EVOLVE
Security

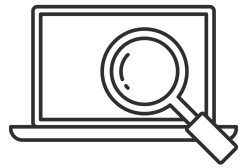
The Resourceful Pentester: Resources, Tools, and Targets for Pentesters

About Us

Evolve Security

APPLICATION
SECURITY

SECURITY
ACADEMY



CONTINUOUS
PENETRATION
TESTING

About Me

Jim Holcomb

- Pentester
- Developer (Python, JavaScript, PHP)
- SysAdmin (Linux, BSD)

Agenda

Presentation

- Finding guidance
- Tools Available
- PTES
- Hacking Equifax

Workshop

- Hacking Cyberstorm Workshop

Finding Guidance

Where do I Start?

Finding Guidance

Getting Started

- Infosec
  - https://www.reddit.com/r/netsecstudents/wiki/index#wiki_where_to_start
  - https://www.reddit.com/r/netsec/wiki/start
  - https://github.com/Hack-with-Github/Awesome-Hacking
  - https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet
- Programming
  - https://wiki.python.org/moin/BeginnersGuide
  - https://learnpythonthehardway.org/
- Twitter
  - @hacks4pancakes, @briankrebs, @georgiaweidman, @SwiftOnSecurity, @TroyHunt, @thegrugq

Finding Guidance

Getting Started: Part 2

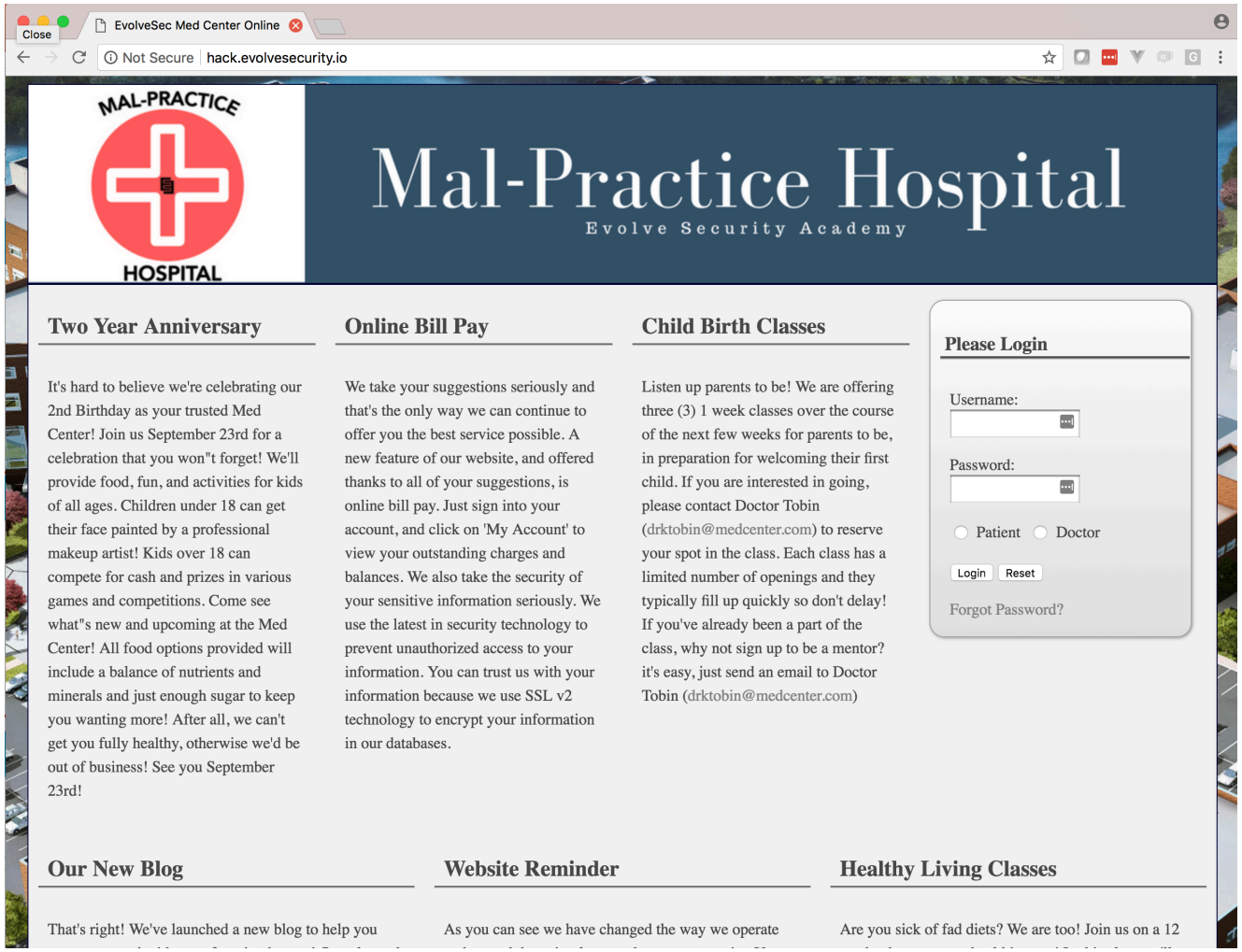
- Networking
  - http://www.tcpipguide.com/free/index.htm
- Linux
  - https://linuxacademy.com/ (Freemium)
  - http://www.funtoo.org/Linux_Fundamentals,_Part_1
  - https://wiki.archlinux.org/
- Windows
  - https://github.com/PowerShell/PowerShell/tree/master/docs/learning-powershell
  - https://github.com/PaulSec/awesome-windows-domain-hardening

Finding a Target

Finding a Target

Hack.evolvesecurity.io

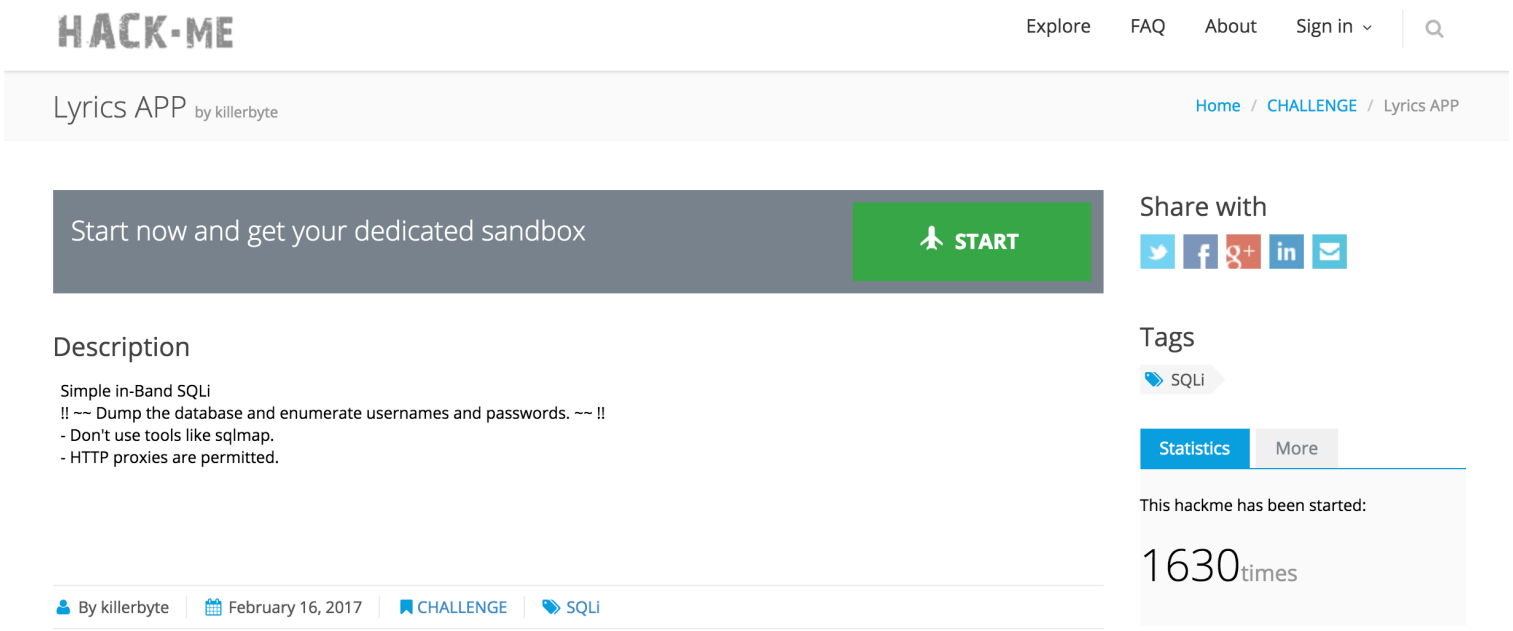
Hack.evolvesecurity.io is a vulnerable server managed by Evolve Security that allows aspiring pentesters to practice attacking web applications.



Finding a Target

Hack.me

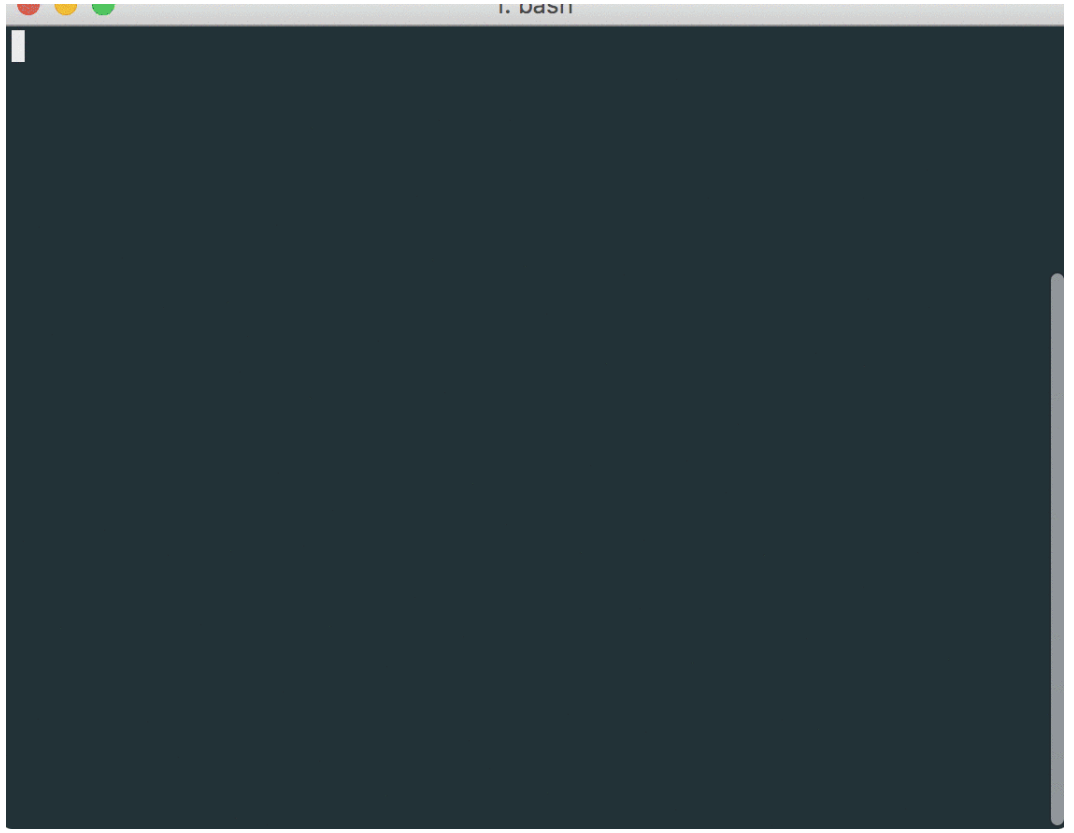
Hack.me allows users to spin up community built vulnerable web applications in a sandboxed environment with no installation required.



Finding a Target

OverTheWire.com

OverTheWire.com provides users with a WarGame like environment in which they can master security concepts.

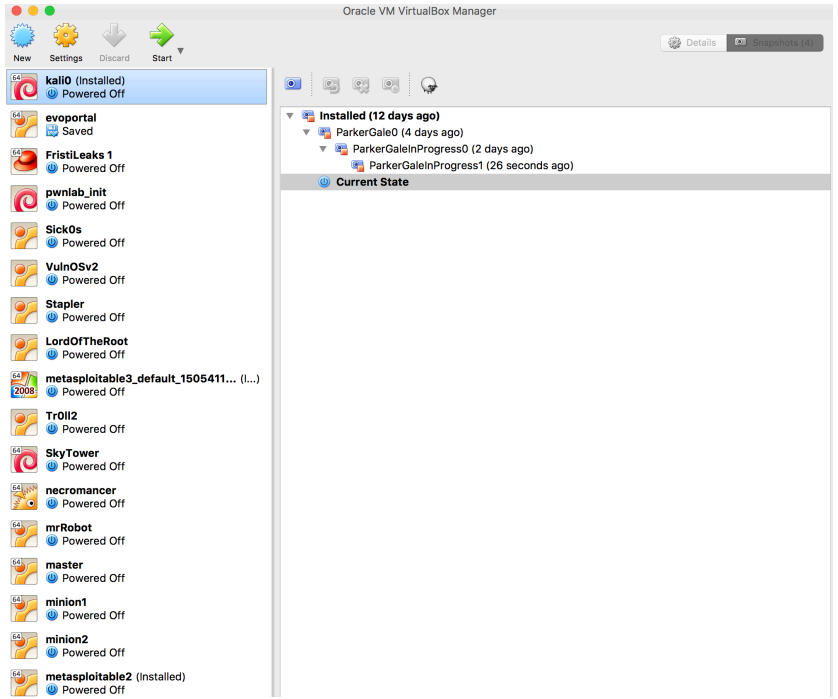


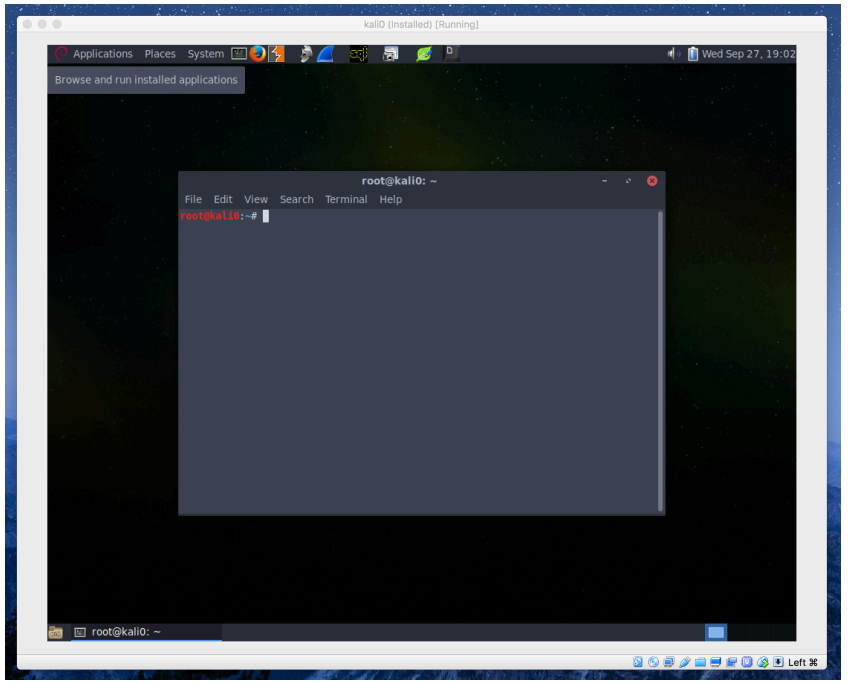
Building a Lab

Building a Lab

Virtualbox

Virtualbox is an AMD64/Intel64 virtualization engine that allows users to run virtual machines.

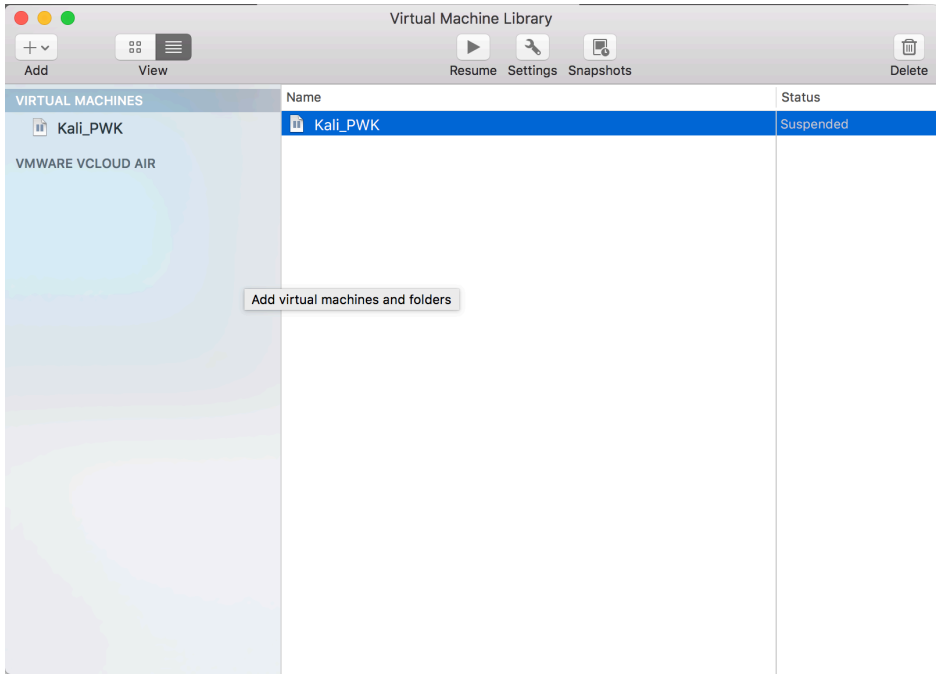




Building a Lab

Vmware

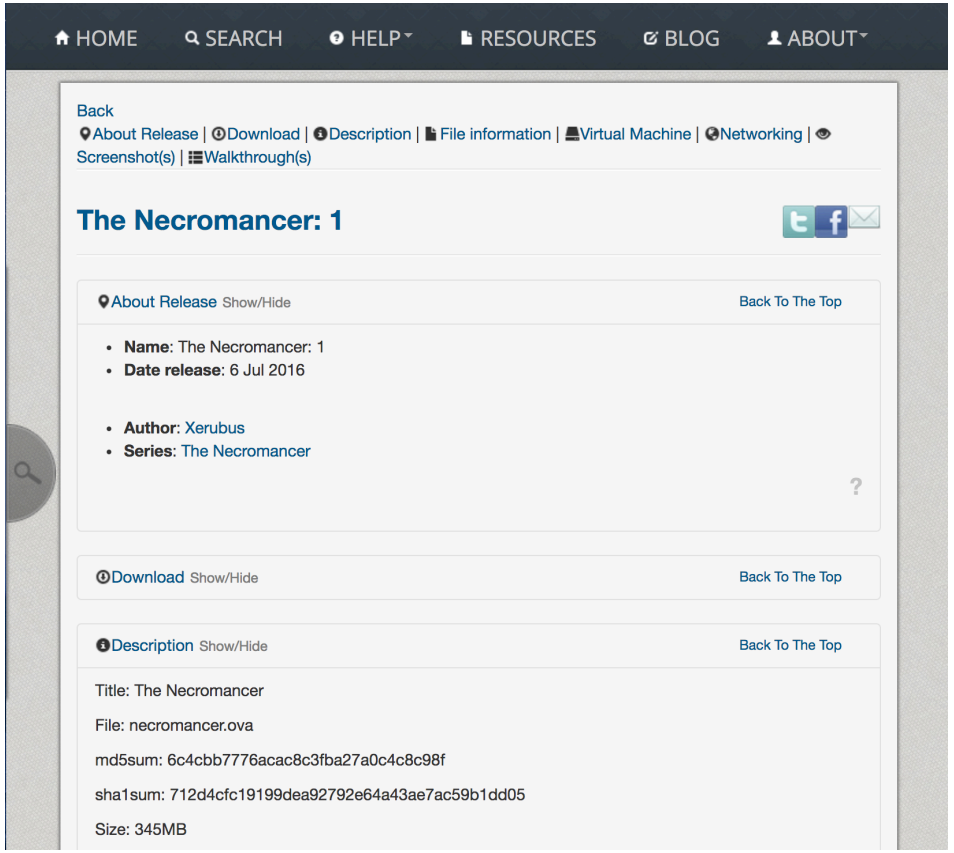
Vmware offers a wide array of virtualization environments such as Vmware Fusion (Mac) and Vmware Workstation (Windows) which operate in a similar manner to VirtualBox.



Building a Lab

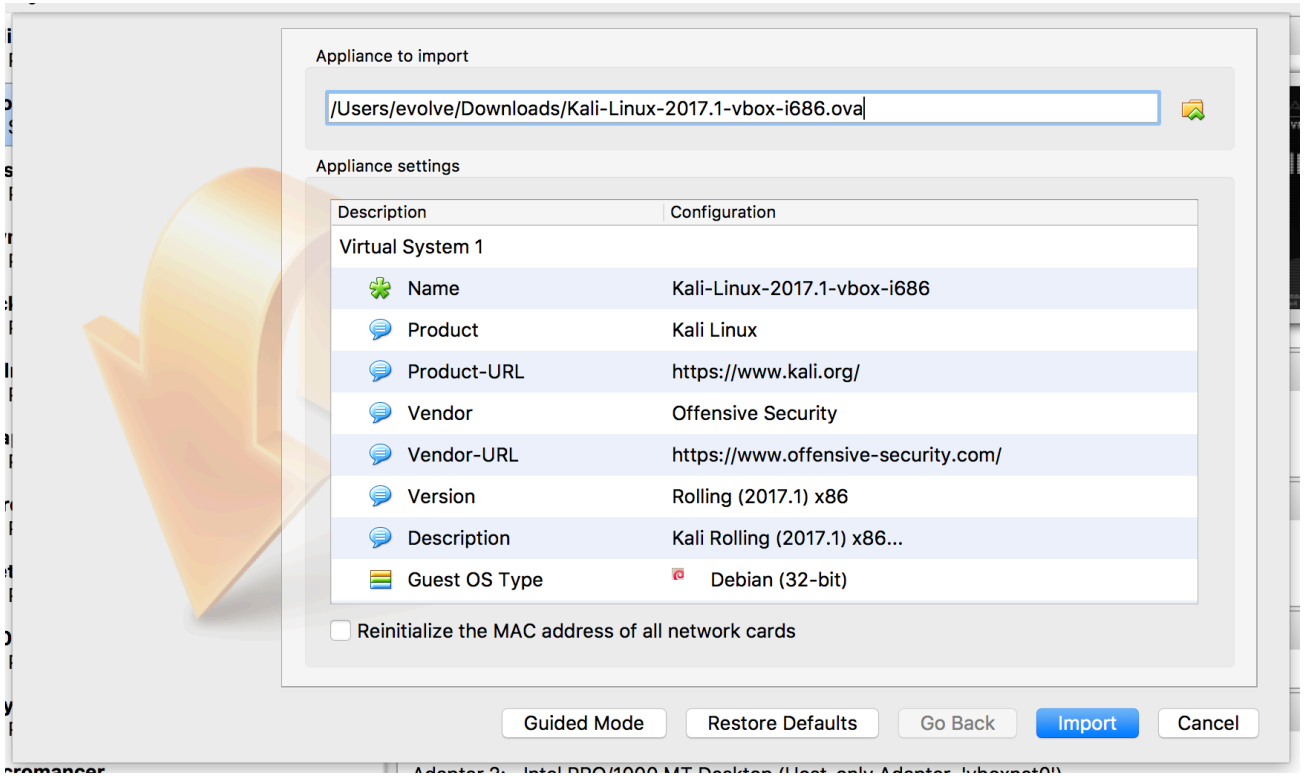
Finding Vulnerable Machines

Vulnhub.com offers a wide a array of community created vulnerable machines. They are stored in different formats. Some are compatible with only Virtualbox or Vmware but many (.ova, .vmdk, .iso) can be added to both.



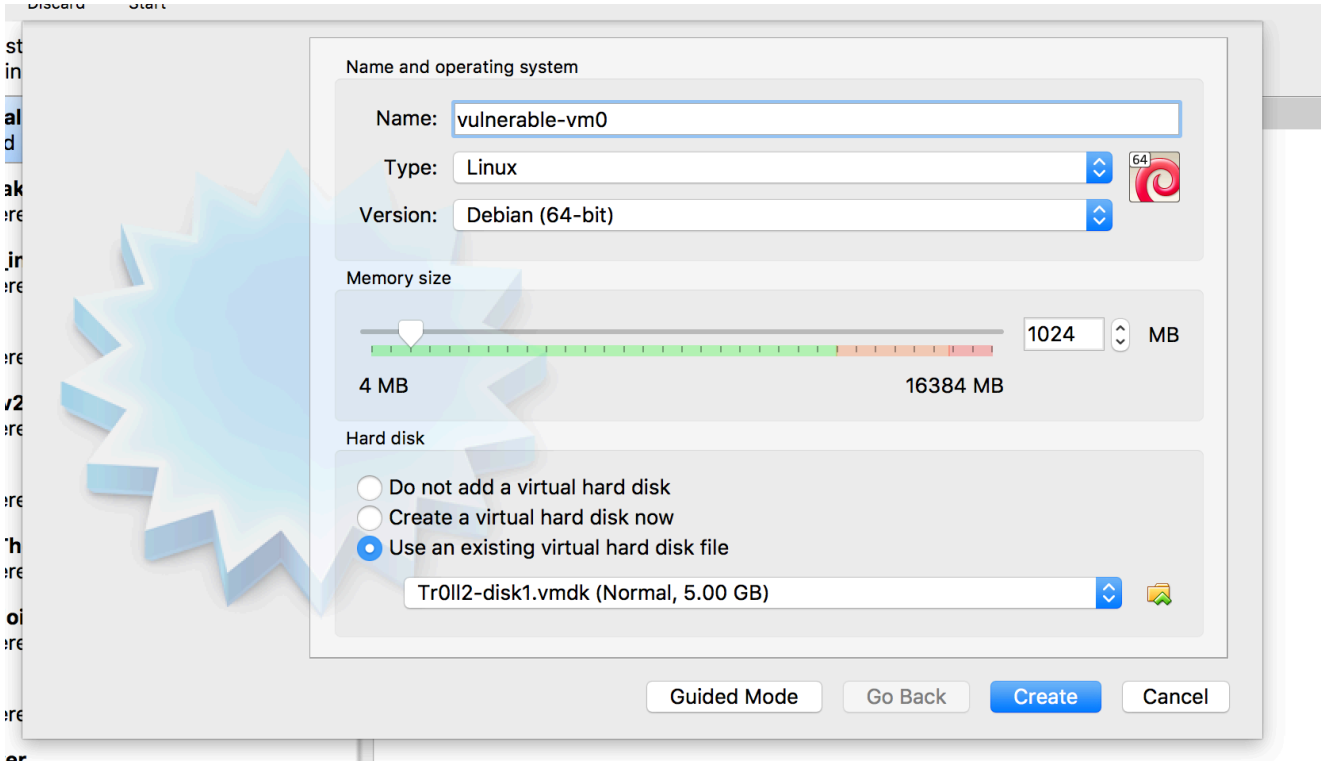
Installing Vulnerable Machines

Importing an OVA



Building a Lab: Installing Vulnerable Machines

Attaching a VMDK



Finding a Target

Exploit Exercises

- https://exploit-exercises.com/

Metasploitable2

- https://www.vulnhub.com/entry/metasploitable-2,29/

Metasploitable3

- https://github.com/rapid7/metasploitable3

Capture The Flags

- https://ctf365.com

The Pentester’s Strategy Guide

Penetration Testing Execution Standard

What Is It?

- **Pre-engagement Interactions:** Meeting, Scoping, Communication
- **Intelligence Gathering**: OSINT, Compliance, Active/Passive
- **Threat Modeling:** Assets vs Attacker, Prioritization
- **Vulnerability Analysis:** Scanning, Banner Grabbing, Version Detection
- **Exploitation:** Establish Access, Precise Action, Evasion, Buffer Overflows, Social Engineering, Evil Twin
- **Post Exploitation:** Establish Control and Persistence, Privileged Analysis
- **Reporting:** Executive Summary and Technical Report

PTES vs Hacking Methodology

PTES

- Pre-engagement Interactions
- Intelligence Gathering
  - Passive
  - Active
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

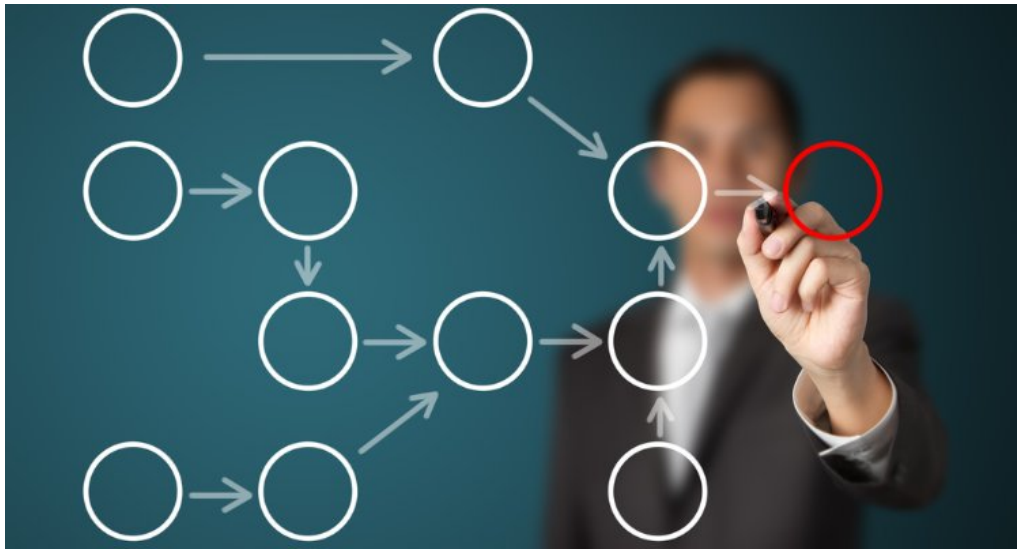
“Hacking Methodology”

- Reconnaissance
  - Active
  - Passive
- Enumeration
- Exploitation
- Persistence
- Escalation
- Exfiltration
- Anti-forensics/Evasion

Pre Engagement Interactions

PTES: Pre Engagement Interactions

How do I do it?



- Meet with Clients/Owners
- Define Points of Contact
- Establish Scope (Red Team, White/Black Box)
- Determine Goals of Test
- Ask Questions:
  - Can we test during business hours?
  - Will source code be made available?
  - How large are the applications/networks beings assessed (Web Pages, IPs etc)

Intelligence Gathering

PTES: Intelligence Gathering (Passive)

How do I do it?

- Open Source Intelligence (OSINT)
- Visit Company Website
  - Gather DNS Records
- Visit Company's Physical Location
- Company Organization Chart Review
- Social Media(Linkedin, Github etc)
  - Email Addresses
- Search for Legal Documents
- Research Current Open Positions
  - What skills are required?

PTES: Intelligence Gathering (OSINT)

Awesome OSINT: https://github.com/jivoi/awesome-osint

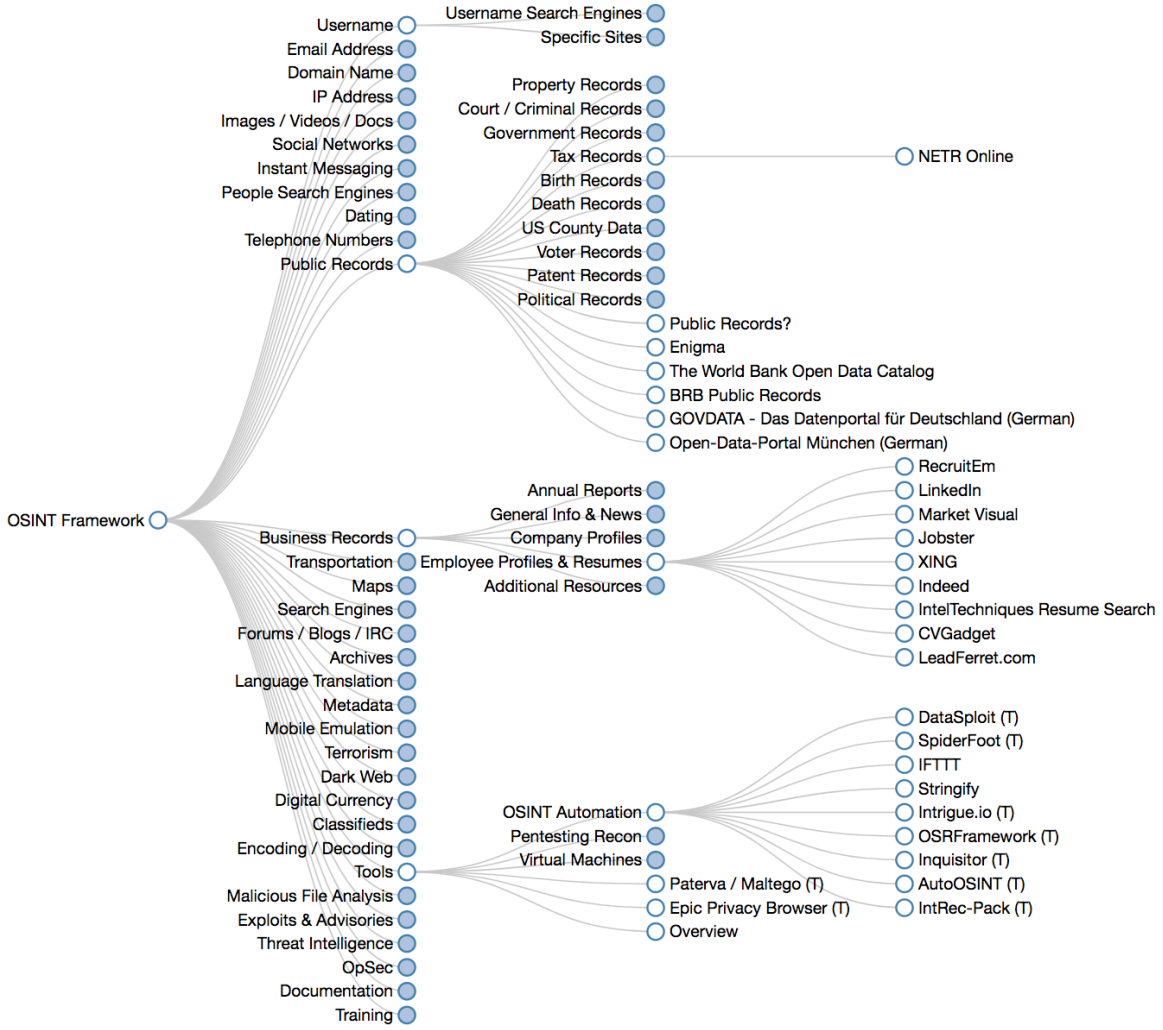
Awesome OSINT 

A curated list of amazingly awesome open source intelligence tools and resources. Open-source intelligence (OSINT) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources)

Contents

PTES: Intelligence Gathering (OSINT)

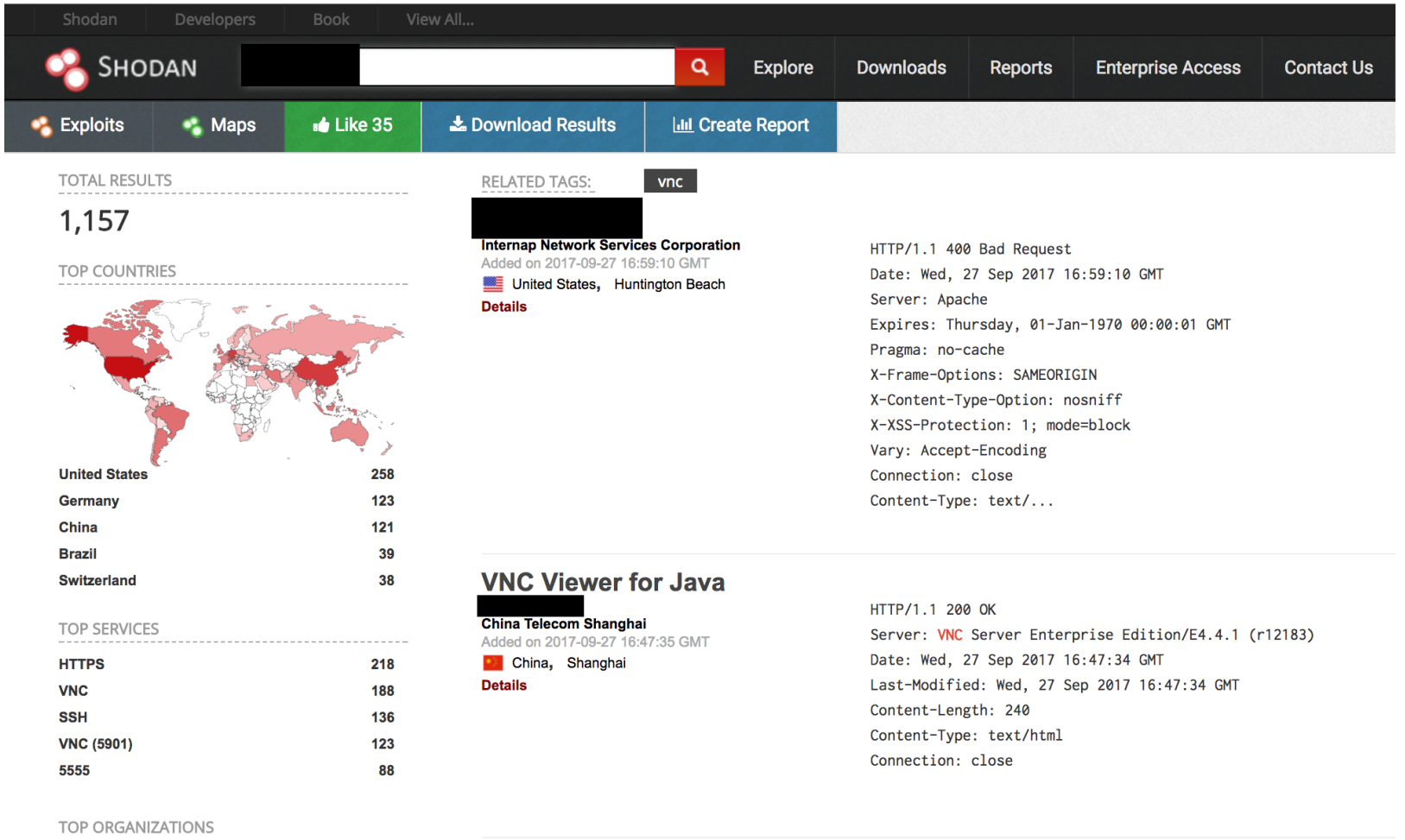
OSINT Framework:
http://osintframework.com/



PTES: Intelligence Gathering (OSINT)

Shodan:

http://shodan.io/



PTES: Intelligence Gathering (OSINT)

Maltego:

- https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

Recon-ng:

- https://bitbucket.org/LaNMaSteR53/recon-ng/wiki/Usage%20Guide

Harvestor

- https://github.com/laramies/theHarvester

Discover Scripts

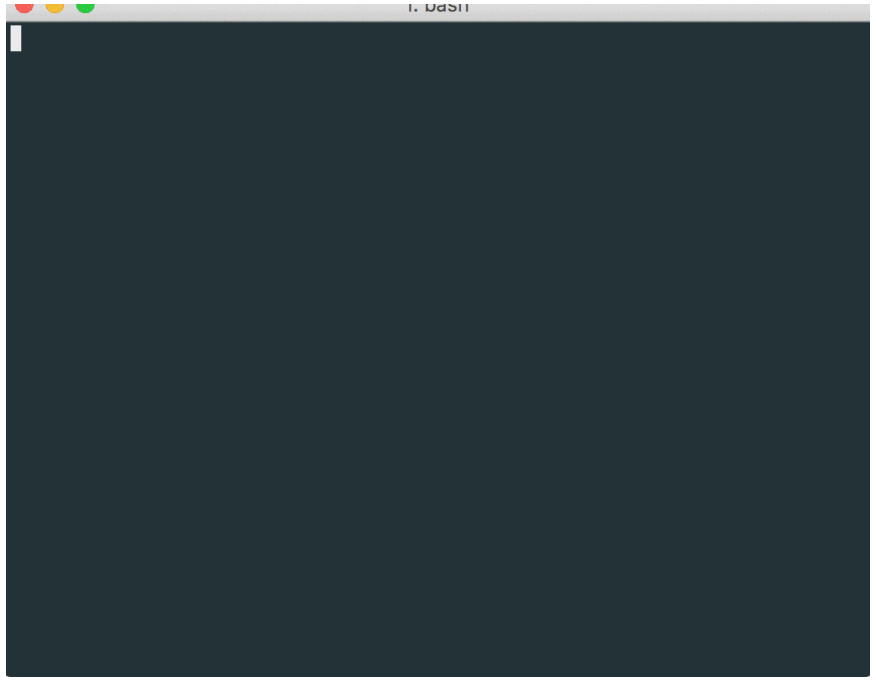
- https://github.com/leebaird/discover

PTES: Intelligence Gathering (Active)

How do I do it?

- Internet Footprint
  - Systems (Linux, Windows)?
  - Services/Versions (ssh, http, vnc, file share)?
- Internal Network
  - Wifi
    - Router Brand, Type, Version
    - WEP, WPA Personal/Enterprise
- Physical
    - Guards
    - Cameras

PTES: Intelligence Gathering (Active)



Nmap (Network/System Scanner):

- https://nmap.org/

Netcat/Ncat (TCP/UDP)

- https://github.com/nmap/nmap/tree/master/ncat

Airmon-ng (Wifi Monitoring)

- https://github.com/aircrack-ng/aircrack-ng

Kismet (Network Detector / Sniffer)

- https://github.com/kismetwireless/kismet

Enum4linux (Samba Enumeration)

- https://tools.kali.org/information-gathering/enum4linux

OneSixtyOne (SNMP)

- https://github.com/trailofbits/onesixtyone

Finding Guidance

Threat Modeling

PTES: Threat Modeling

Creating a Model

- Requirements
  - Representation (Internal/External)
  - Capabilities
  - Qualifications (as related to business/target)
  - Repeatability/Consistency
- Asset Analysis
- Threat Capabilities
- Motivation Modeling

PTES: Threat Modeling

OWASP

- https://www.owasp.org/index.php/Threat_Risk_Modeling

STRIDE

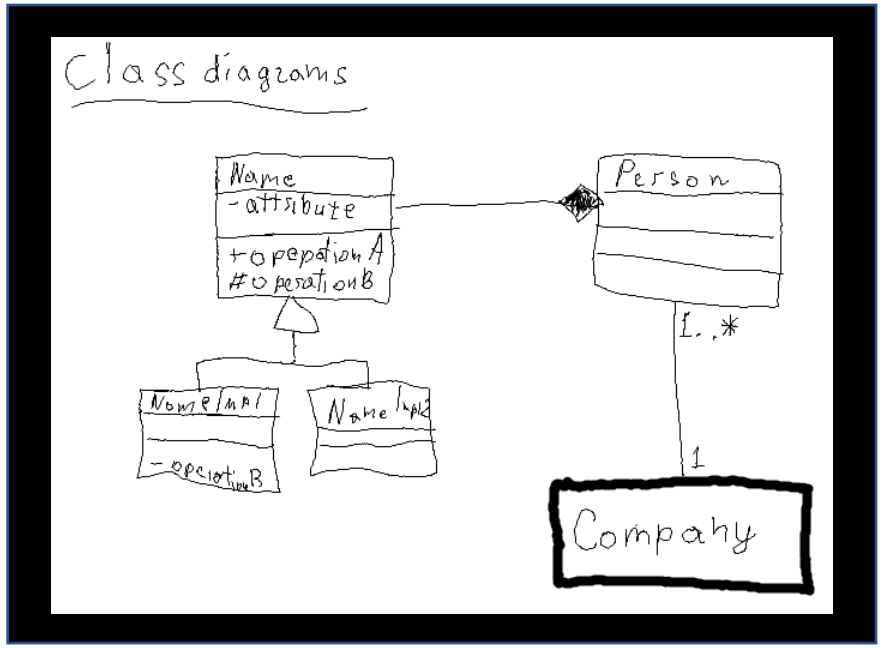
- https://en.wikipedia.org/wiki/STRIDE_(security)

Staruml (UML, Freemium)

- http://staruml.io/download

Lucid Chart (UML)

- https://www.lucidchart.com/

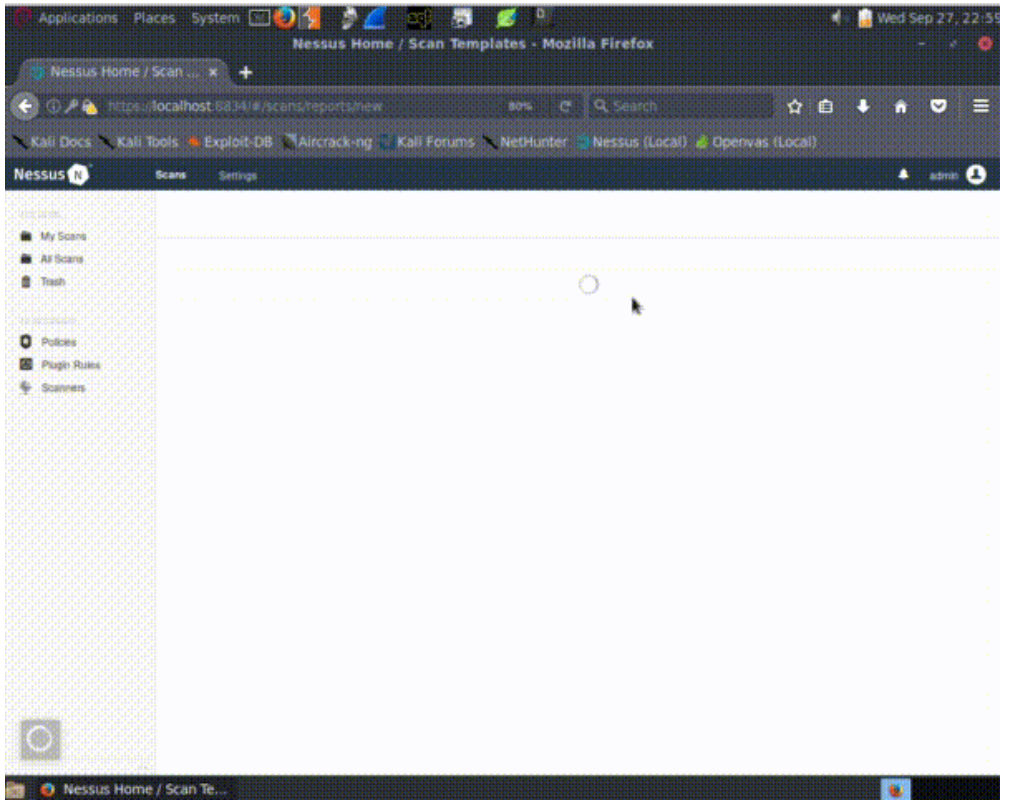


Vulnerability Analysis

PTES: Vulnerability Analysis

How do I do it?

- Discovering flaws
  - System Configuration
  - Vulnerable Application Design
    - Cross Account Access
- Manual Analysis
  - Custom Packets
  - QA Application
  - Exploit Research
- Automated Scanning



PTES: Vulnerability Analysis (Automated)

Nessus (closed-source)

- https://www.tenable.com/products/nessus-vulnerability-scanner

Nmap (Scripts):

- https://nmap.org/

Nexpose (closed-source)

- https://www.rapid7.com/products/nexpose/

Burp Suite Scanner (closed-source)

- https://portswigger.net/burp

DotDotPwn (Directory Fuzzing)

- https://tools.kali.org/information-gathering/dotdotpwn

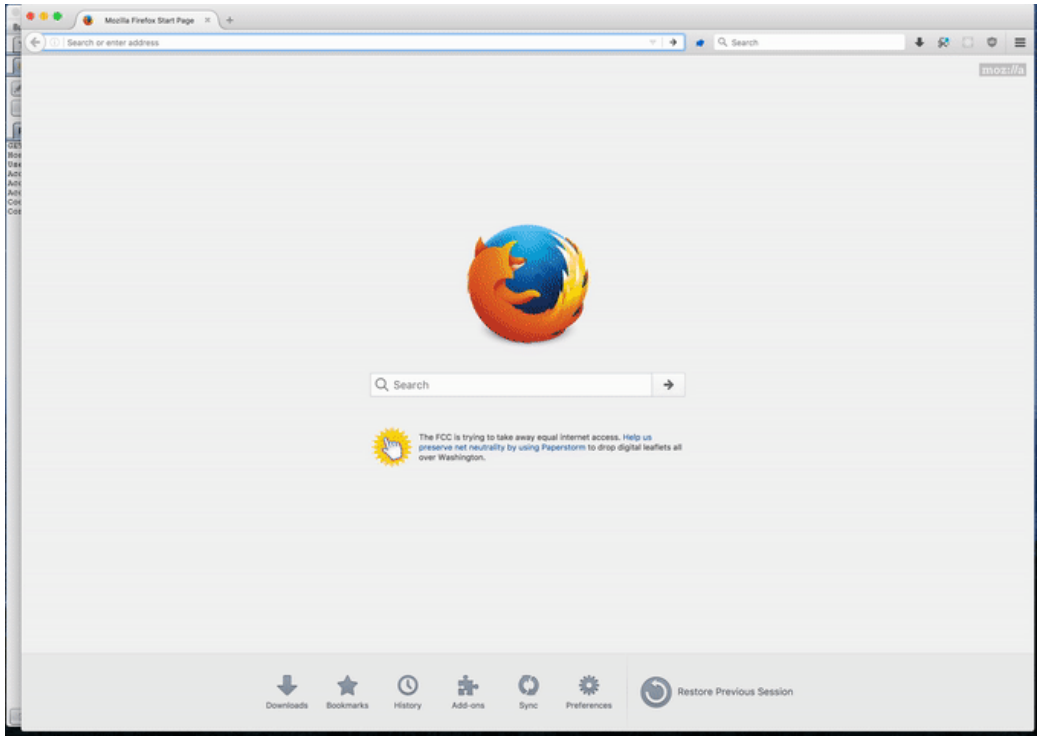
Metasploit Framework (Scanners)

- https://www.offensive-security.com/metasploit-unleashed/

WPScan

- https://tools.kali.org/web-applications/wpscan

PTES: Vulnerability Analysis (Manual)



Burp Suite Proxy

- https://portswigger.net/burp

MITM Proxy

- https://mitmproxy.org

Dirb/Dirbuster (Directory Fuzzing)

- https://tools.kali.org/web-applications/dirb
- https://tools.kali.org/web-applications/dirbuster

DotDotPwn (Directory Fuzzing)

- https://tools.kali.org/information-gathering/dotdotpwn

SearchSploit (ExploitDb)

- https://github.com/offensive-security/exploit-database

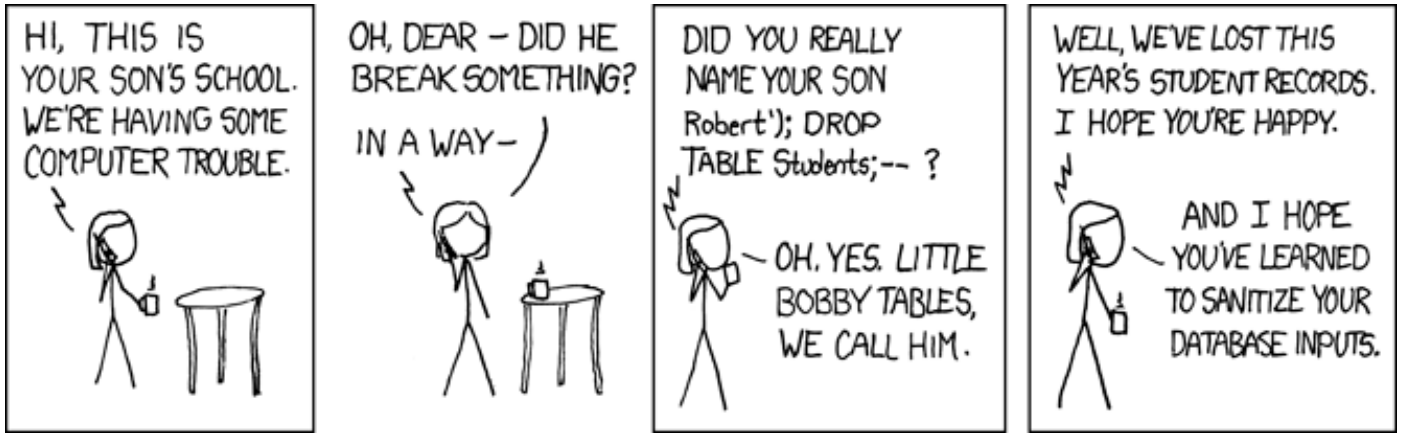
Finding Guidance

Exploitation

PTES: Exploitation

How do I do it?

- Precision Strike
  - Buffer Overflows
  - XSS
  - Database (SQL)
  - Framework Vulnerabilities (Wordpress)
- Bypass
  - AV
  - Firewall
- Brute Force
  - Services (ssh, ftp, web authentication)
- VLAN Hopping



PTES: Exploitation

SearchSploit (ExploitDb)

- https://github.com/offensive-security/exploit-database

Metasploit Framework (Exploits)

- https://www.offensive-security.com/metasploit-unleashed/

Python

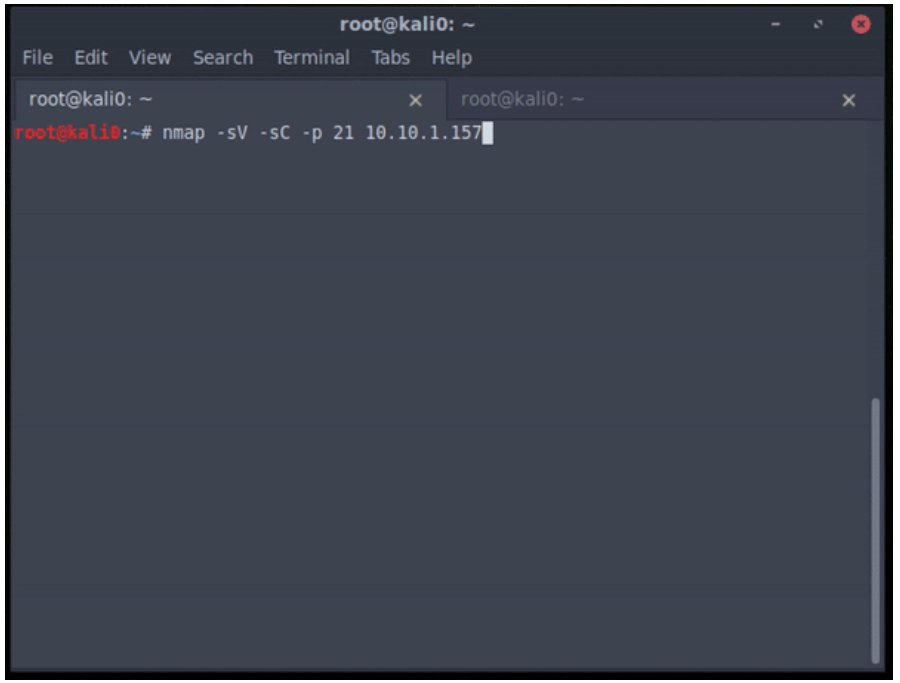
- https://www.nostarch.com/blackhatpython

THC-Hydra/XHydra

- https://github.com/vanhauser-thc/thc-hydra

Airodump-ng (Wifi)

- https://github.com/aircrack-ng/aircrack-ng



Finding Guidance

Post-Exploitation

PTES: Post-Exploitation

How do I do it?

- Privilege Escalation
  - Buffer Overflows
  - Misconfigured Services
- Establish Persistence (Backdoor)
  - Reverse Shell
  - Extracted Credentials
- Data Exfiltration
  - Looting/Pillaging
  - Keylogger
- Data Destruction
- Evasion

PTES: Post-Exploitation

SearchSploit (ExploitDb)

- https://github.com/offensive-security/exploit-database

Metasploit Framework (Post Exploitation)

- https://www.offensive-security.com/metasploit-unleashed/

Reverse Shells

- https://highon.coffee/blog/reverse-shell-cheat-sheet/

Fgdump/Pwdump6

- http://foofus.net/goons/fizzgig/fgdump/default.htm

Shell Commands

- https://github.com/PowerShell/PowerShell/tree/master/docs/learning-powershell
- https://www.shellscript.sh/

Penetration Testing Execution Standard

http://www.pentest-standard.org/index.php/Main_Page

Putting it all together: Hacking Apache Struts v2.5.9

The Scenario

This presentation originally included a demonstration of exploiting CVE-2017-5638. The vulnerable machine used to perform this exploit can be found at: https://github.com/evolvesecurity/vuln-struts2-vm

Focus of this Workshop

PTES

- Pre-engagement Interactions
- **Intelligence Gathering**
  - Passive
  - **Active**
- Threat Modeling
- **Vulnerability Analysis**
- **Exploitation (Bonus)**
- **Post Exploitation (Bonus)**
- Reporting

“Hacking Methodology”

- Reconnaissance
  - Active
  - Passive
- **Enumeration**
- **Exploitation**
- Persistence
- Escalation
- Exfiltration
- Anti-forensics

Let’s hack Cyberstorm!

The Scenario

Company Cyberstorm LLC has contracted Sobol Security to perform an Internal Penetration Test. As Cyberstorm is a secretive startup focused in Artificial Intelligence, there is no public information on them, and they have no human employees.

Sobol Security has met with their contact at Cyberstorm and agreed that Sobol will test three boxes on their internal network. Everything within the three IPs of those servers is in scope; however, an additional box on the same network that is out of scope as this box holds the AI's backups.

The Scenario

This presentation originally included a workshop. The guide for the workshop can be downloaded from the EvolveSec Github Page at https://github.com/evolvesecurity/EvolveSec

Nmap Cheatsheet

Normal SYN (or TCP) Scan

$ nmap IP

Ping Scan

$ nmap –sP IP

Syn Scan

nmap –sS IP

TCP Scan

$ nmap –sT IP

UDP Scan

$ nmap –sU IP

Explicit Ports (all)

$ nmap –p 1-65535 IP

Services Scan

$ nmap -sV IP

Fingerprint OS

$ nmap –O IP

Default Scripts (safe)

nmap –sC IP

Save Output

$ nmap –oN scan.nmap IP

Netcat Cheatsheet

Normal TCP Connection

```
$ nc  10.0.0.3 22
```

Normal UDP Connection

```
$ nc  –u 10.0.0.3 53
```

Do not Resolve DNS

```
$ nc –n 10.0.0.3 22
```

Normal TCP Listener

```
$ nc –l -p 4444
```

Verbose

```
$ nmap –v –l -p 4444
```

THANK YOU!

Contact: Jim Holcomb
Email: Jim@EvolveSecurity.io
Twitter: @3lpsy

Evolvesecurity.io
Evolveacademy.io