WHY THE GOOD GUYS NEED TO THINK LIKE BAD GUYS

CYBERSECURITY PROFESSIONALS KEEP ORGANIZATIONS AND THEIR ASSETS SECURE BY LEARNING THE BAD GUYS' TRICKS OF THE TRADE.

RYAN VANDENBERG
CISSP, CISM

BIO – RYAN VANDENBERG

- Cybersecurity consultant, full-stack software engineer, development manager
- Certifications:
  - CISSP, CISM | eJPT, PenTest+ | Security+, Network+, A+ | AWS Cloud Practitioner
- Previous Companies:
  - Aspire Ventures – Chief Security Officer, Program Manager, Senior Software Engineer
  - Wylei – Co-founder & Vice President, Product Management
- Volunteering:
  - The GateHouse – Board Member; Information Technology Committee, Analytics Committee

AGENDA

- Why we need to think like bad guys
- Who the bad guys are
- Why we must use our powers for good and not evil
- What the bad guys are up to
- What tools the bad guys are using

TERMINOLOGY

- **Threat** – a potential occurrence that can result in an undesirable outcome. This includes potential attacks by criminals or other attackers.
- **Vulnerability** – any type of weakness. The weakness can be due to a flaw or limitation in hardware or software. It can also be the absence of a security control, such as the absence of anti-virus software on a computer.
- **Exploitation** – action of launching a threat against an asset.

Source: (ISC)2 Certified Information Systems Security Professional Official Study Guide

BURGLAR ANALOGY

If you never check the locks on your home's doors and windows, can you be sure that they're adequately securing you and your family?

This is why we must think like a bad guy.

Your home is like a corporate network or business website.

WHO IS JIGGLING THE DOORKNOB?

More terminology:

- **White hat** – aka “ethical hackers” who use their capabilities to uncover security issues to safeguard organizations from black hat hackers.
- **Black hat** – breaks into computer networks with malicious intent. Motivated by self-serving reasons.
  - **Script kiddie** – someone who runs premade scripts to try to find vulnerabilities. Often doesn’t understand what these scripts are really doing; unsophisticated.
  - **Hacktivist** – a hacker with a mission/goal. Possibly trying to create social change. Goals may be crashing your website or exfiltrating data from your network.
  - **Nation state actor** – Government funded experts often targeting national security. Very sophisticated and highly capable.

Sources: Resource Center Definitions – kaspersky.com; Threat Actors – professormesser.com

“WITH GREAT POWER COMES GREAT RESPONSIBILITY”

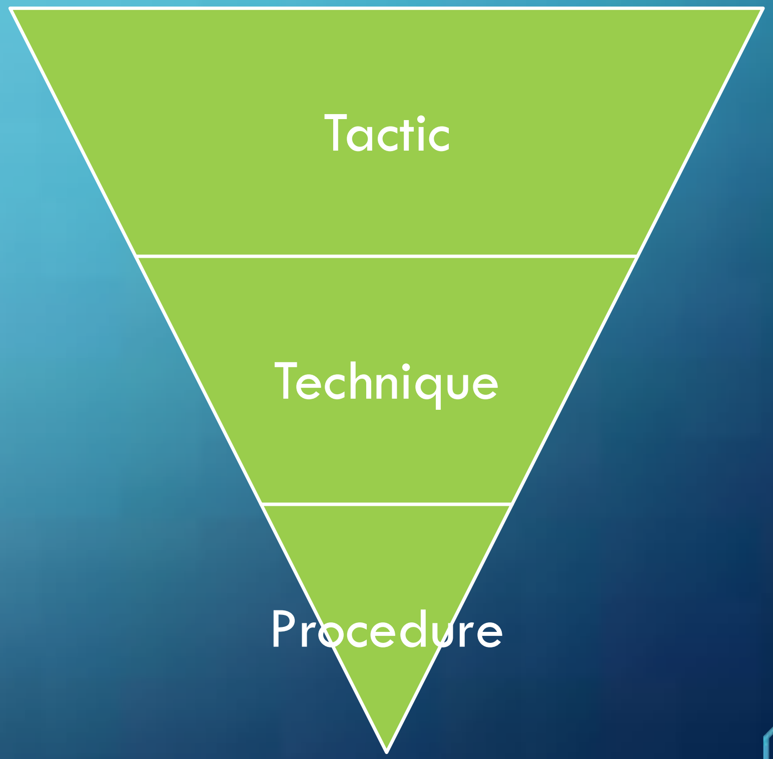
- Remember – we’re the good guys. Do not use these tools on targets without permission. Use preconfigured lab or home lab environments instead.
- Steven Levy describes the general tenets of hacker ethics including: sharing, openness, decentralization.

  Source: Hackers: Heroes of the Computer Revolution, Steven Levy
- “Computer hacking under 18 U.S.C. § 1030 and other related internet crimes often cross state lines due to the fact the computers in question are located in different states, meaning this type of white collar fraud crime can be prosecuted in a federal courtroom. The federal crime of computer hacking is normally prosecuted under the **Computer Fraud and Abuse Act.**”

  Source: Eisner Gorin LLP– egattorneys.com

TACTICS, TECHNIQUES AND PROCEDURES

- **Tactic** – highest-level description of this behavior (intended effect)
- **Technique** – gives a more detailed description of behavior in the context of a tactic (tool/ mechanism)
- **Procedure** – an even lower-level, highly detailed description in the context of a technique (execution)



RECONNAISSANCE

- If I sit across the street from your house, will I see you using the same key to unlock your car, your front door, your shed and your mailbox?
- Many people still reuse passwords despite the risks.
- Security Researcher Troy Hunt has created the website “Have I been pwned?” https://haveibeenpwned.com

646 pwned websites

12,441,047,441 pwned accounts

115,667 pastes

227,240,010 paste accounts

Largest breaches

- [illegible] Collection #1 accounts
- [illegible] Verifications.io accounts
- [illegible] Onliner Spambot accounts
- [illegible] Data Enrichment Exposure From PDL Customer accounts
- [illegible] Exploit.In accounts
- [illegible] Facebook accounts
- [illegible] Anti Public Combo List accounts
- [illegible] River City Media Spam List accounts

Recently added breaches

- [illegible] accounts
- [illegible] accounts
- [illegible] Twitter (200M) accounts
- [illegible] Deezer accounts
- [illegible] accounts
- [illegible] accounts
- [illegible] accounts
- [illegible] accounts
- [illegible] accounts
- [illegible] accounts

VULNERABILITY SCANNING

- Examining a door on the home, does it look like it will unlatch itself if I push on it?
- Is the type of doorknob that is installed the kind that will let me unlock it with a paperclip?
- Do we see panes of cracked glass that could be pushed in so that we can open the latch?

SHODAN

- “Shodan is a search engine for Internet-connected devices. Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between.”

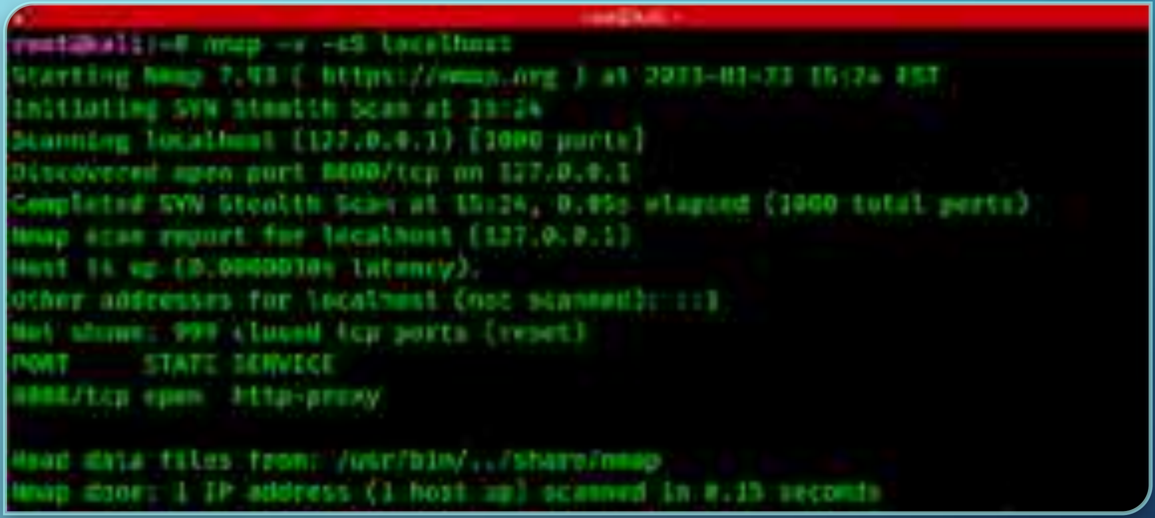
  Source: shodan.io

- Example: find all Citrix devices in Germany that are vulnerable to CVE-2019-19871

```
vuln:CVE-2019-19781 country:DE
```

NMAP

- Created by Gordon “Fyodor” Lyon in 1997
- Most commonly known as a port scanner, but it does much more - 14 categories of modules
- Output can be used in other tools
- GUI version available - Zenmap
- https://nmap.org



```
root@kali:~# nmap -v -sS localhost
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 15:24 EST
Initiating SYN Stealth Scan at 15:24
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 8080/tcp on 127.0.0.1
Completed SYN Stealth Scan at 15:24, 0.05s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp open  http-proxy

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

NESSUS

- Vulnerability scanning tool with reporting capabilities
- Created in 1998 by Renaud Deraison as a free remote security scanner
- In October 2005, the project changed from GNU Public License to a proprietary license
- It is now owned by company Tenable, Inc.
- Open-source forks still exist as OpenVAS and Greenbone
- https://tenable.com

PENETRATION TESTING

- Penetration testing goes beyond vulnerability testing techniques because it actually attempts to exploit systems. The tester tries to defeat security controls and break into a targeted system or application to demonstrate the flaw.

  Source: (ISC)2 Certified Information Systems Security Professional Official Study Guide

- Penetration testing started in the 1990s as “adversary simulation”. The objective wasn’t to find every potential security flaw but to instead attempt to identify likely attack patterns by malicious actors.
  Compliance teams and regulators quickly adopted the practice.

  Source: Bugcrowd 2020 Ultimate Guide to PenTesting Report

WHY PENETRATION TESTING?

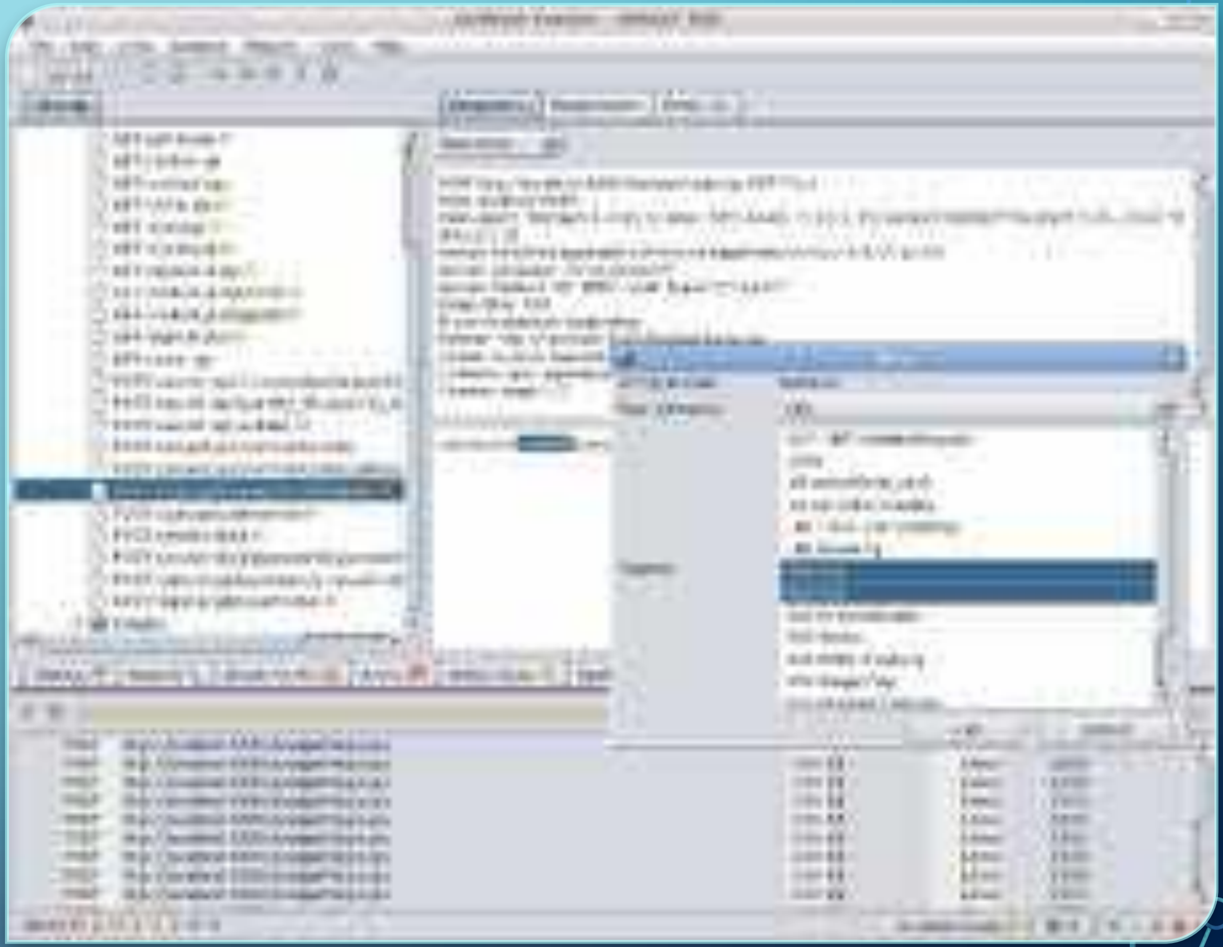
- Protect the organization and its assets
- Protect customer data
- Reduce cyber risk
- Satisfy stakeholder requirements
- Preserve the organization’s image and reputation

BURP SUITE

- This is a standard tool for web application penetration testers
- Both a vulnerability scanner and a penetration testing tool
- Can perform SQL Injection and Cross-site Scripting (XSS) attacks
- Community Edition (free) available; professional license is $449/year
- https://portswigger.net/burp

OWASP ZED ATTACK PROXY (ZAP)

- Open-source alternative to Burp Suite
- Both a vulnerability scanner and a penetration testing tool
- Can perform SQL Injection and Cross-site Scripting (XSS) attacks
- Created by the Open Web Application Security Project (OWASP)
- https://zaproxy.org



METASPLOIT FRAMEWORK

- Open-source tool for developing and executing exploit code against a remote target machine or network.
- Preinstalled on Kali Linux
- Created in 2003 by H.D. Moore as a portable network tool using Perl.
- By 2007 it was completely rewritten in Ruby.
- October 2009 – acquired by Boston based security company Rapid7

```
       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 pos
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: Open an interactive Ruby terminal
irb

msf6 >
```

OPPORTUNITIES TO LEARN MORE

- **TryHackMe** – tryhackme.com
- **PentesterLab** – pentesterlab.com
- **OWASP Juice Shop** – owasp.org/www-project-juice-shop/
- **Darn Vulnerable Web Application** – github.com/digininja/DVWA
- **Black Hills Information Security** – blackhillsinfosec.com

QUESTIONS?

THANK YOU FOR THE OPPORTUNITY TO SPEAK WITH YOU TODAY!