



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



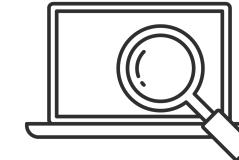
Evolve Security



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 Guidance

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.

The screenshot shows a web browser window with the title "EvolveSec Med Center Online". The address bar says "Not Secure" and "hack.evolvesecurity.io". The page itself is titled "Mal-Practice Hospital" and "Evolve Security Academy". It features a large red cross logo with "MAL-PRACTICE" at the top and "HOSPITAL" at the bottom. Below the logo, there are three main sections: "Two Year Anniversary", "Online Bill Pay", and "Child Birth Classes". Each section has a brief description and a "Read More" link. To the right, there is a "Please Login" form with fields for "Username" and "Password", and radio buttons for "Patient" and "Doctor". Buttons for "Login" and "Reset" are also present. At the bottom, there are links for "Our New Blog", "Website Reminder", and "Healthy Living Classes".

MAL-PRACTICE HOSPITAL

Two Year Anniversary

It's hard to believe we're celebrating our 2nd Birthday as your trusted Med Center! Join us September 23rd for a celebration that you won't forget! We'll provide food, fun, and activities for kids of all ages. Children under 18 can get their face painted by a professional makeup artist! Kids over 18 can compete for cash and prizes in various games and competitions. Come see what's new and upcoming at the Med Center! All food options provided will include a balance of nutrients and minerals and just enough sugar to keep you wanting more! After all, we can't get you fully healthy, otherwise we'd be out of business! See you September 23rd!

Online Bill Pay

We take your suggestions seriously and that's the only way we can continue to offer you the best service possible. A new feature of our website, and offered thanks to all of your suggestions, is online bill pay. Just sign into your account, and click on 'My Account' to view your outstanding charges and balances. We also take the security of your sensitive information seriously. We use the latest in security technology to prevent unauthorized access to your information. You can trust us with your information because we use SSL v2 technology to encrypt your information in our databases.

Child Birth Classes

Listen up parents to be! We are offering three (3) 1 week classes over the course of the next few weeks for parents to be, in preparation for welcoming their first child. If you are interested in going, please contact Doctor Tobin (drktobin@medcenter.com) to reserve your spot in the class. Each class has a limited number of openings and they typically fill up quickly so don't delay! If you've already been a part of the class, why not sign up to be a mentor? It's easy, just send an email to Doctor Tobin (drktobin@medcenter.com)

Please Login

Username:

Password:

Patient Doctor

Our New Blog

That's right! We've launched a new blog to help you

Website Reminder

As you can see we have changed the way we operate

Healthy Living Classes

Are you sick of fad diets? We are too! Join us on a 12



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.

The screenshot shows the Hack.me website interface. At the top, there's a navigation bar with 'Explore', 'FAQ', 'About', 'Sign in', and a search icon. Below the navigation is a banner for the 'Lyrics APP' challenge, created by 'killerbyte'. The banner features a large green 'START' button with a rocket icon. To the left of the button, the text reads 'Start now and get your dedicated sandbox'. To the right, there's a 'Share with' section with social media icons for Twitter, Facebook, Google+, LinkedIn, and Email. Below the banner, the challenge details are listed under 'Description': 'Simple in-Band SQLi', '!! ~~ Dump the database and enumerate usernames and passwords. ~~ !!', '- Don't use tools like sqlmap.', and '- HTTP proxies are permitted.' To the right, under 'Tags', is a 'SQLi' tag with a blue arrow icon. At the bottom, there are 'Statistics' and 'More' buttons, and a message stating 'This hackme has been started: 1630 times'. At the very bottom of the page, there's a footer with links: 'By killerbyte', 'February 16, 2017', 'CHALLENGE', and 'SQLi'.



Finding a Target

OverTheWire.com

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





Finding Guidance

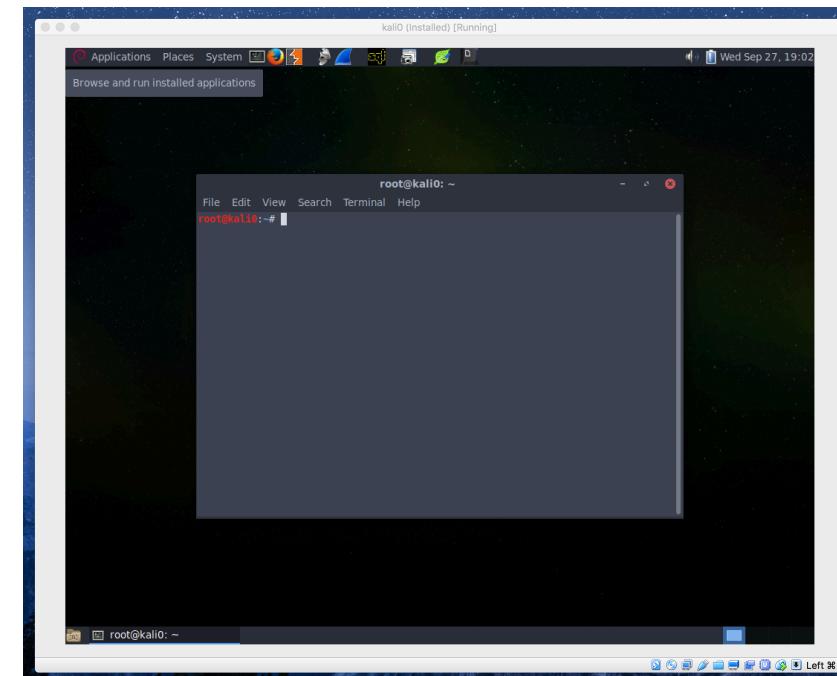
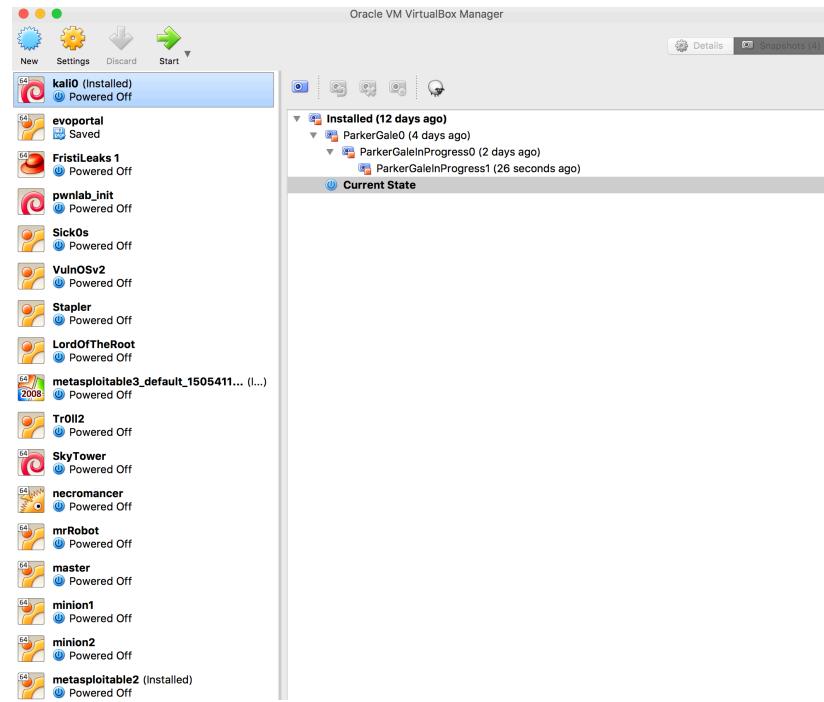
Building a Lab



Building a Lab

Virtualbox

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

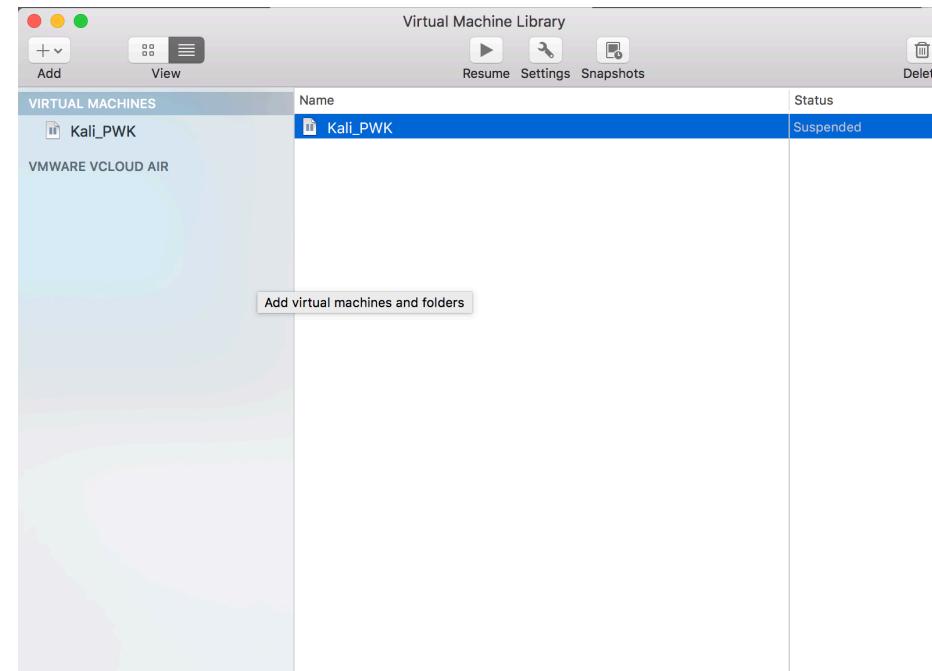




Building a Lab

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 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.

The screenshot shows a web page from Vulnhub.com. At the top, there's a navigation bar with links for HOME, SEARCH, HELP, RESOURCES, BLOG, and ABOUT. Below the navigation, the page title is "The Necromancer: 1". There are social sharing icons for Twitter, Facebook, and Email. The main content area has sections for "About Release", "Download", "Description", and "File information". Under "About Release", it says "Name: The Necromancer: 1" and "Date release: 6 Jul 2016". It also lists the author as "Xeribus" and the series as "The Necromancer". Under "Download", there's a link to download the .ova file. The "Description" section includes the title "The Necromancer", file type ".ova", and provides MD5 and SHA1 checksums. The "File information" section shows the file size as 345MB.

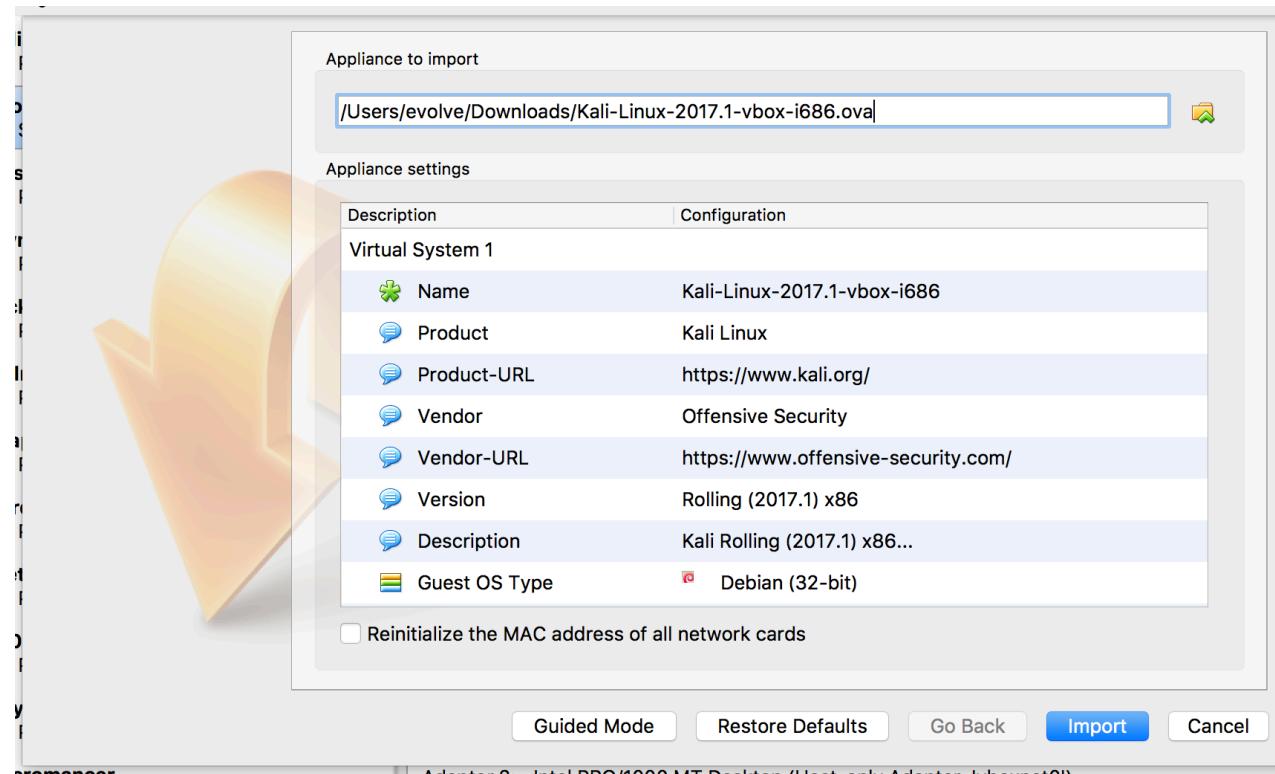
Section	Details
About Release	Name: The Necromancer: 1 Date release: 6 Jul 2016 Author: Xeribus Series: The Necromancer
Download	Download .ova file
Description	Title: The Necromancer File: necromancer.ova MD5sum: 6c4ccb7776acac8c3fba27a0c4c8c98f SHA1sum: 712d4cfbc19199dea92792e64a43ae7ac59b1dd05 Size: 345MB



Building a Lab

Installing Vulnerable Machines

Importing an OVA

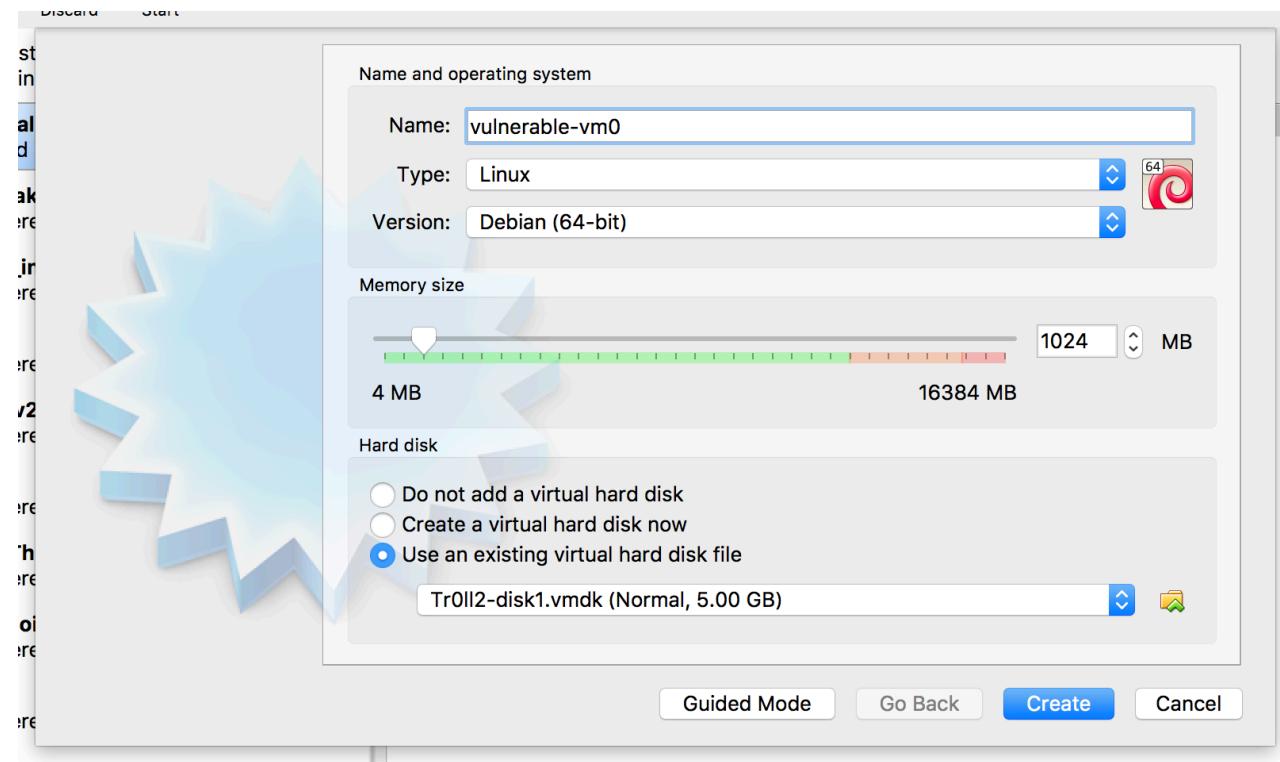




Building a Lab

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>



Finding Guidance

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



Finding Guidance

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)





Finding Guidance

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 awesome

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)



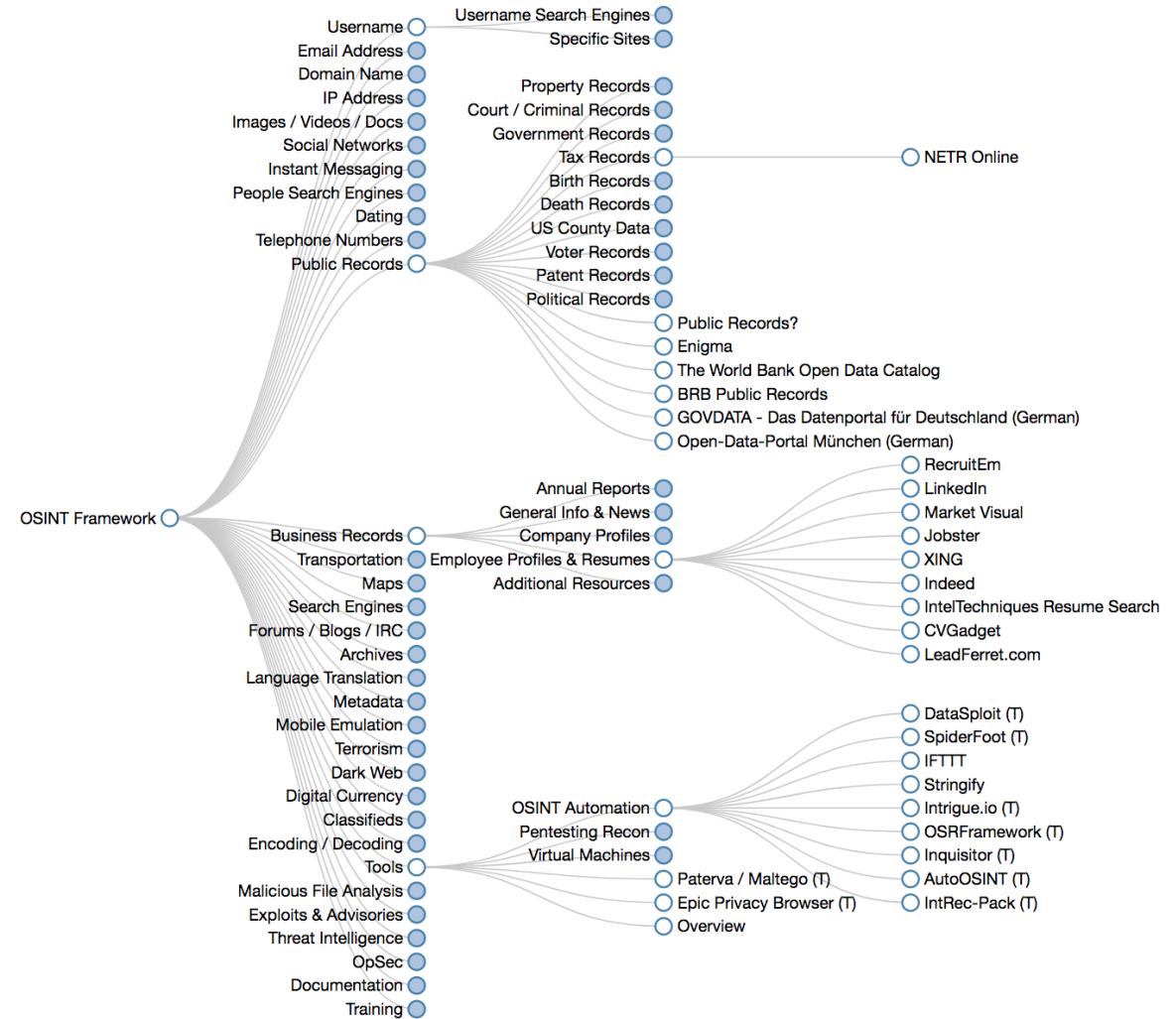
Contents

- [General Search](#)
- [Main National Search Engines](#)
- [Meta Search](#)
- [Specialty Search Engines](#)
- [Visual Search and Clustering Search Engines](#)
- [Similar Sites Search](#)
- [Document and Slides Search](#)
- [Pastebins](#)
- [Code Search](#)
- [Major Social Networks](#)
- [Real-Time Search, Social Media Search, and General Social Media Tools](#)
- [Social Media Tools](#)
 - [Twitter](#)



PTES: Intelligence Gathering (OSINT)

OSINT Framework:
<http://osintframework.com/>





PTES: Intelligence Gathering (OSINT)

Shodan:

<http://shodan.io/>

Shodan Developers Book View All...

SHODAN

Exploits Maps Like 35 Download Results Create Report

TOTAL RESULTS 1,157

TOP COUNTRIES

COUNTRY	RESULTS
United States	258
Germany	123
China	121
Brazil	39
Switzerland	38

TOP SERVICES

SERVICE	RESULTS
HTTPS	218
VNC	188
SSH	136
VNC (5901)	123
5555	88

TOP ORGANIZATIONS

RELATED TAGS: vnc

Internap Network Services Corporation
Added on 2017-09-27 16:59:10 GMT
United States, Huntington Beach
[Details](#)

HTTP/1.1 400 Bad Request
Date: Wed, 27 Sep 2017 16:59:10 GMT
Server: Apache
Expires: Thursday, 01-Jan-1970 00:00:01 GMT
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
X-Content-Type-Option: nosniff
X-XSS-Protection: 1; mode=block
Vary: Accept-Encoding
Connection: close
Content-Type: text/...

VNC Viewer for Java
China Telecom Shanghai
Added on 2017-09-27 16:47:35 GMT
China, Shanghai
[Details](#)

HTTP/1.1 200 OK
Server: VNC Server Enterprise Edition/E4.4.1 (r12183)
Date: Wed, 27 Sep 2017 16:47:34 GMT
Last-Modified: Wed, 27 Sep 2017 16:47:34 GMT
Content-Length: 240
Content-Type: text/html
Connection: close



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>

Harvester

- <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

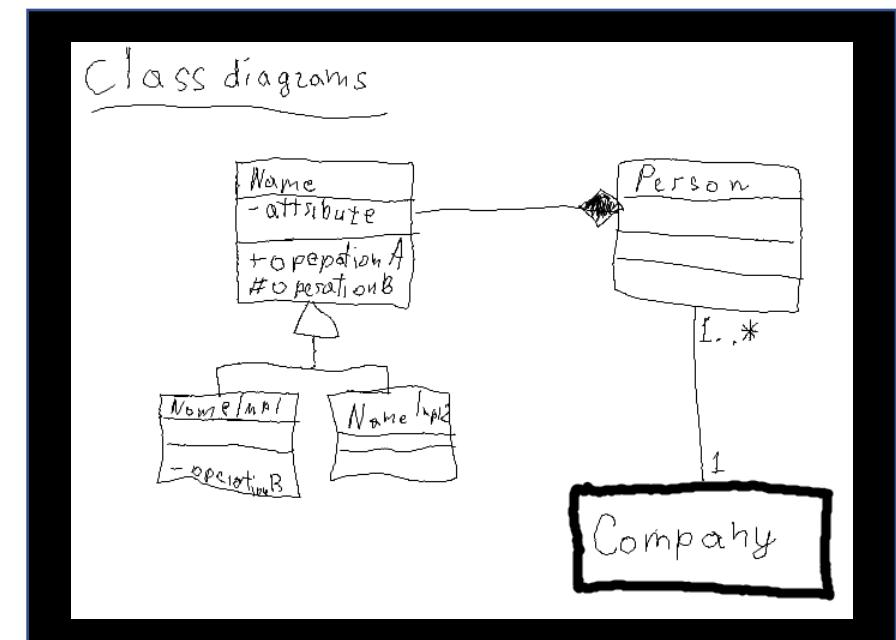
- [https://en.wikipedia.org/wiki/STRIDE_\(security\)](https://en.wikipedia.org/wiki/STRIDE_(security))

Staruml (UML, Freemium)

- <http://staruml.io/download>

Lucid Chart (UML)

- <https://www.lucidchart.com/>





Finding Guidance

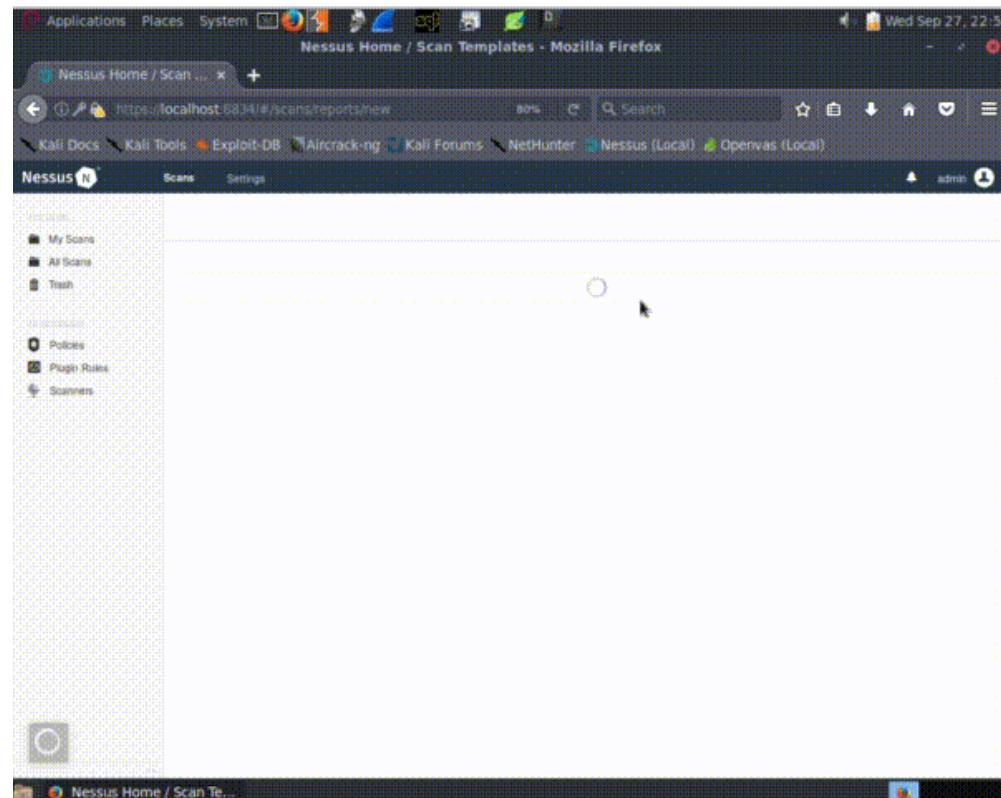
Vulnerability Analysis



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)

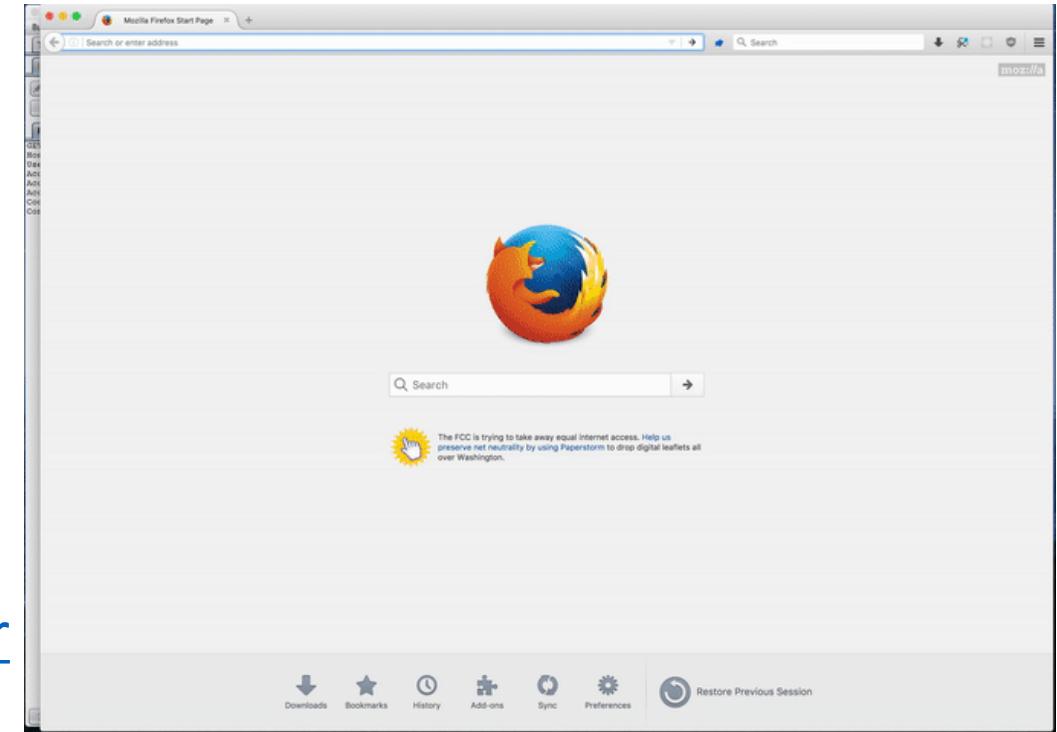
- <https://tools.kali.org/web-applications/dirb>
- <https://tools.kali.org/web-applications/dirbuster>

DotDotPwn (Directory Fuzzing)

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

SearchSploit (ExploitDb)

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





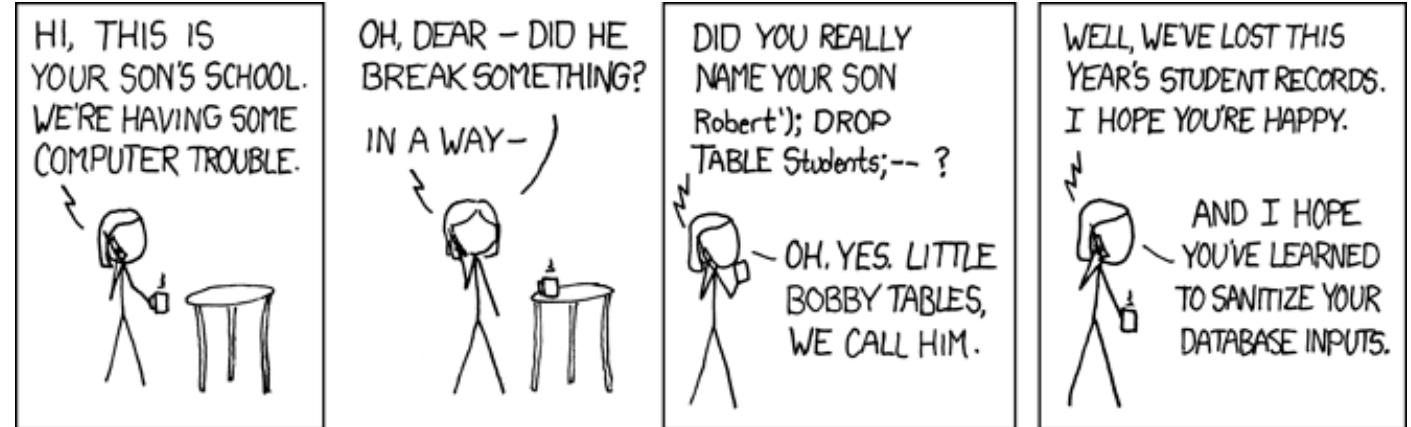
Finding Guidance

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>

The screenshot shows a terminal window titled "root@kali0: ~". The window has two tabs open. The active tab displays the command: `root@kali0:~# nmap -sV -sC -p 21 10.10.1.157`. The background tab shows the same terminal prompt. The terminal interface includes a menu bar with File, Edit, View, Search, Terminal, Tabs, and Help.



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.shells script.sh/>



Penetration Testing Execution Standard

THEY'RE MORE WHAT YOU'D CALL



GUIDELINES

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

Workshop



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
```

Explicit Ports (all)

```
$ nmap -p 1-65535 IP
```

Ping Scan

```
$ nmap -sP IP
```

Services Scan

```
$ nmap -sV IP
```

Syn Scan

```
nmap -sS IP
```

Fingerprint OS

```
$ nmap -O IP
```

TCP Scan

```
$ nmap -sT IP
```

Default Scripts (safe)

```
nmap -sC IP
```

UDP Scan

```
$ nmap -sU 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](https://twitter.com/@3lpsy)

Evolvesecurity.io

Evolveacademy.io