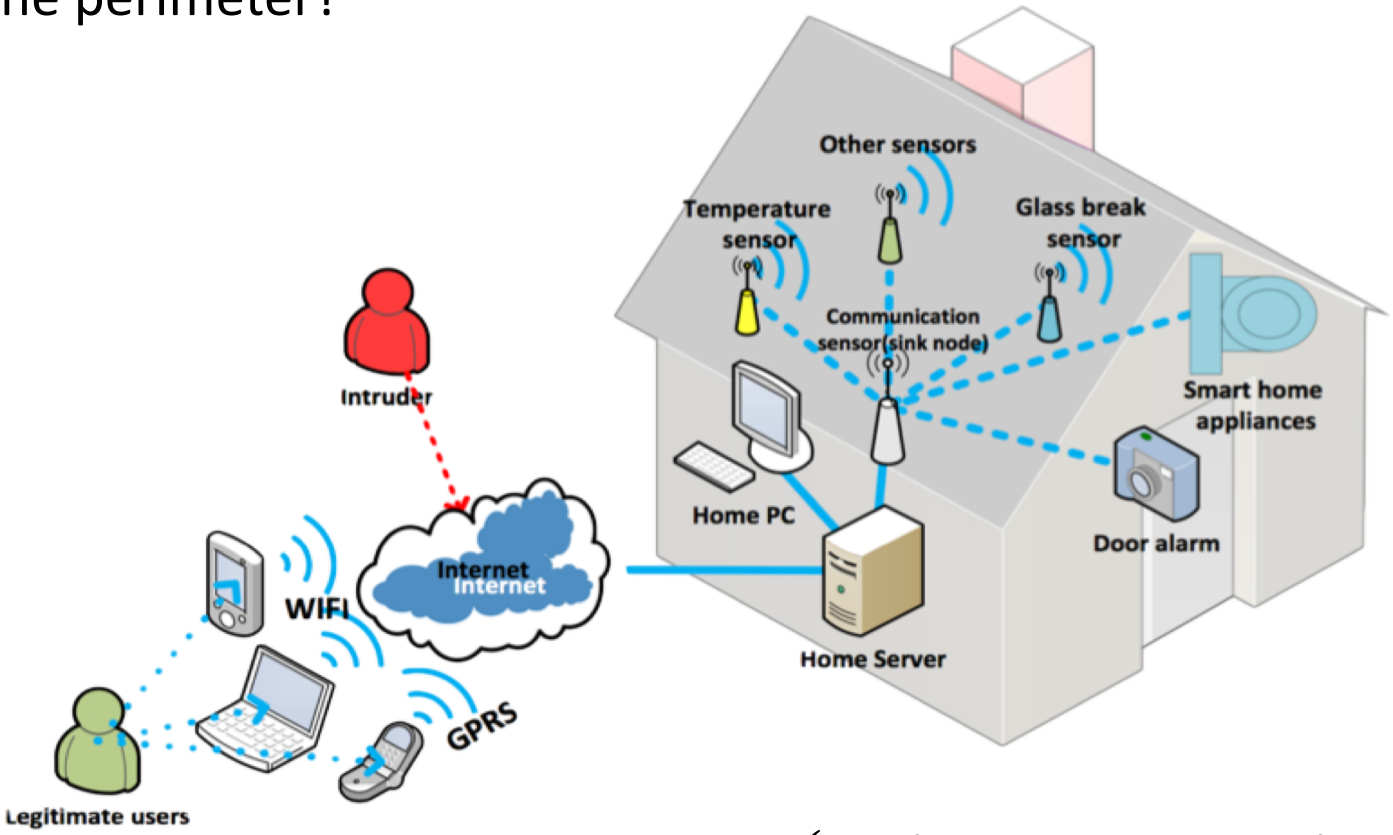
THE SMART CONNECTED HOME

- ✓ A smart connected home leverages IoT technologies to improve the quality and efficiency of life to the residents

Image: Shutterstock

THE SMART CONNECTED HOME

- ✓ Where is the perimeter?



- ✓ Where is my guest list?

MALICIOUS THREAT AGENTS

FOCUS ON THE ENEMIES

"*Know your enemy* and know yourself and you can fight a thousand battles without disaster"

- Sun Tzu

LICENTIATE THESIS

MALICIOUS THREAT AGENTS

HACKERS

- ✓ Individuals (“hobby hackers”) that include malicious persons, script kiddies, and nosy employees of an organization

SHODAN
Computer Search Engine

- ✓ Viruses, worms, phishing
- ✓ Primarily motivated by curiosity
- ✓ Skill-level: Apprentice

Low

THIEVES

- ✓ Opportunistic individuals that are associated with stealing mostly for personal financial gain

- ✓ System/physical intrusion, DoS, spoofing

- ✓ Main motive is monetary gain

- ✓ Skill-level: Apprentice

Low

HACKTIVISTS

- ✓ Individuals or members of a larger group that pursue a political or social agenda

- ✓ DoS, fraud, and identity theft

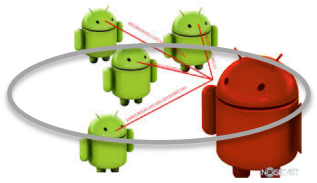
- ✓ Primarily aim to promote and publicize their cause

- ✓ Skill-level: Apprentice

Low

COMPETITORS AND ORGANIZED CRIME

- ✓ Commercial competitors that compete for revenues or resources, and private criminal organizations



- ✓ Botnets, ransomware, and inside information

- ✓ Competitive advantage, CI, and monetization

- ✓ Skill-level: Journeyman

TERRORISTS

- ✓ Individuals that rely on violence or fear-related behavior to support personal socio-political agenda

- ✓ Damage/loss, outages, and physical attacks
- ✓ Terrorism
- ✓ Skill-level: Master

High

NATION STATES

- ✓ Highly sophisticated individuals that are funded by governments and associated with a military unit

ADVANCED PERSISTENT THREAT

- ✓ Customized malware, spear phishing attacks, and zero-day attacks

- ✓ Cyber warfare, (counter-)intelligence

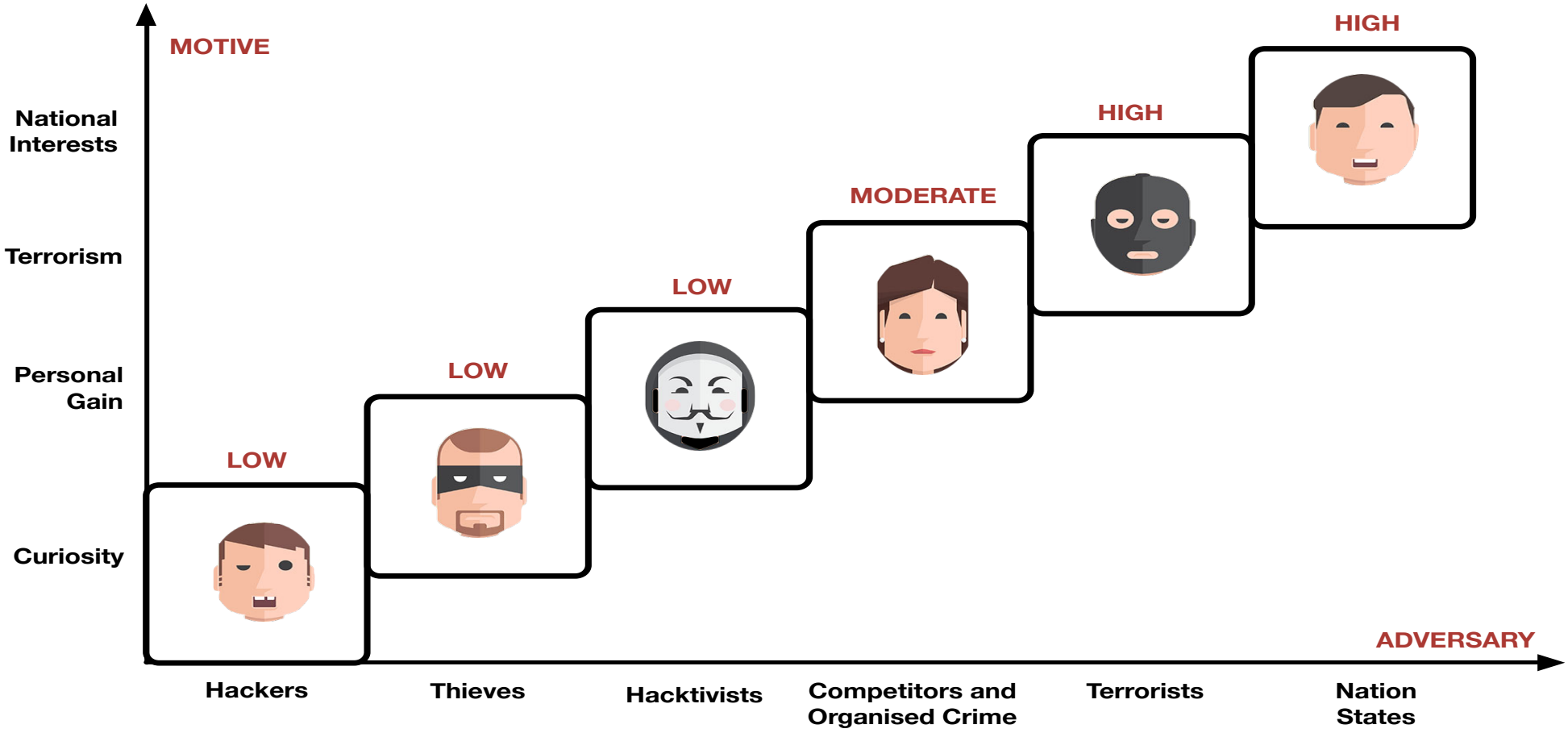
- ✓ Skill-level: Master

High

THREAT AGENT SKILLS

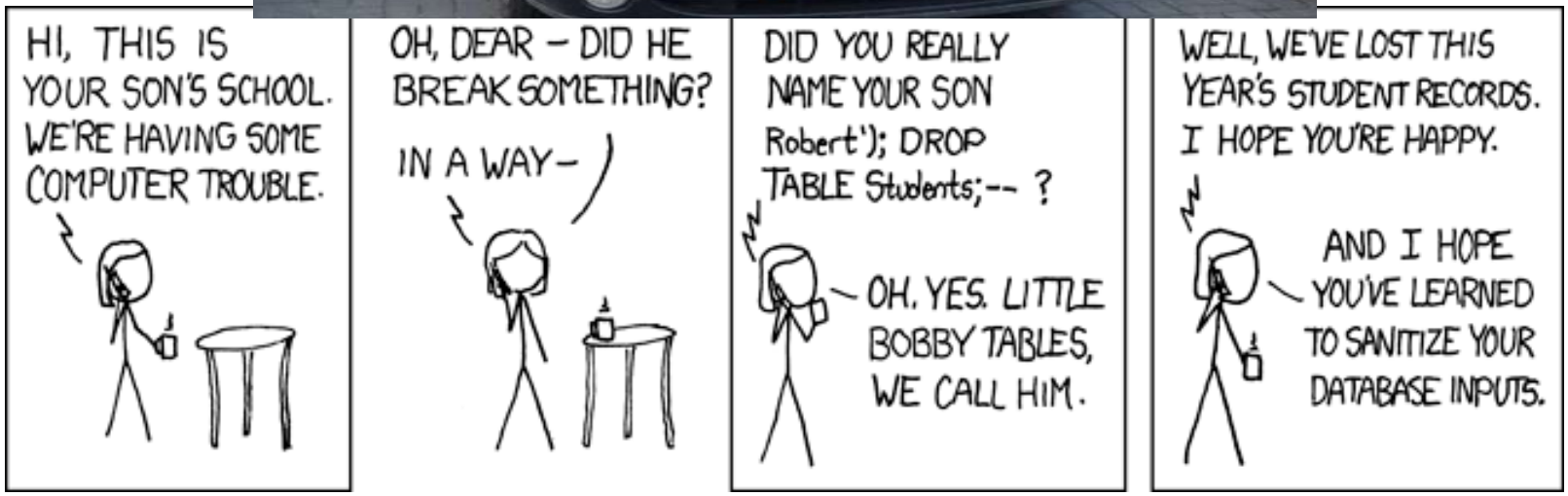
Low	Medium	High
Minimal technical skills 	Sufficient technical skills 	High-level technical skills 
Largest number of attackers	Locate new vulnerabilities	Write new powerful attack toolkits
Easiest to defend against	Threat agents with such skills are likely found in all classes	Hardest to defend against

THREAT MODEL

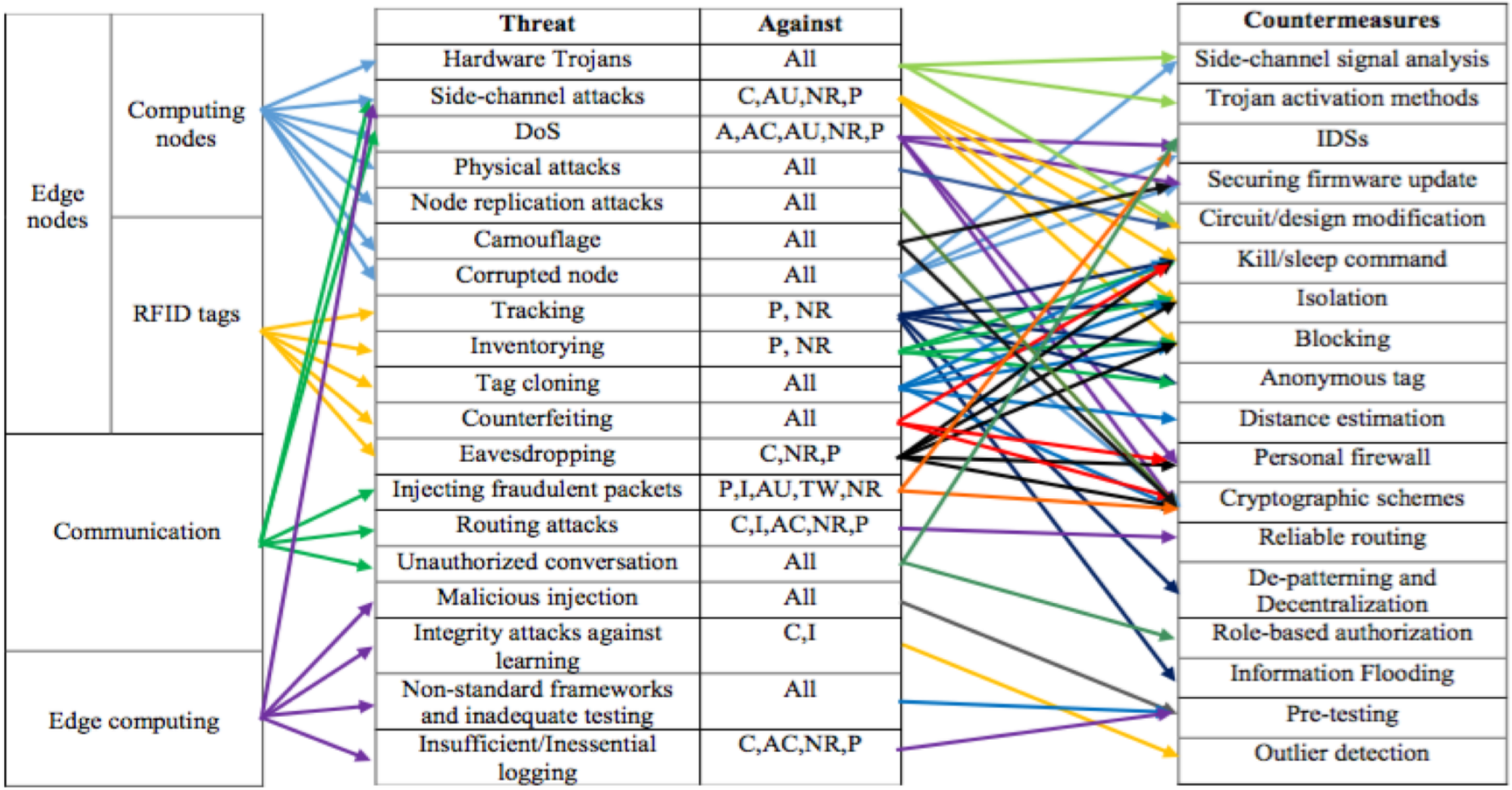


ATTACKS AND TOOLS

SQL INJECTION ATTACKS

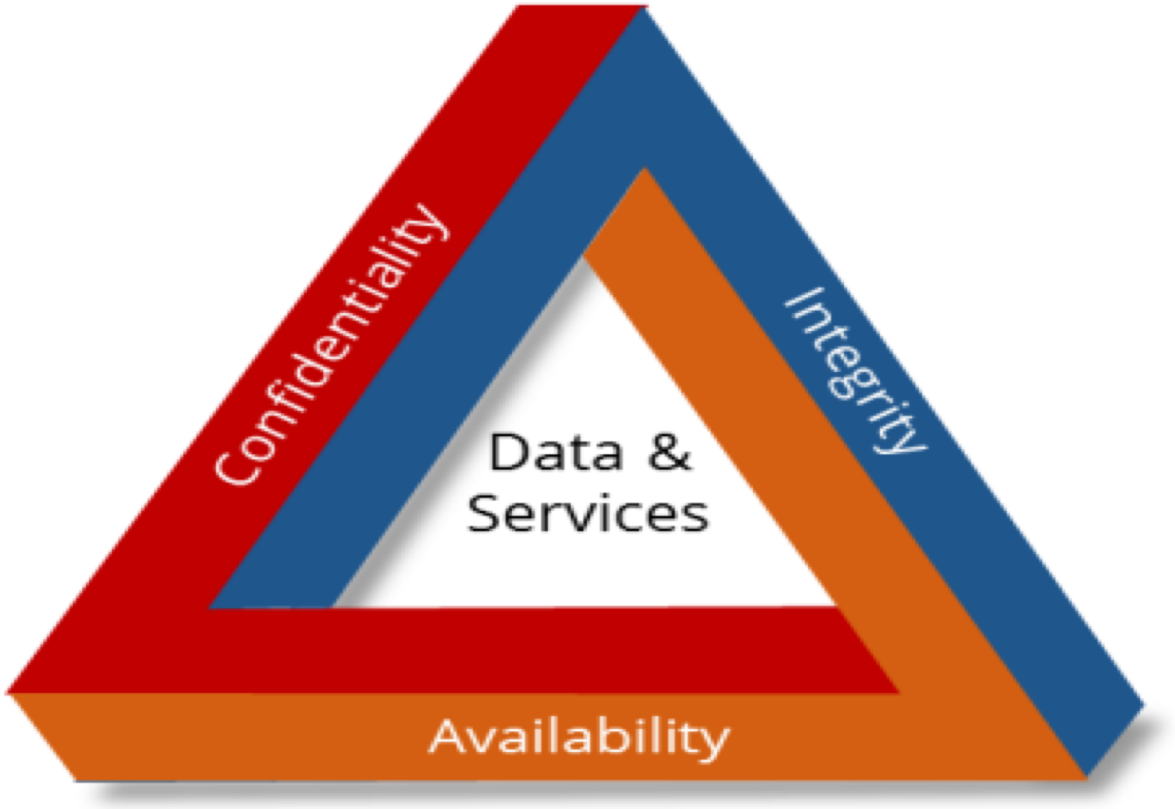


IOT ATTACKS AND COUNTERMEASURES



Source: Mosenia et al. "A comprehensive study of security of internet-of-things." *IEEE Transactions on Emerging Topics in Computing* 5.4 (2016): 586-602.

THE CIA TRIAD



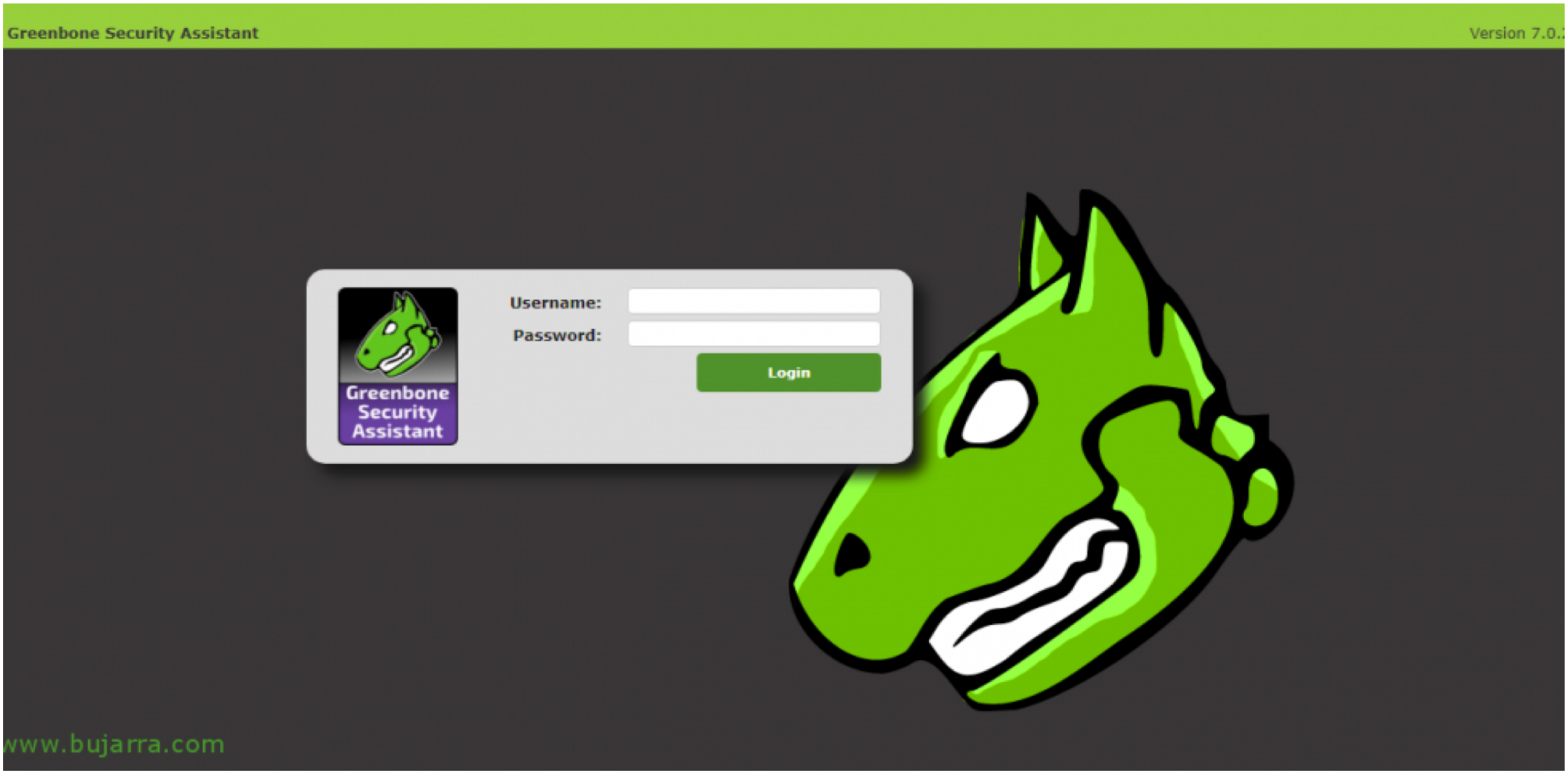
SECURITY TESTING TOOLS

- ✓There are a variety of toolsets used by security professionals that could also be used for malicious purposes
- ✓These toolsets are used by penetration testers when testing the security posture of a system
- ✓The same tools in the hands of an adversary can be used for malicious purposes

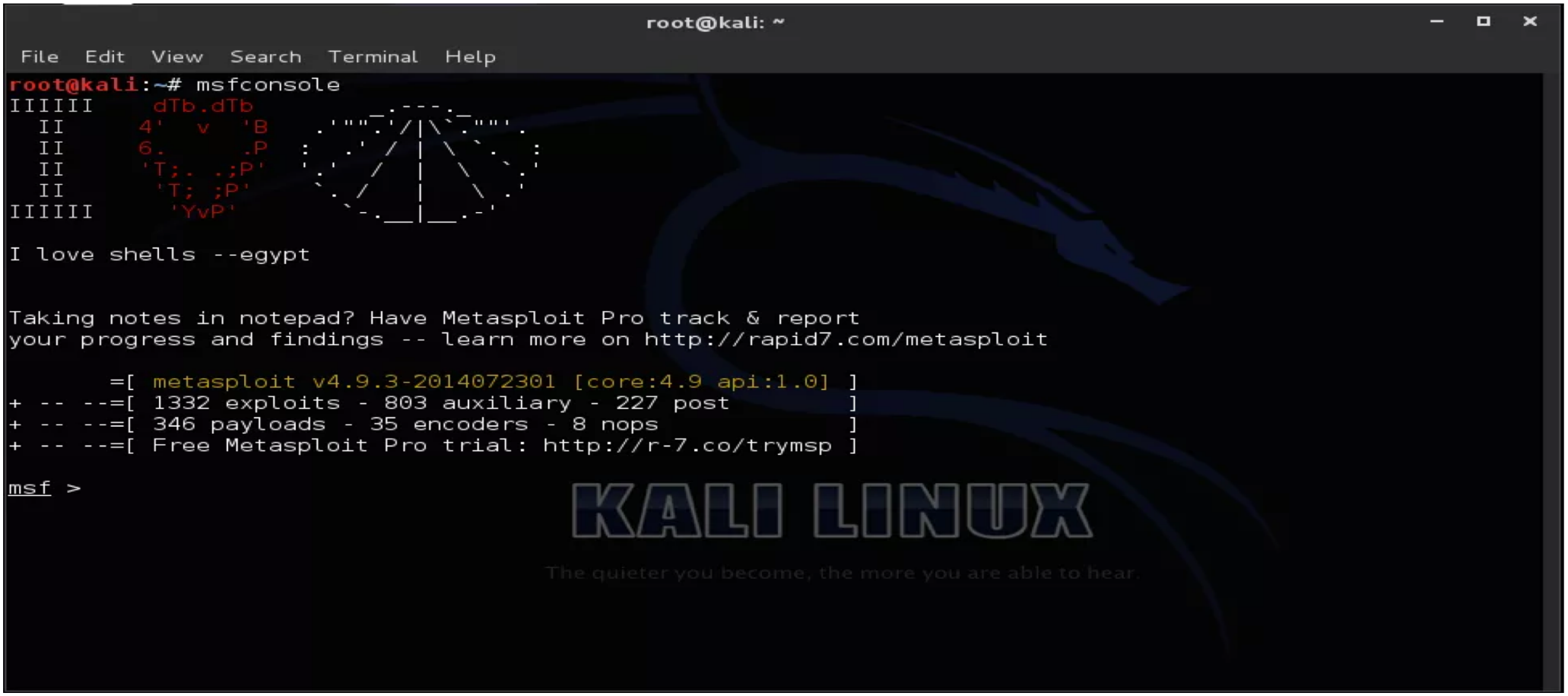
KALI LINUX


Applications
Places
Fri 13:48
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Activities Overview
Iceweasel
Terminal
Files
metasploit...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad
Tweak Tool

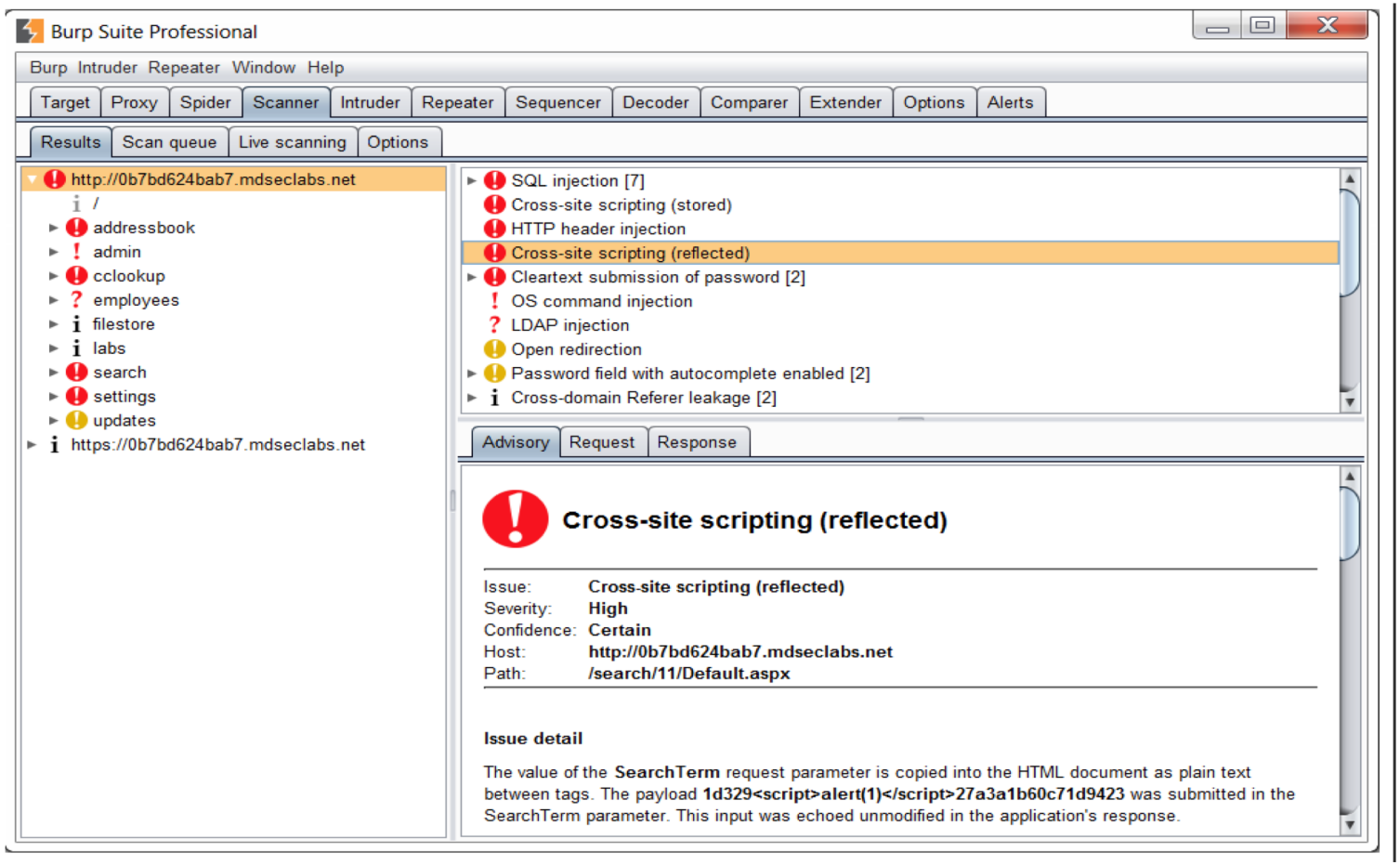
OPENVAS VULNERABILITY SCANNER



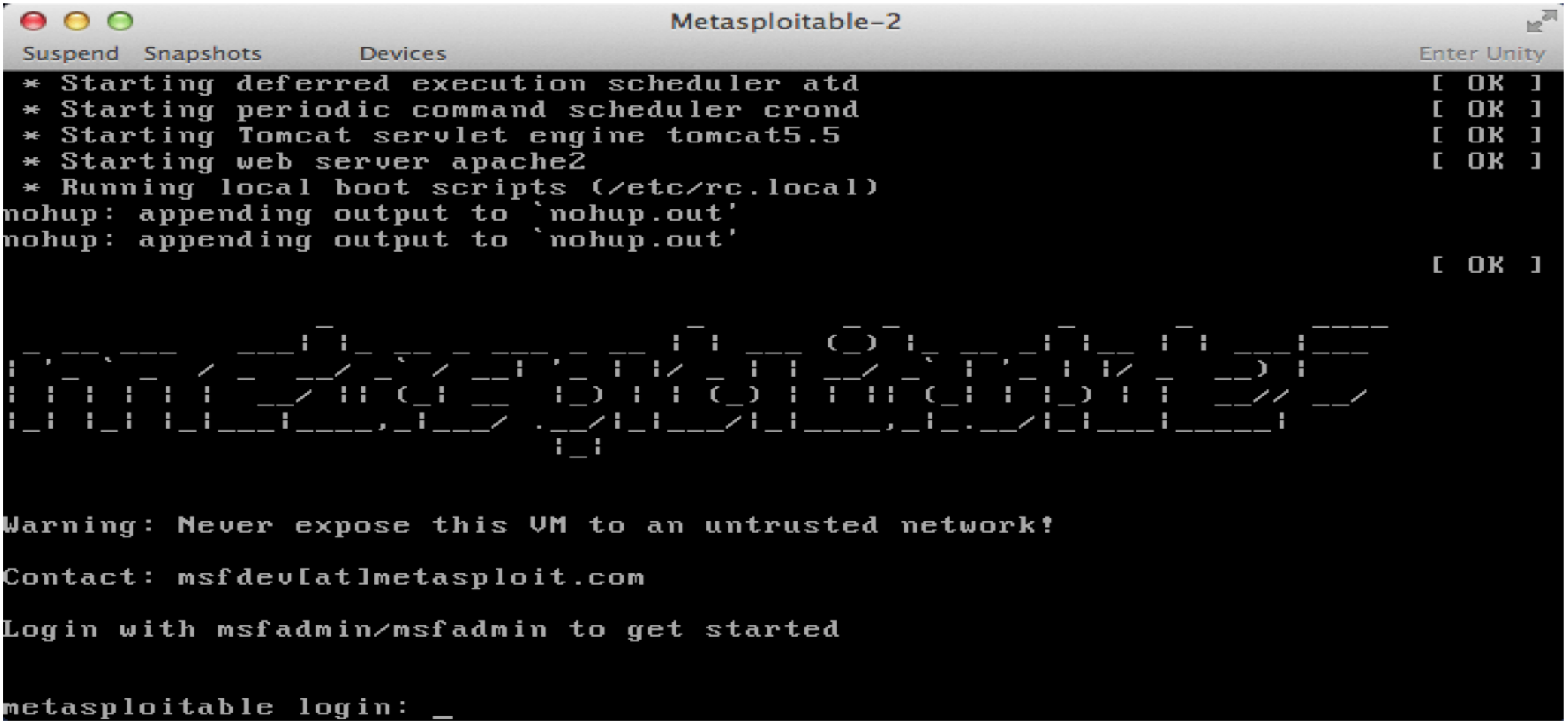
METASPLOIT


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
I love shells --egypt
Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit
=[metasploit v4.9.3-2014072301 [core:4.9 api:1.0]]
+ -- --=[1332 exploits - 803 auxiliary - 227 post]
+ -- --=[346 payloads - 35 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >
KALI LINUX
The quieter you become, the more you are able to hear

BURP SUITE


Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Results Scan queue Live scanning Options
http://0b7bd624bab7.mdseclabs.net
/
addressbook
admin
cclookup
employees
filestore
labs
search
settings
updates
https://0b7bd624bab7.mdseclabs.net
SQL injection [7]
Cross-site scripting (stored)
HTTP header injection
Cross-site scripting (reflected)
Cleartext submission of password [2]
OS command injection
LDAP injection
Open redirection
Password field with autocomplete enabled [2]
Cross-domain Referer leakage [2]
Advisory Request Response
Cross-site scripting (reflected)
Issue: Cross-site scripting (reflected)
Severity: High
Confidence: Certain
Host: http://0b7bd624bab7.mdseclabs.net
Path: /search/11/Default.aspx
Issue detail
The value of the SearchTerm request parameter is copied into the HTML document as plain text between tags. The payload 1d329<script>alert(1)</script>27a3a1b60c71d9423 was submitted in the SearchTerm parameter. This input was echoed unmodified in the application's response.

METASPLOITABLE



PRACTICAL

SHORT DEMONSTRATION

John

Fortinet Threat Map

Shodan


THANK YOU
FOR YOUR
ATTENTION !
FULLCIRCLE SECURITY
Expertise. Knowledge. Success.
bugejajoseph.com
HOME
ACADEMIC
PRESENTATIONS
SERVICES
ABOUT
CONTACT