
esentire®
What to Expect From a Penetration Test
CodeMash 2016

Introductions

esentire

- Chris Maddalena, OSCP
  - @cmaddalena - IRC, GitHub, Twitter
  - Information Security Consultant
    - Penetration testing
    - Phishing
    - Security training
  - Co-host of the PVCSec podcast
  - #misec!

Brief Storytime

There once was a company that had a penetration test…

…and no one was really sure what to make of it.

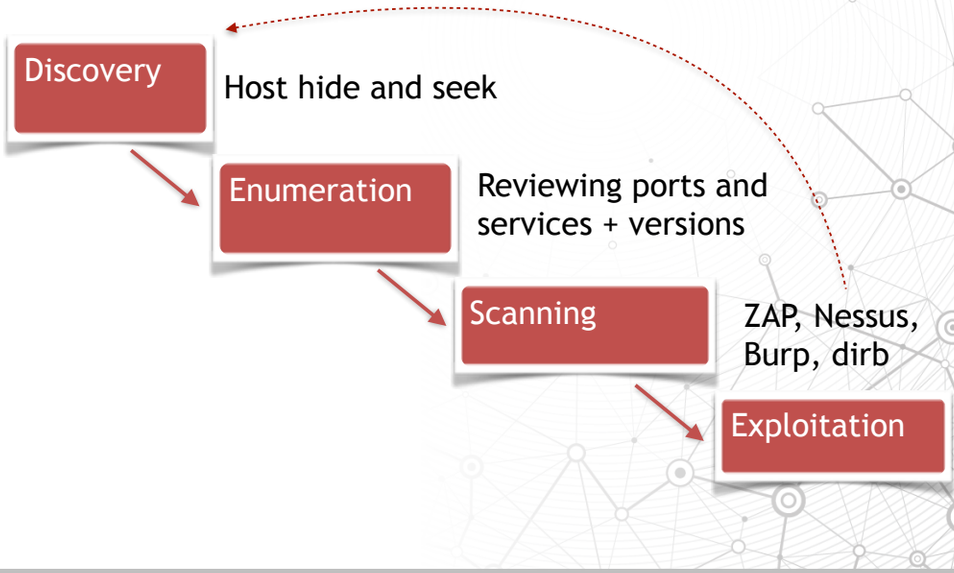
What is a Penetration Test?

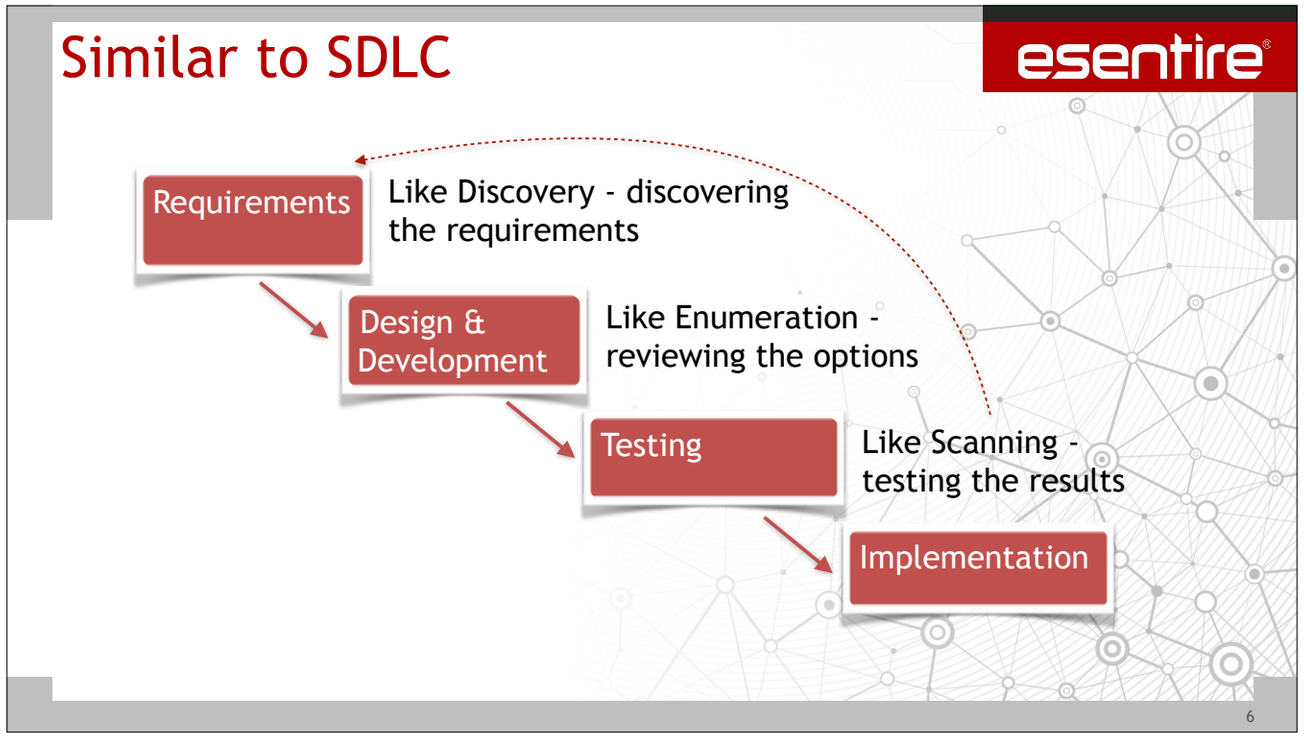
esentire

- Penetration tests are one form of “red teaming”.
- Security professionals using tools, knowledge, and creativity to try to discover problems.
- The result is a report detailing the findings from the perspective of an attacker.

An Attacker's Methodology

esentire





The SDLC is similar to the attacker's methodology
Both pen testers and QA testers are going to put the app through its paces
The end goal is just different

The Attacker's Toolbox

- Kali Linux's suite of tools
- Vulnerability Scanners (OpenVAS, Nessus, NexPose)
- Proxies (Burp, ZAP)
- Scanners (nmap, sqlmap)
- Recon tools (Google, Shodan)
- And much more

Kali comes with many of the popular tools pre-installed and ready to be used

Discovering Passive OSINT

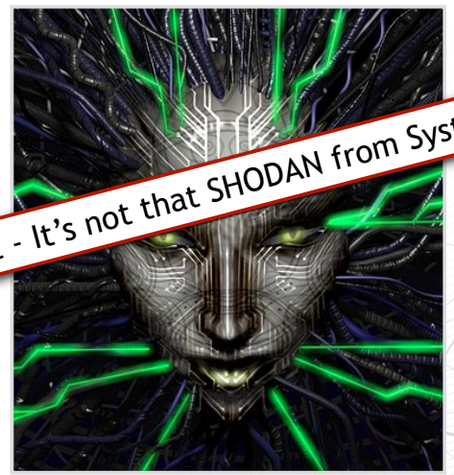
- A big reason why we cannot rely on obscurity for security.
- OSINT tools can enable attackers to stumble into opportunities, and it's easier when they have a target to narrow it down.

- Let's take a look at some passive intelligence gathering…

Introducing SHODAN

esentire

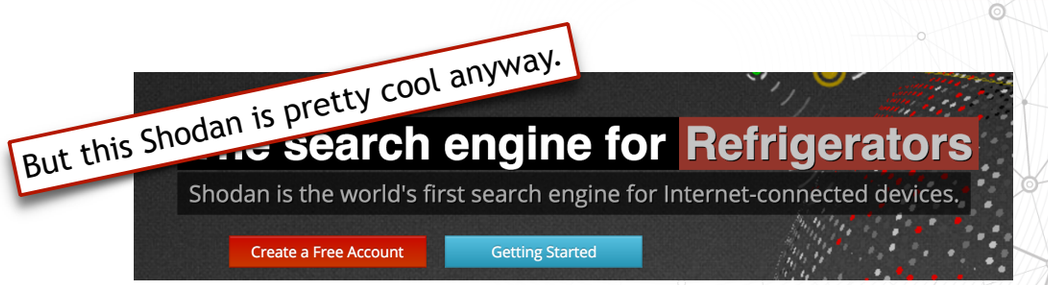
» The **S**entient **H**yper **O**ptimized **D**ata **A**ccess **N**etwork!



Scratch that - It's not that SHODAN from System Shock...

Introducing Shodan.io

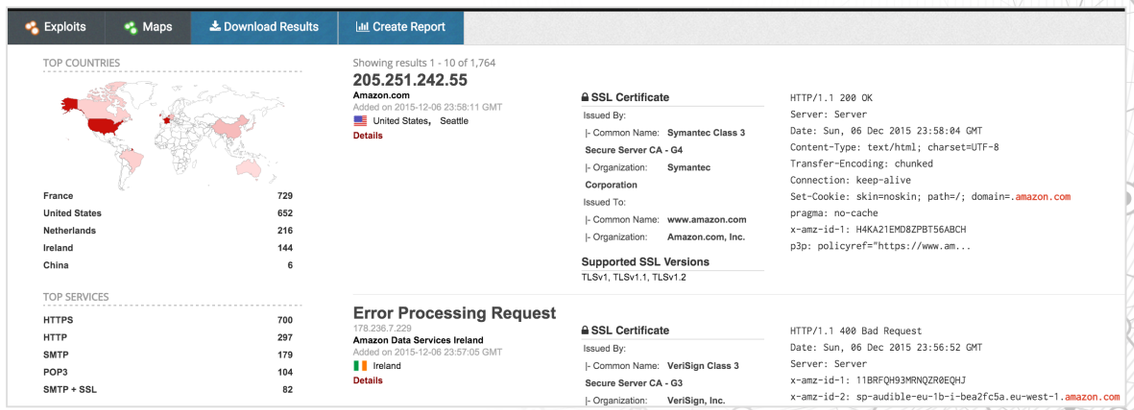
esentire



- A search engine for the *Internet of Things*.
  - Reveals services rather than webpages.
- Free, with a subscription option…
  - …which was just $5 on Black Friday.

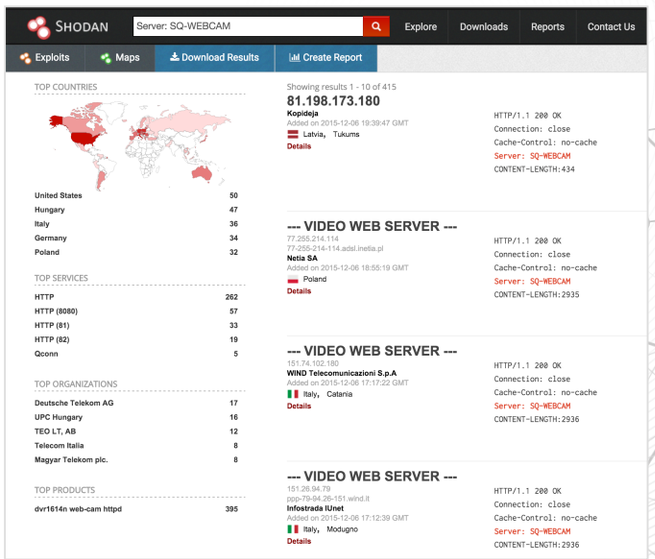
Shodan is a search engine for the INTERNET OF THINGS
What that really means is it’s designed to show you services, not webpages.

Shodan Delivers Domains



You can search for domains, like amazon.com.

Shodan Delivers Webcams



But where Shodan really signs is here, searching for products and services.

Yep, Those Are Webcams

https://www.shodan.io/host/213.168.188.38

If you make something available externally, Shodan will find it.

Black Hat Shodan

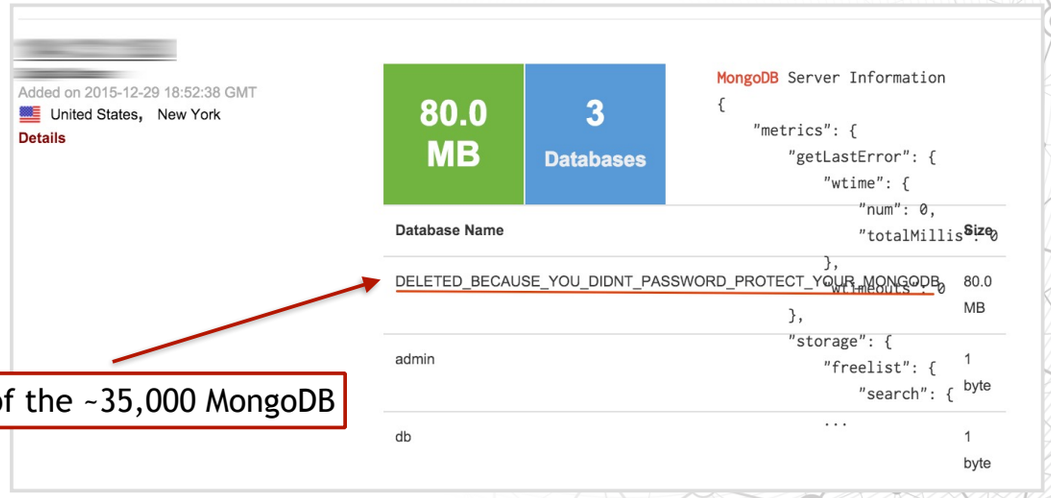
esentire

23
tcp
telnet

```
Connection refused: too many users
```

Black Hat Shodan

esentire



One of the ~35,000 MongoDB

https://www.shodan.io/host/104.131.18.0

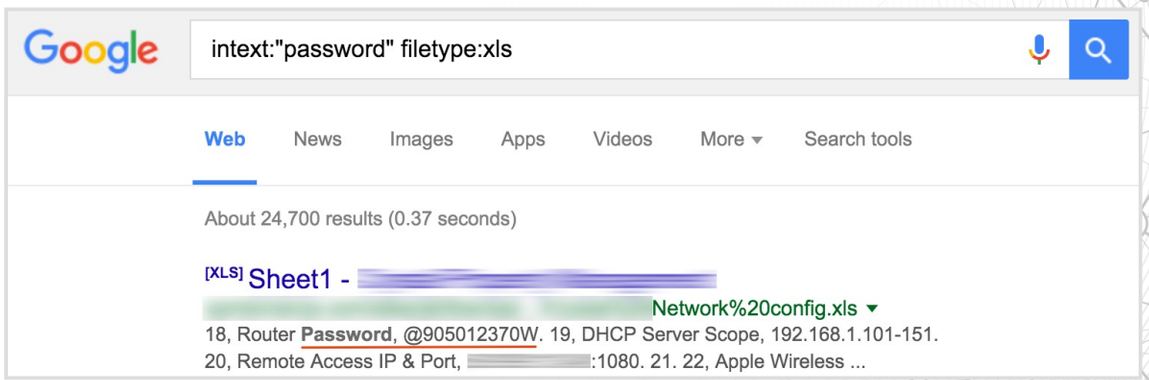
This is where it gets nasty.
Latest news regarding the 35,000+ of open MongoDB DBs with 684.8TB
http://www.csoonline.com/article/3016067/security/over-650-terabytes-of-data-up-for-grabs-due-to-publicly-exposed-mongodb-databases.html

Introducing Google Hacking

- https://www.exploit-db.com/google-hacking-database/
- Google does the hard work, finding and indexing everything publicly available
- Google's search keywords make it easy to filter results to find:
  - Files and their contents with *intext* and *filetype*.
  - Webcams, routers, and other webpages that can be found by the URL contents with *inurl*.

Googling for Passwords, For Real

esentire



You Don't Always Need an API

esentire

- You can learn a lot from an organization without turning to anything like Shodan.
  - *whois*
  - *theharvester*
  - Have I Been Pwned

```
Domain Name: CHRISMADDALENA.COM
Registry Domain ID: 1590194265_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-07-29T23:49:22Z
Creation Date: 2010-03-25T20:56:52Z
Registrar Registration Expiration Date: 2016-03-25T20:56:52Z
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Hover
```

Moving on to Active Scanning

- Once you find something of interest, the next step is to take action with active investigation techniques and tools.

```
kali# wpscan www.chrismaddalena.com
_____________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

      WordPress Security Scanner by the WPScan Team
                     Version 2.8
         Sponsored by Sucuri - https://sucuri.net
  @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_____________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]y
[i] Updating the Database
[i] Update completed.
[+] URL: http://www.chrism
[+] Started: Wed Dec 30 21
```

```
Parameter: username (POST)
    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind (SELECT)
    Payload: username=wrong' AND (SELECT * FROM (SELECT(SLEEP(5)))CGms) AND 'sWoY'='sWoY&password=wrong&submit=Log In
---
[22:28:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.10
web application technology: Apache 2.2.3, PHP 5.1.6
back-end DBMS: MySQL 5.0.11
```

Kali, theharvester, wpscan, and Nikto

DEMO TIME

Common Findings: OWASP Top 10

esentire

» Often discovered during penetration tests…

Common Findings

- The OWASP Top 10 are penetration tester favorites.
- They are also often targeted for sport and potential profit.
- They can appear over time as new issues are discovered in aging versions of platforms and CMSs.
- Bug bounty hunters enjoy the $$$ rewards.
- Others may simply enjoy finding the problems for mischief.

Why This Matters

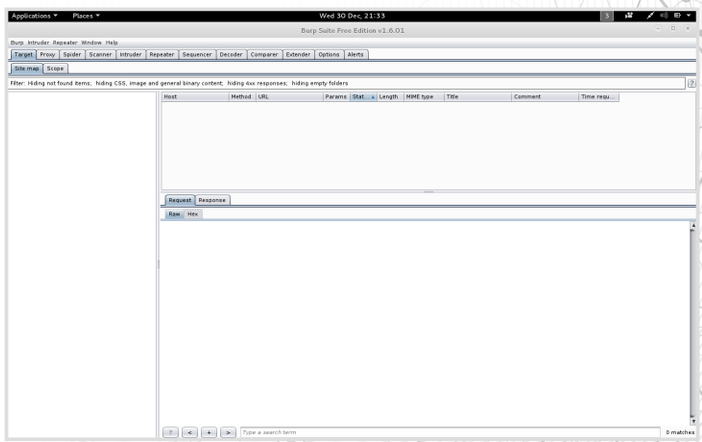
- It can provide a foothold or access to data.
- Possible outcomes to a web app's compromise during a test:
  - Manipulation of the app. (ex: Auth Bypass, SQLi)
  - Access to the server running the app, and the server's data and files. (ex: LFI)
  - Control of the server running the app. (ex: RFI)
- Malicious outcomes to a compromise:
  - Compromise of the app's users. (ex: XSS)
  - Destruction or manipulation of the app's data.

Finding These Vulnerabilities

- They can be found manually, but this is time consuming.
  - Manual testing is still important. 
- Penetration testers use tools to analyze web apps.
  - Acunetix ($$)
  - Burp Suite (Free or $)
  - OWASP ZAP (Free)

Burp (Excuse me) Proxy

- Free to use, only slightly limited.
- Full license is $300/ year.
- It can spider, capture GET/POST, brute force, repeat requests, and more.



Burp Proxy in Action

esentire

- Burp can do a LOT, but the proxy is fantastic.
- You can capture and review requests!

Request

Raw | Params | Headers | Hex

```
POST /demo1 HTTP/1.1
Host: [redacted]:3000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

year=res.write('SSJS Injection')
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
X-Powered-By: Express
Date: Thu, 05 Feb 2015 17:41:53 GMT
Connection: keep-alive
Content-Length: 14

SSJS Injection
```

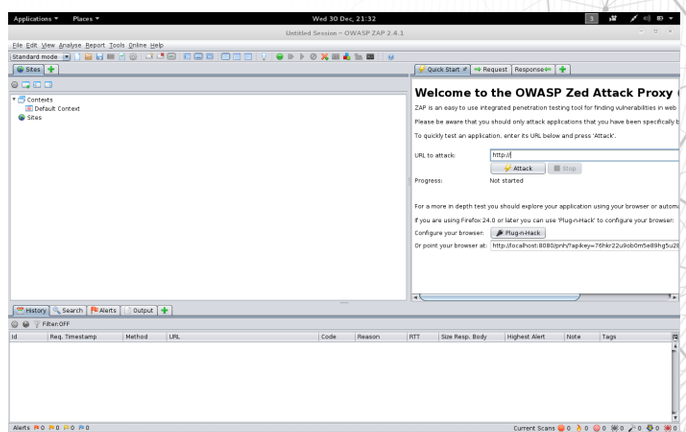
- Here is a Server Side JavaScript exploit example.

Example from **s1gnalcha0s** on GitHub

Server Side JavaScript Injection against Node.js example

ZAP (Zed Attack Proxy)

- Totally free!
- As easy as entering a URL to get started.
- Runs through a whole battery of tests to find low hanging fruit.
- Simple to run during the testing phase, while at lunch, whenever.



Burp, SQLMap, and OWASP ZAP

DEMO TIME

Applying This Information

- Try out ZAP on your own applications.
  - Consider using it consistently, during testing or as a semi-regular audit tool.
- Give Burp a try to see exactly how your apps work.
  - You can use it on other websites and apps, too!
  - Be curious and learn.

But Why?

- Finding the low hanging fruit will save time later.
  - Fix it now while the app is in testing.
  - Avoid a penetration tester finding it later.
- ZAP experience may become important to you.
  - Web app security won't be going away.
  - Being able to talk about your experience with it could be beneficial in interviews.
- It's really simple to get started.
  - Even if you don't do much more, that's MUCH better than nothing.

Learning Resources

- Local security groups and conferences
  - #misec
  - #ohsec
  - BSides - Great one day conferences.
    - BSides Indy (March), BSides Cleveland (June), BSides Detroit (July)
    - CONverge (Detroit, July)
    - CircleCityCon (Indy, June)
- Web Application Hacker's Handbook
- Bug Hunter's Methodology

Final Thoughts & Questions

» Questions?


esentire®
Thank You!
Chris Maddalena
@cmaddalena