



Edge Hill University

The Department of Computer Science System Penetration Testing 2019

Courework

Jakub (Jacob) Strykowski 24325457

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
PORTFOLIO 1	4
AN INTRODUCTION TO INFORMATION GATHERING AND OPEN SOURCE INTELLIGENCE (OSINT).....	4
USE THE TOOLS LISTED BELOW TO GATHER INFORMATION ABOUT YOUR CHOSEN WEBSITE.	6
1.1.1 <i>GOOGLE SEARCH AND GOOGLE HACKS</i>	6
1.1.2 <i>Google Hacking - Conclusion</i>	15
1.1.3 <i>Whois</i>	16
1. WEB ROBOTS	21
2. EMAIL HARVESTER.....	23
3. NMAP	25
4. BANNER GRABBING – NETCAT	29
5. YOUR CHOICE OF INFORMATION GATHERING TOOL OR COMMAND OR SOFTWARE.....	30
1.5.1 <i>Python</i>	30
1.5.2 <i>Nmap</i>	31
CONCLUSION AND LIST OF REFERENCES.....	34
REFERENCES PORTFOLIO 1	35
PORTFOLIO 2	36
TECHNICAL REPORT VULNERABILITY ASSESSMENT - INTRODUCTION.....	36
VULNERABILITY ASSESSMENT TOOL	36
VULNERABILITY VALIDATION	37
CVE-2010-0425	38
CVE-2010-4478	39
CVE-2019-10210	40
CVSS Version 2.0	40
CVSS Version 3.x.....	41
CONCLUSION PORTFOLIO 2	41
APPENDICES PORTFOLIO 2	42
BIBLIOGRAPHY	48
PORTFOLIO 3	49
PREPARATION PHASE	51
XSS.....	51
SQL INJECTION	53
HEARTBLEED.....	57
PEN TESTING PHASE AND RECOMMENDATION PHASE	59
<i>Happy Shop Inc – Network diagram</i>	59
<i>Virtual Box Set Up</i>	60
STEP 2: TARGET SCANNING/PROBING	60
<i>Netdiscover -i eth0</i>	61
<i>Figure 1</i>	61
<i>Figure 2</i>	61

<i>Figure 3</i>	62
<i>Figure 4</i>	62
<i>Figure 5</i>	63
<i>Nmap -O (IP Address)</i>	63
<i>Figure 6</i>	64
<i>Figure 7</i>	64
<i>Figure 8</i>	65
<i>Figure 9</i>	66
<i>Figure 10</i>	66
<i>Figure 11</i>	67
<i>Figure 12</i>	67
STEP 4: VULNERABILITY ASSESSMENT	68
VULNERS FOR CVE FOR WEB SERVER (192.168.56.101).....	72
<i>Figure 13</i>	72
DATABASE SERVER (192.168.56.105)	73
<i>Figure 14</i>	73
WINDOWS 7 (192.168.56.103).....	74
<i>Figure 15</i>	74
WINDOWS XP (192.168.56.104).....	75
<i>Figure 16</i>	75
STEP 5: VULNERABILITY ASSESSMENT OF WEB SERVER	76
NIKTO –HOST IP_ADDRESS –PORT 80.....	80
<i>Figure 17</i>	80
CONFIGURING BURP SITE FREE EDITION	81
<i>Figure 18</i>	81
<i>Figure 19</i>	81
<i>Figure 20</i>	82
<i>Figure 21</i>	82
<i>Figure 22</i>	83
<i>Figure 23</i>	83
<i>Figure 24</i>	84
CONCLUSION	84
REFERENCES PORTFOLIO 3	85

PORTFOLIO 1

AN INTRODUCTION TO INFORMATION GATHERING AND OPEN SOURCE INTELLIGENCE (OSINT)

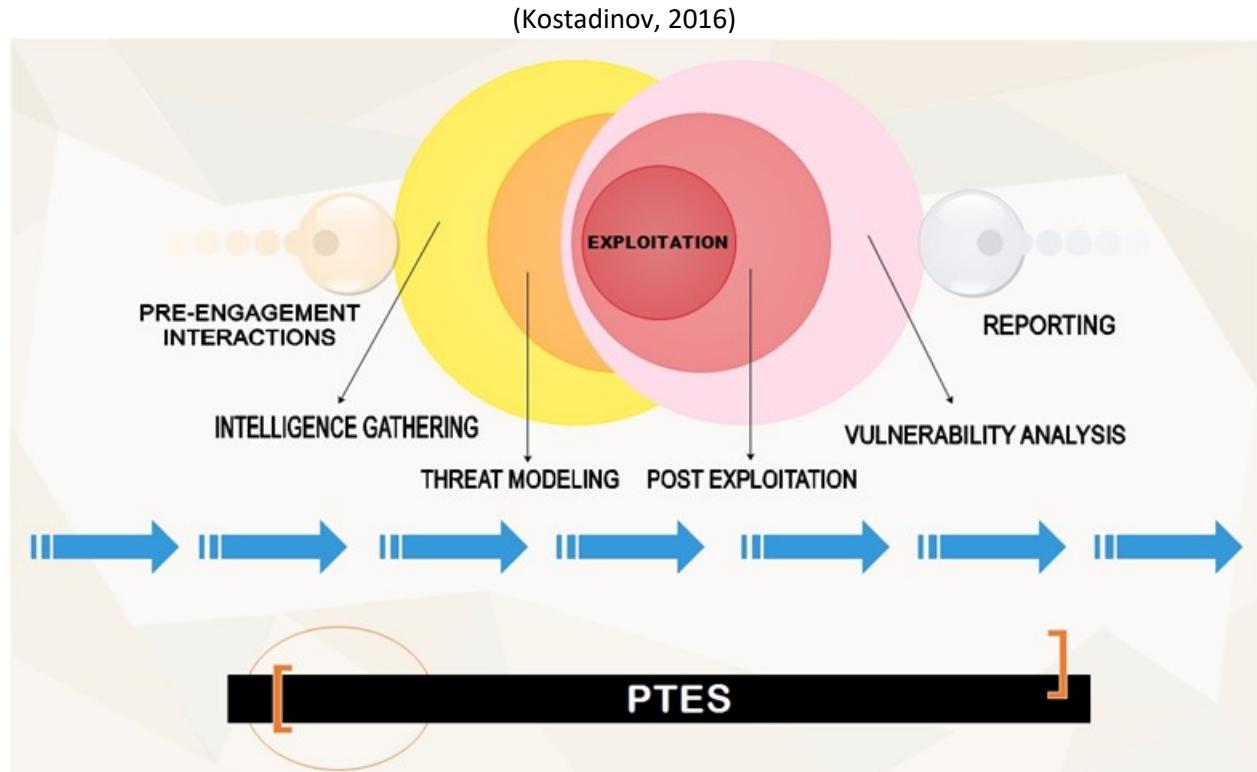


Figure 1

System penetration testing is one of the solutions for problem with cybercrime. Company or individual can hire a system pen tester to validate security of their systems. The process starts from pre-arrangement meeting (figure 1) where both sides discuss the goals and limitations. Next step is information gathering, pen tester collects publicly available information about client and looks for data which would helpful in future exploitation of the client's system. Information gathering is crucial for later steps, because without useful information pen tester would not be able to find any vulnerability which are necessity in exploitation of the system (Dimov, 2019).

"Information gathering is not just a phase of security testing; it is an art which every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing"
(<https://www.w3schools.in/>, nd).

However, more gathered information would obtain by providing more vulnerabilities. Information Gathering can be doing in two ways passive and active. Passive Information Gathering based on information which pen tester can collect without establishing connection with the target (Obbayi, 2019). Pen tester during passive Information Gathering have more time, because victim do not know about being targeting by pen tester. Examples of passive Information Gathering are data about topology of organisation network and types of using services within, but also credentials of personnel which pen tester may use to fishing or blackmail at later date (Ollmann, 2004). Pen tester for passive Information Gathering can use: Google Hacking, the Harvester, Whois or Web Robots (Dimov, 2019). Active Information Gathering require pen tester to establish connection with target, it is a potential

risk for pen tester of being stopped by client's cybersecurity department. Pen tester should carefully scan the target's network to avoid detection by Intrusion Detection System or Security Information and Event Management's tools (Obbayi, 2019). Pen tester to active Information Gathering can use programmes: Nmap, Netcat or SPARTA (nd, nd).

Open source intelligence (OSINT) is a process of intelligence collection, it used data from publicly available sources which produce actionable intelligence (Wikipedia, 2019). The information used to OSINT can be in various forms like text, file, audio, video, image etc (Passi, 2018).

Why do it?

- Determinate various entry points in an organization, which can be physical electronic and/or humans
- Many companies publish information which attacker can use.
- Many employees use social accounts, where they share information which attacker can use to compromise themselves or their employee. The best source of employees' personal information are social media, websites like Facebook, Twitter, LinkedIn etc hold a lot of user data.
- The gather information is published in the internet in many cases for free and everybody can access it unless it is restricted by law or an organization (Passi, 2018).

Why not do it?

- OSINT may be not time-effective
- Gather information might be deliberate or accidentally manipulated.

OSINT forms:

- Passive reconnaissance used only public facing infrastructure, also this form of gathering does not require sending any traffic to target, and pen tester can stay as much as it is possible anonymous. Examples of Passive Information gathering are: OSINT Framework, Google Hacks, theHarvester, Maltego. The cons are time it takes and result with not completed information, of course the information can be gathered in faster way with active scanning, but active scan can be easier detected (CYBERSEC, 2018).
- Semi-passive is form of OSINT where pen tester gathers information using methods which would appear like normal Internet traffic and behaviour. Pen tester cannot use brutal force DNS request or run network level port scan, because during semi passive it is not looking for "unpublished" servers or directors. However, the key here is to be unspotted by target, in that reason pen tester can only looking at metadata in published documents or files (nd, nd). Examples of Semi-Passive Information gathering are Whois, social engineering (Dimov, 2019).
- Active information gathering starting when pen tester actively engaging with target. In this stage pen tester is actively mapping client's network infrastructure, it is looking for 'unpublished' services, files or directories. Active information gathering is largest part of information gathering process, it is called "reconnaissance" or "scanning", the tools used to it are Nmap, Banner Grabbing, Nikto etc.

USE THE TOOLS LISTED BELOW TO GATHER INFORMATION ABOUT YOUR CHOSEN WEBSITE.

1.1.1 GOOGLE SEARCH AND GOOGLE HACKS

The internet is huge part of nowadays live. It allows people to buying things, sharing videos or mailing. The banking system in our society is now online, more and more finical operation is doing online. Users who want to use all services have to fill a valuable credentials. The risk the personal information would been stolen is growing to number of used websites. The hackers can theft money form bank account or hack other services using user's data or even find the place of living. This piece of paper would state how important is personal data security.

Google Search and Google Hack Operator	List of information gathered
--	------------------------------

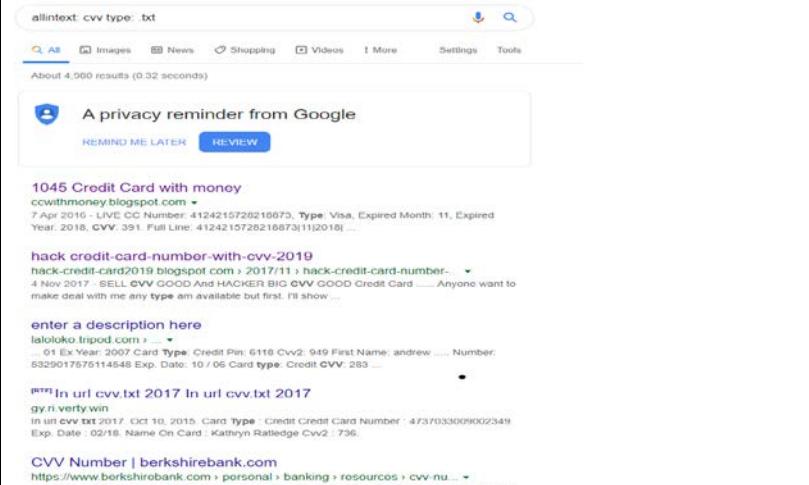


Figure 2

1.1.1.1 allintext: CVV

It results is site with 1045 Credit Card numbers and CVV and a lot of different websites with more result. On hack-credit-card-with-cvv is an information about “approval” this credit card number. Probably not all of these websites are valid, otherwise, a few of record looks quite litigable. (It is not ethical to check those data).



(nd, 2016)

Figure 3

(nd, 2017)

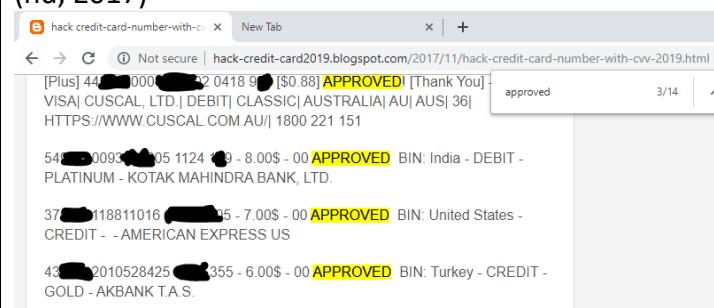


Figure 4



Figure 5

1.1.1.2 *Intitle: index of/admin*

The screenshot shows a Google search results page for the query "intitle: index of/admin". The results include:

- Index of /admin - LawWagon**
https://www.lawwagon.com › admin
Name · Last modified · Size · Description · Parent Directory, ~, assets.zip, 2019-04-24 18:08, 20.0M. assets/, 2019-02-27 10:37, ~, assets_min/, 2019-04-25 12:17, ~
- Index of /admin - Sunrise Valley Resort**
www.sunrisevalleywayanad.com › admin
Name · Last modified · Size · Description · Parent Directory, ~, accordion1/, 2018-03-15 09:43, ~, alert/, 2018-03-15 09:58, ~, css/, 2018-03-15 09:58, ~
- Index of /admin - Montebello Villa Hotel**
www.montebellovillahotel.com › admin
Name · Last modified · Size · Description · Parent Directory, ~, mvhlogo01.png, 2019-03-14 23:28, 5.5K. promo/, 2019-01-29 21:18, ~, sig/, 2019-01-31 03:49, ~

Figure 6



Figure 7

Using of the google hacking operator intitle: allowed to collect the video from cctv upper reception. On screen shot it's highlight information:

- Personal data of client. It would be even fiscal information like credit/debit card number
- Notes for staff, there could be information, about work hours of staff, files, or even password
- Third is the computer view. It would be able to consider what software company is using. There screen of computer can give access to private company information

Google bmw.com filetype:pdf

Information about the software update

Content	Installation
<p>These instructions provides information about the software update.</p> <p>The content of this software update depends on the software version of your vehicle.</p> <p>For details about the software update and supported devices, please refer to the description below.</p> <p>One of the following versions will be installed depending on your vehicle:</p> <ul style="list-style-type: none"> ▷ HN 003.255.080 & MN 002.255.071 & TN 002.255.080 ▷ HN 003.255.080 & MN 003.001.002 & TN 003.255.080 ▷ HN 003.255.080 & MN 003.003.001 & TN 003.255.080 ▷ HN 003.255.080 & MN 003.009.004 & TN 003.255.080 ▷ HN 003.255.080 & MN 003.011.002 & TN 003.255.080 ▷ HN 003.255.080 & MN 003.013.001 & TN 003.255.080 	<p>The installation of the software updates requires the consent to the use rights conditions. For this purpose, refer to www.bmw.com/update. For the installation, save the file for the software updates on a USB device to the main directory and connect the USB device at the centre armrest.</p> <p>In addition, observe the notes in the Owner's Handbook Navigation, Entertainment, Communication under software update.</p> <p>After installing the software update in the vehicle, the new software version will be displayed:</p> <ol style="list-style-type: none"> 1. "My Vehicle" 2. "Drive settings" 3. "Software update" 4. "Show current version"
Conditions	Notes
<p>The software update is only available for certain vehicles that are equipped with the USB audio interface.</p> <p>You can check if your vehicle is supported on the website under www.bmw.com/update or in the compatibility matrix under www.bmw.com/bluetooth.</p> <p>For more information about the software update, refer to the Owner's Handbook Navigation, Entertainment, Communication.</p>	<p>Switch off the vehicle at the end of the software update.</p> <p>Transmitted data from external devices will be re-synchronized where required.</p> <p>Tracks or playlists that were played back prior to the software update must be reselected.</p> <p>This is also required for the restoration of earlier software versions:</p> <ol style="list-style-type: none"> 1. "My Vehicle" 2. "Drive settings" 3. "Software update" 4. "Restore software" <p>When the software is restored or updated by the service partner, manually generated changes for music files may be deleted.</p>

2

Information about the software update UPD0508

If the following menu item is not displayed correctly after the software update, briefly deactivate Bluetooth for the installation:

1. "Communication"
2. "Manage mobile devices"
3. "Settings"
4. "Bluetooth:"

Software update (TN & MN 002.052.001)

The software update makes the following adjustments:

ConnectedDrive

▷ Improves ConnectedDrive Services.

Figure 8

(Wikipedia, 2018)

ConnectedDrive

From Wikipedia, the free encyclopedia

ConnectedDrive is a collection of electronic features for BMW vehicles. ConnectedDrive was introduced in 2008 at the Geneva Motor Show^{[1][2]} as a web browser built-in to the car's infotainment system. Additional features have been added since, such as Smartphone integration, synchronising with calendars, head-up display, lane departure warning system, traffic information, active cruise control, night vision and traffic information.^[3]

2015 security flaw [edit]

In 2015, ADAC (a German motoring association) discovered security flaws in the ConnectedDrive system which potentially allowed attackers to remotely unlock the vehicle.^{[5][6]} To fix this flaw, BMW released a security update, which was automatically installed via the Internet.^[7] There are no reports of the flaw being used to gain unauthorised access to a vehicle.^[8]

1.1.1.3 filetype

After using operator 'filetype' I found the file with information about software update(figure8). I checked what is Improves Connected Drive Service. On Wikipedia it paragraph about flaws which is potentially risky for this system. (2015) The file is from 2018, but this vulnerability can be not update in cars without access to the internet. The car owners have to install update manually, it can be seemed that a few people did not download it. The cars with this system can connecting with smartphone it could be different way to hack this system. Additionally, this system is important for safety of car users (figure9):

- lane departure warning system
- active cruise control
- night vision

The hackers who break into this system can blackmail BMW and demand considerable money for not using it. The application of allintext is scan text to search input phrase. In this case it was used to find information about Security updated in BMW company. The result is page containing

Figure 9

(BMW, 2018)

allintext: bmw security update

About 22,000,000 results (0.48 seconds)

A privacy reminder from Google

REMIND ME LATER REVIEW

[Comfort access key security update - G30/G31 2017- - BMW 5 Series ...](#)

<https://forum.bmw5.co.uk> › Technical › G30/G31 2017- ▾
2 Jan 2019 - 7 posts - 4 authors
Comfort access key **security update** ... I read that **BMW** had introduced motion detection into comfort 700 Euro to fix their security problem ?

[BMW Fixes Security Flaws in Several Well-Known Car Models](#)

<https://www.bleepingcomputer.com> › News › Security ▾
22 May 2018 - **BMW** Fixes **Security** Flaws in Several Well-Known Car Models ... component **update** system, and is also working on delivering firmware patches ...

- [BMW security hack - solution now implemented - Page 1 - General](#)
...
<https://www.pistonheads.com> › gassing › topic ▾
8 Feb 2015 - Basically the **security** hole is in the communication between vehicle and ...
Supposedly **BMW** has now sent a remote **update** via SMS to all ...

information regarding lack in car security.
There is a brief description and list of cars with that vulnerability.

Figure 10

(Keeling, 2018)

manchestereveningnews.co.uk/news/greater-manchester-news/keyless-car-relay-theft-advice-14496158

Manchester EveningNews

NEWS MAN UTD MAN CITY WHAT'S ON IN YOUR AREA SPORT CELEBS BUSINESS LIVE PROPERTY S

2010, 8 NOV 2018 | UPDATED 2012, 8 NOV 2018

Enter your postcode for local news and info Enter your postcode Go In YourArea

09-25-2017 Mon 01:02:04

WEST MIDLANDS POLICE Click for Sound Camera 01

FOOTAGE SHOWS HOW EASY IT IS FOR THIEVES TO STEAL A CAR USING A RELAY DEVICE

Figure 11

BMW 225xe, 318i, 318d, 520d, 640d, 730d, 740, 740d, i3, i3 94 Ah (7/2016), i3 94 Ah (5/2016), X1, X1 SD
18d

Figure 12

1.1.1.4 Lauren Eshbach, allintext
1824 Allen lane Abington pa 19001
allintext:2156574817

(nd, n.d.)

The screenshot shows a search results page for 'eshbach' on telephoneDirectories. It lists several entries, with the relevant one being 'Laurel Eshbach 1824 Allen Ln..... 2156574817'. Other entries include 'Laureen Mount' and 'Mike Bodo'.

Figure 13

(nd, 2018)

The screenshot shows a Redfin listing for 1824 Allen Ln, Abington, PA 19001. The house was sold on July 13, 2018, for \$359,438. The listing includes details like 3 beds, 1.5 baths, and 1,514 sq ft. A large image of the house is displayed, showing a white garage and a brick exterior. A 'SOLD JUL 13, 2018' banner is visible at the top left of the image.

Redfin Estimate for 1824 Allen Ln

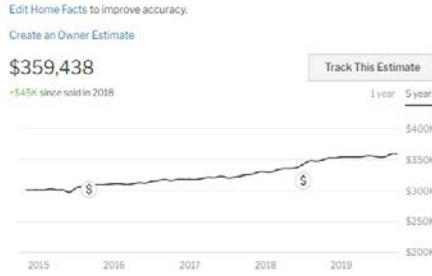


Figure 14

In previous example is record with name and credit card. The person who lose the credit card detail is suspect for being obvious target for gather more information.

- Using the address can give more information. The house was sold in 2018 (figure 14). First information is that the target has money after selling the house, otherwise, He is still in telephone Dictionaries perhaps he lives there until now. Both scenarios give attackers a lot valuable information.
- In google graphic (figure 17) is two pictures as a result for search "Lauren Eshbach". The consideration is not basic which one is the target, although pictures in bed room (figure 18) signalize person with white skin. The same pictures also give a detail about family, the

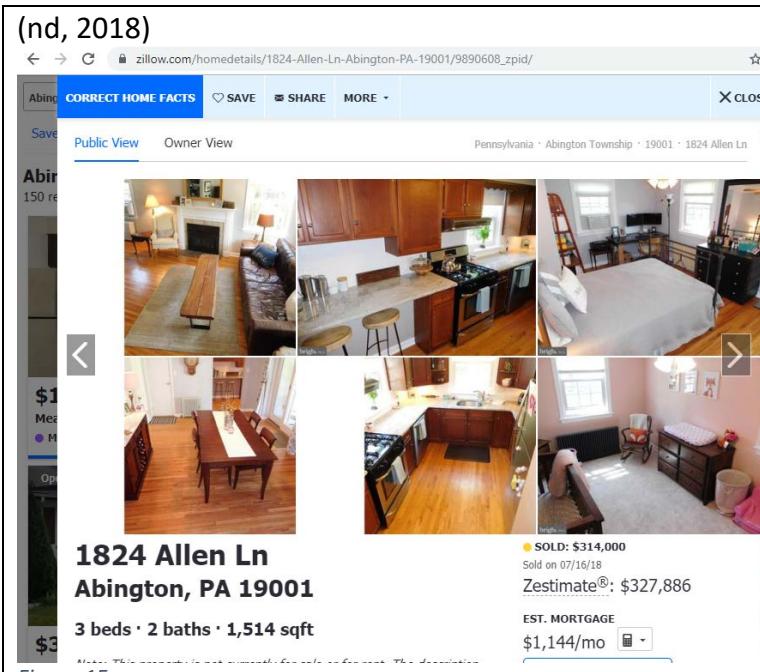


Figure 15

Lauren may have wife and daughter. Also, a box under the desk is containing cables, headphones this is next confirmation that this is real photo of Lauren. (figure15)

- Only one person with this name and address have LinkedIn account(figure16)

(Eshbach, nd)

This website uses cookies to improve service and provide tailored ads. By using this site, you agree to our [Privacy Policy](#) and [Terms of Use](#).

Laurel Eshbach
Digital Marketing Consultant at Accenture
Philadelphia, Pennsylvania • 373 connections

[Join to Connect](#)

Figure 16

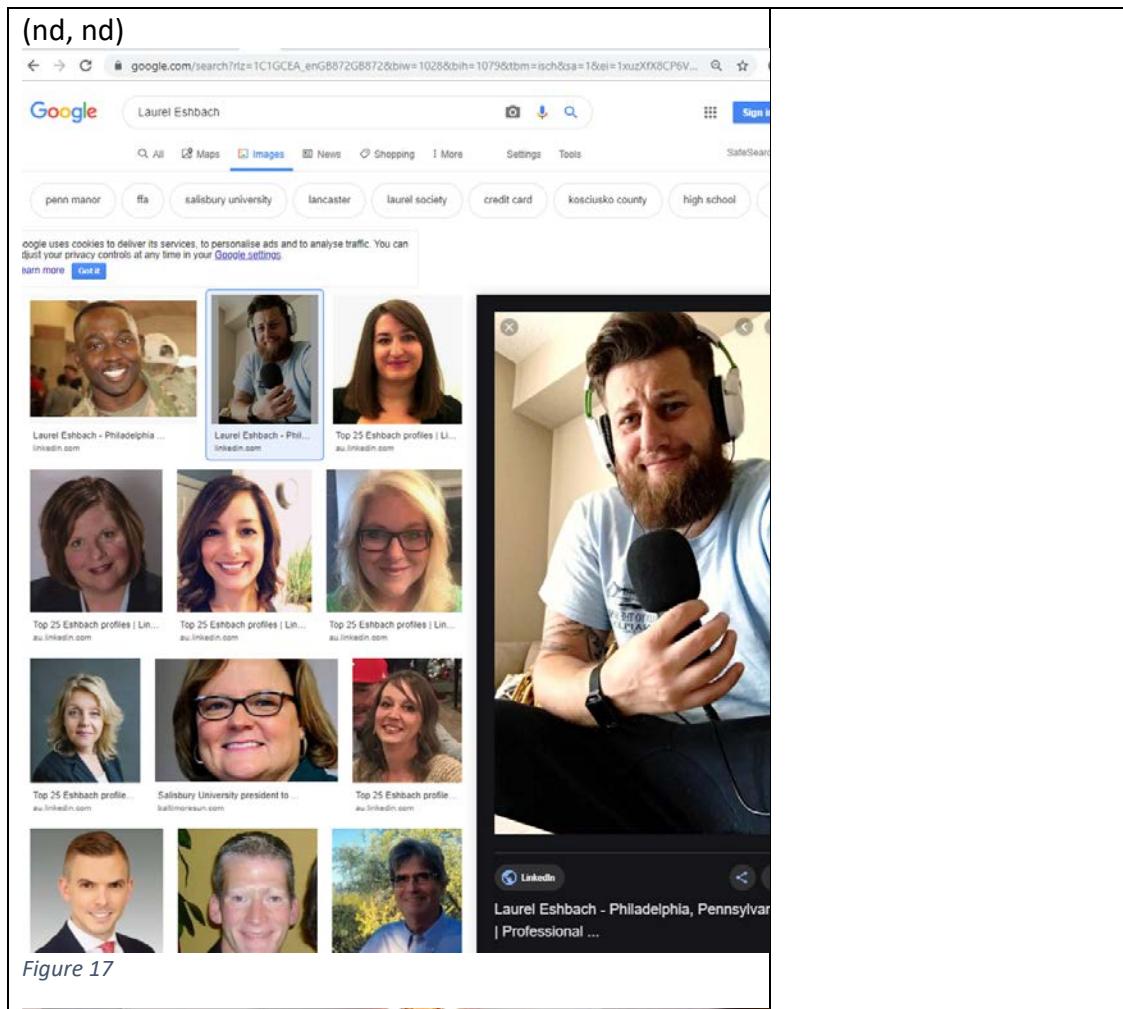
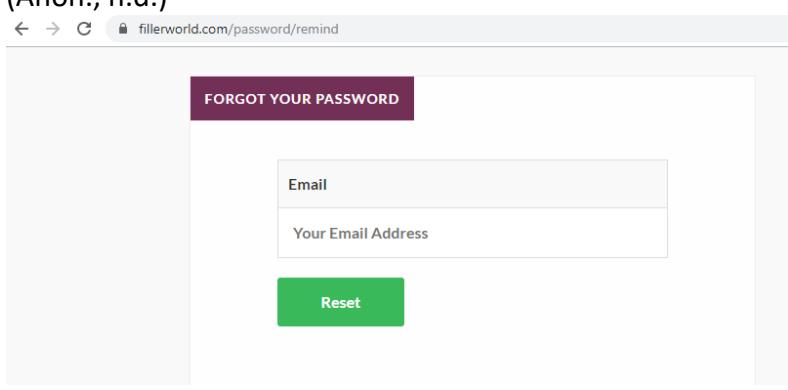


Figure 17



Figure 18

<p>1.1.1.5 site:*/password/remind</p> <p>(Anon., n.d.)</p>	
 <p>Figure 19</p>	<p>If attacker penetrated an email address, it can use this formula to magnify its privilege and get access to different websites.</p>

(Reference: <http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf>)

1.1.2 Google Hacking - Conclusion

The Google search is a powerful tool which allow users to find immeasurable amount of information. The fact the hackers also use it is not surprising. The google hack is a tool, which can be used to footprinting. It makes all leaks of date even more dangers for costumers comprised services. The crucial information is shared online by intruders or even people public sensitive data on social medias. Attackers can used information published online to prepare theft. An example presents the data collected using google hack command 'allintext: 'ccv' '. In white next on first page of result can be find lists credit card with note about true validity checked by datasheet author.

1.1.3 Whois

1.1.3.1 WHOIS example_1

Raw Whois Data

Domain Name: 2600.COM
Registry Domain ID: 2781441_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-10-04T19:10:16Z
Creation Date: 1994-02-03T05:00:00Z
Registrar Registration Expiration Date: 2021-02-04T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: 2600 Magazine
Registrant Organization: 2600 Magazine
Registrant Street: PO BOX 848
Registrant City: MIDDLE ISLAND
Registrant State/Province: NY
Registrant Postal Code: 11953-0848
Registrant Country: US
Registrant Phone: +1.6317512600
Registrant Phone Ext:
Registrant Fax: +1.7032650070
Registrant Fax Ext:
Registrant Email: emmanuel@2600.COM
Registry Admin ID:
Admin Name: Goldstein, Emmanuel
Admin Organization:
Admin Street: P.O. Box 848
Admin City: Middle Island
Admin State/Province: NY
Admin Postal Code: 11953
Admin Country: US
Admin Phone: +1.6317512600
Admin Phone Ext:
Admin Fax: +1.6317512600
Admin Fax Ext:
Admin Email: emmanuel@2600.COM
Registry Tech ID:
Tech Name: Goldstein, Emmanuel
Tech Organization:
Tech Street: P.O. Box 848
Tech City: Middle Island
Tech State/Province: NY
Tech Postal Code: 11953
Tech Country: US
Tech Phone: +1.6317512600
Tech Phone Ext:
Tech Fax: +1.6317512600
Tech Fax Ext:
Tech Email: emmanuel@2600.COM
Name Server: PHALSE.2600.COM
Name Server: NS1.HE.NET
DNSSEC: unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Figure 21

In this exercise a target is website 2600.com (figure 20). The selection this website is based on fact that the company has public index of secret containing pictures and articles about “secret service” (figure 22) and has online store (figure 23) with payment. This composition seems to be dangerous for personal information of costumers.

2600.com

Domain Information

Domain:	2600.com
Registrar:	Network Solutions, LLC
Registered On:	1994-02-03
Expires On:	2021-02-04
Updated On:	2016-01-28
Status:	ok
Name Servers:	ns1.he.net phalse.2600.com

Figure 20

Index of /secret/more

[ICO]	Name	Last modified	Size	Description
[ICO]	Parent Directory	-	-	-
[TXT]	codes.html	2001-02-25 21:22	17K	
[TXT]	freq.html	2001-02-25 21:22	552	
[TXT]	freq1.html	2001-02-25 21:22	7.0K	
[TXT]	freq2.html	2001-02-25 21:22	9.5K	
[TXT]	lairs.html	2001-02-25 21:22	12K	
[TXT]	objects.html	2001-02-25 21:22	2.7K	
[TXT]	people.html	2001-02-25 21:22	6.7K	
[TXT]	photo.html	2001-02-25 21:22	1.7K	
[DIR]	ss/	2013-04-13 12:37	-	
[IMG]	ss1.gif	2001-02-25 21:22	275K	
[IMG]	ss2.gif	2001-02-25 21:22	60K	
[IMG]	ss3.gif	2001-02-25 21:22	66K	
[TXT]	unknown.html	2001-02-25 21:22	1.4K	
[IMG]	varney4.gif	2001-02-25 21:22	140K	
[TXT]	words.html	2001-02-25 21:22	851	

Figure 22

List of information gathered example_1

store.2600.com/8373445/checkouts/7502a0ae27134e919a70222b9bab45db

Express checkout
\$ 7.99
PayPal

Contact information
Already have an account? [Log in](#)

Email

Shipping address

First name _____ Last name _____
 Company (optional) _____
 Address _____
 Apartment, suite, etc. (optional) _____
 City _____
 Country/Region Postcode _____
 Phone _____
[Return to cart](#) [Continue to shipping](#)

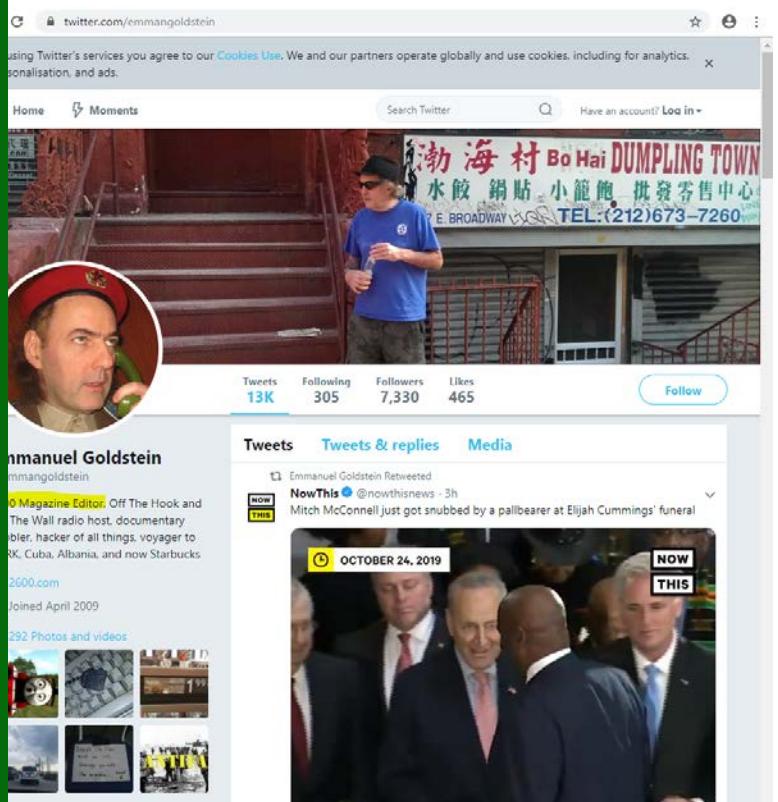


Figure 23

Figure 24

The most important is to gather information is administrator's credential(figure24). Those data might be helpful to break the password and get access to databased with clients' information.

(wikipedia, 2019)

Born	Eric Gordon Corley December 16, 1959 (age 59) Suffolk County, New York
Pen name	Emmanuel Goldstein
Occupation	Writer, editor, publisher, talk show host, voice actor, film director
Nationality	American
Alma mater	Stony Brook University English
Notable works	2600 Magazine, Dear Hacker, The Best of 2600: A Hacker Odyssey
Website	www.2600.com

Figure 25

The suspicion was not equivalent because the targeted admin is the well-known hacker (figure 25) and attacking his website does no seemed to be cost-effective.

1.1.3.3 WHOIS example 2



The screenshot shows a web browser window with the URL `whois.com/whois/indiamart.com`. The page displays detailed WHOIS information for the domain `INDIAMART.COM`. The data is organized into several sections: General Information, Registrant Details, Admin Contact, Technical Contact, and DNS Servers.

Domain Name: INDIAMART.COM
Registry Domain ID: 714683_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2019-08-26T08:38:45Z
Creation Date: 1996-03-08T05:00:00Z
Registrar Registration Expiration Date: 2029-03-09T04:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: IndiaMART InterMESH Limited
Registrant Organization: IndiaMART InterMESH Limited
Registrant Street: 7th Floor, Plot No. 7
Registrant City: Noida
Registrant State/Province: UP
Registrant Postal Code: 201301
Registrant Country: IN
Registrant Phone: +91.2067777777
Registrant Phone Ext:
Registrant Fax: +91.2067777777
Registrant Fax Ext:
Registrant Email: **dinesh@INDIAMART.COM**
Registry Admin ID:
Admin Name: Agarwal, Dinesh
Admin Organization: Indiamart Intermesh Ltd.
Admin Street: 7th Floor, Plot no 7, Sector 142
Admin City: Noida
Admin State/Province: U.P.
Admin Postal Code: 201301
Admin Country: IN
Admin Phone: +91.2067777777
Admin Phone Ext:
Admin Fax: +91.2067777777
Admin Fax Ext:
Admin Email: **dinesh@INDIAMART.COM**
Registry Tech ID:
Tech Name: Agarwal, Dinesh
Tech Organization: Indiamart Intermesh Ltd.
Tech Street: 7th Floor, Plot no 7, Sector 142
Tech City: Noida
Tech State/Province: U.P.
Tech Postal Code: 201301
Tech Country: IN
Tech Phone: +91.2067777777
Tech Phone Ext:
Tech Fax: +91.2067777777
Tech Fax Ext:
Tech Email: **dinesh@INDIAMART.COM**
Name Server: NS-1287.AWSDNS-32.ORG
Name Server: NS-1779.AWSDNS-30.CO.UK
Name Server: NS-961.AWSDNS-56.NET
Name Server: NS-62.AWSDNS-07.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: **abuse@web.com**
Registrar Abuse Contact Phone: +1.8003337680

Figure 26

From figure 25 can be read information about company called IndiaMART, figure 26 shows: company's address, admin's email and phone number. The information about admin can be used in process of footprinting. Also, data about company address can help with active information gathering.

1. WEB ROBOTS

Website developers used robots.txt to give instruction about their site to web robots (The Robots Exclusion Protocol). There are two standards for files “User-agent: *” what means everybody can access it and ‘Disallow: /’ what means robot should not have access to this file. However, the malicious robots can ignore it and access this file, because this file is shared online. (Reference: <http://www.robotstxt.org/robotstxt.html>)

```

User-agent: *
Disallow: /at/de/contacts/c/claudia-grabner.html
Disallow: /at/de/contacts/l/liane-hirner-002.html
Disallow: /ca/en/*.PDF
Disallow: /ca/en/*.pdf
Disallow: /ca/fr/*.PDF
Disallow: /ca/fr/*.pdf
Disallow: /content/pwc/global/forms/contactUsNew.html?parentPagePath=/content/pwc/de/*
Disallow: /de/contacts/c/claudia-grabner.html
Disallow: /de/publications/2017/PwC-LodgingTourismCapability%20Statement_E.pdf
Disallow: /de/technologie-medien-und-telekommunikation/gemo-2018.pdf
Disallow: /de/technologie-medien-und-telekommunikation/gemo-2018-executive-summary.pdf
Disallow: /en/events/1_Roche_Ian_Bishop_PWC_Geneva.pdf
Disallow: /en/events/10_Graduate%20Institute_Richard_Baldwin_PWC_Geneva.pdf
Disallow: /en/events/11_International%20Accounting%20Standards_Nic_Anderson_PWC_Geneva.pdf
Disallow: /en/events/2_UBS_Geoff_Robinson_PWC_Geneva.pdf
Disallow: /en/events/3_Richemont_Lesley_Griffiths_PWC_Geneva.pdf
Disallow: /en/events/4_Swiss%20Re_Swiss%20Re_Jutta_Bopp_PWC_Geneva_.pdf
Disallow: /en/events/5_S&P_Osman_Sattar_PWC_Geneva.pdf
Disallow: /en/events/6_Schroders_Harry_Jack_PWC_Geneva.pdf
Disallow: /en/events/7_Nestle_Adre_Besson_PWC_Geneva.pdf
Disallow: /en/events/8_ISS_Thomas_von_Oehsen_PWC_Geneva.pdf
Disallow: /en/events/9_Swissquote_Yvan_Cardenas_PWC_Geneva.pdf
Disallow: /en/publications/2017/pwc-sports-survey-2017.pdf
Disallow: /en/publications/2018/PwC%20Sports%20Survey-2018_web.pdf
Disallow: /gx/en/audit-services-risk-assurance-services/assets/PwCs_journals_ai.pdf
Disallow: /ie/en/eloqua/*
Disallow: /it/CEO17
Disallow: /it/ceo17
Disallow: /it/CEO2017
Disallow: /it/ceo2017

```

Figure 27

Figure 27 shows a lot of disallowed files which can contain important information for example about CEO as can be seen on the bottom of figure.

```

Disallow: /*/shop/bag*
Disallow: /*/shop/change_password*
Disallow: /*/shop/checkout*
Disallow: /*/shop/create_account*
Disallow: /*/shop/favorites*
Disallow: /*/shop/identify_user*
Disallow: /*/shop/mobile/checkout/start*
Disallow: /*/shop/mobile/*
Disallow: /*/shop/np/order*
Disallow: /*/shop/np/giftorguestorder*
Disallow: /*/shop/np/sign_in*
Disallow: /*/shop/question/answer/report*
Disallow: /*/shop/question/subscribe*
Disallow: /*/shop/question/unsubscribe/*
Disallow: /*/shop/review/vote*
Disallow: /*/shop/reviews/report*
Disallow: /*/shop/rs-mvt/rel/*
Disallow: /*/shop/sentry*
Disallow: /*/shop/sentryx/change_password*
Disallow: /*/shop/sentryx/create_account*
Disallow: /*/shop/sentryx/create_account_confirm*
Disallow: /*/shop/sentryx/identify_user*
Disallow: /*/shop/sentryx/sign_in*
Disallow: /*/shop/signed_in_account*

```

Figure 28

Figure 28 shows a lot of disallowed files which might contain crucial for security of website information, for example files with changes in password politics. Hackers can use this information to prepare the attack, an important fact is that apple.com has an online shop and hackers might steal financial information of users.

2. EMAIL HARVESTER (theharvester):

(Reference: <https://tools.kali.org/information-gathering/theharvester>)

Theharvester is tool used in passive information gathering, it is gathering information published online like emails, subdomains, host, employee names, open ports. It is preinstalled on Kali Linux and is helpful in first part of gathering process when pen tester and be as quiet as it is possible, in that reason should not connect to client.

theharvester	List of information gathered
<pre>Harvesting results [+] Emails found: ----- No emails found [+] Hosts found in search engines: ----- Total hosts: 12 [-] Resolving hostnames IPs... .microsoft.com:empty Account.microsoft.com:104.72.181.144 compass-ssl.microsoft.com:104.68.185.35 developer.microsoft.com:23.55.30.212 docs.microsoft.com:23.55.4.231 mail.microsoft.com:157.58.197.10 msdn.microsoft.com:23.43.20.145 msdn2.microsoft.com:23.43.20.145 office.microsoft.com:52.109.88.49 schemas.microsoft.com:2.19.146.99 support.microsoft.com:23.217.4.158 www.microsoft.com:23.43.32.148 root@kali:~#</pre>	From figure 29 can be read data about services which are provided by Microsoft. Also, the harvester search result with ip port addresses which might be used in active gathering information where are used net scanners like Nmap. An example of result is developer.microsoft.com with ip address 23.55.30.212.

Figure 29

theharvester	List of information gathered
<pre>root@kali:~# theharvester -d google.com -l 500 -b google [+] Hosts found Searching 500 results... Harvesting results [+] Emails found: ----- No emails found [+] Hosts found in search engines: ----- Total hosts: 2 [-] Resolving hostnames IPs... support.google.com:216.58.210.46 www.google.com:172.217.169.68</pre>	Figure 30 resulted with website addresses and ip addresses of those websites. There are not any emails and just two websites: support.google.com with ip address 216.58.210.46 and www.google.com with ip address 172.217.169.68

3. NMAP

Nmap or the full name is ‘Network scanner’, it is a free and open source network scanner created by Gordon Lyon (wikipedia, 2019; nd, nd). Pen testers use Nmap for task as network inventory, managing services upgrade schedules, and monitoring host or service uptime.

Nmap is so popular even it was used in twelve movies one of them was The Matrix Reloaded, the popularity of this tool cause large user support community (nd, nd). An example of standard scan is “nmap -sV [target’s ip address]” and If pen tester uses Kali Linux, it does not need to install Nmap because Nmap is pre-installed. Nmap is simple for new user to star it out because to run a command in terminal is just needed to write “nmap”, settings and target’s ip address. Nmap is command line based, otherwise there are also programmes which add graphic user interface to nmap for example Zen map. One of the Nmap advantages is portability, because most operating system are supported, for example Linux, Microsoft Windows and Mac Os. Nmap can scan thousands of machines, in that reason it can be used to build topology of huge networks.

Nmap has a few useful features:

1. Active port scanning
2. Host discovery
3. OS detection
4. Application version detection

NMAP	<pre>root@kali:~# nmap -sT 192.168.56.103 Starting Nmap 7.70 (https://nmap.org) at 2019-10-11 11:11 +0000 UTC Nmap scan report for 192.168.56.103 Host is up (0.00086s latency). Not shown: 990 closed ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds 5357/tcp open wsdapi 49152/tcp open unknown 49153/tcp open unknown 49154/tcp open unknown 49155/tcp open unknown 49156/tcp open unknown 49157/tcp open unknown MAC Address: 08:00:27:2C:95:0F (Oracle VirtualBox v Figure 31</pre>
List of information gathered	The operation nmap – sT 192.168.56.103 show us list of open ports on this ip address. Command -sT use TCP connection for gather information, it can be useful when firewall block UDP connection.

NMAP	<pre>root@kali:~# nmap -sV -p 80 192.168.56.103 Starting Nmap 7.70 (https://nmap.org) at 2019-10-07 09:56 EDT Nmap scan report for 192.168.56.103 Host is up (0.00045s latency). PORT STATE SERVICE VERSION 80/tcp closed http MAC Address: 08:00:27:2C:95:0F (Oracle VirtualBox virtual NIC) Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds</pre> <p><i>Figure 32</i></p> <pre>root@kali:~# nmap -sV -p 135 192.168.56.103 Starting Nmap 7.70 (https://nmap.org) at 2019-10-07 10:15 EDT Nmap scan report for 192.168.56.103 Host is up (0.00041s latency). PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC MAC Address: 08:00:27:2C:95:0F (Oracle VirtualBox virtual NIC) Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 23.18 seconds</pre> <p><i>Figure 33</i></p>
List of information gathered	This port 80 is web service port and it is closed (figure32). The port 135 is open, it is possible to get system information and name of software working on that computer (figure33). In this case of port 135 the operation system is Windows

List of information gathered	<pre> root@kali:~# nmap -sT 192.168.56.101 -p 22 --script=banner Starting Nmap 7.70 (https://nmap.org) at 2019-10-29 12:16 EDT Nmap scan report for 192.168.56.101 Host is up (0.00060s latency). PORT STATE SERVICE 22/tcp open ssh _banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds </pre> <p><i>Figure 34</i></p> <p>Banner script is used to collect information during five-second-long TCP connection with targeted ip address and/or port of it. The script is available at: https://github.com/nmap/nmap/blob/master/scripts/banner.nse. Figure 34 shows 'banner' : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 and information about service: ssh and port is open.</p>
------------------------------	--

4. BANNER GRABBING – NETCAT

Netcat is program used to monitor the flow of data between systems. The history of this tool started in 1995. It support TCP and UDP transfer protocols and can be compation of WireShark.

Netcat	List of information gathered
<pre>root@kali:~/Documents# nc -vn 192.168.56.101 22 (UNKNOWN) [192.168.56.101] 22 (ssh) open SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntul ^C</pre>	-vn flag in netcat is used to basic scanning of port, or port port 22 can be changed to list of ports. The result (figure35) is name of service and version of it: SSH-2.0 - openSHH_47p1 Debian Ubutnu1

Netcat	List of information gathered
<pre>root@kali:~/Documents# nc -vn 192.168.56.101 21 (UNKNOWN) [192.168.56.101] 21 (ftp) open 220 (vsFTPd 2.3.4) ^C</pre>	Figure 35 shows the basic netcat scan ip address (figure36) 192.168.56.101 and targeted port is 22. Gather information is that port 21 is open.

5. YOUR CHOICE OF INFORMATION GATHERING TOOL OR COMMAND OR SOFTWARE

1.5.1 Python

Tool	List of information gathered
<pre>root@kali:~/Documents# python ./banner_grab.py 192.168.56.101 1 65535 TCP Port 21 - 220 (vsFTPD 2.3.4) urity.txt.gpg TCP Port 22 - SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntul TCP Port 23 - 0000 00#00 TCP Port 25 - 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)</pre>	<p>It is using python repository called banner grab where with list of vulnerabilities. Python script make scanning easier for pen tester, because it do scan automatically . On figure 37 are result of scan 192.168.56.101 and port range 1 65535. It can be seen the port 22 is running Debian-8ubuntul or port 25 is metasploitable.</p>
<pre>import socket import select import sys if len(sys.argv) != 4: print "Usage - ./banner_grab.py [Target -IP] [First Port] [Last Port]" print "example - ./banner_grab.py 10.0.0.5 1 100" print "Example wi;; grab banners for TCP ports 1 through 100 on 10.0.0.5" sys.exit() ip = sys.argv[1] start = int(sys.argv[2]) end = int(sys.argv[3]) for port in range(start,end): try: bangrab = socket.socket(socket.AF_INET, socket.SOCK_STREAM) bangrab.connect((ip, port)) ready = select.select([bangrab],[],[],1) if ready[0]: print "TCP Port " + str(port) + " - " + bangrab.recv(4096) bangrab.close() except: pass sys.exit()</pre>	<p>Figure 37</p> <p>Figure 38</p>

1.5.2 Nmap

In this paragraph I will present basic Nmap's tools which are popular way to gather information.

1.5.2.1 Active port scanning

```
root@kali:~# nmap 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-02 09:06 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse D
serversity.txt.gpg
Nmap scan report for 192.168.56.105
Host is up (0.000098s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:55:8B:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Figure 39

1.5.2.2 Host discovery

-Pn (No PING) Nmap suggested this command in case of Sophos' firewall.

```
root@kali:~# nmap -Pn 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-02 09:15 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
servers
Nmap scan report for 192.168.56.105
Host is up (0.00011s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:55:8B:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Figure 40

1.5.2.3 OS detection

```
root@kali:~# nmap -O 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-02 09:08 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse D
servers
Nmap scan report for 192.168.56.105
Host is up (0.00032s latency).
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Figure 41

1.5.2.4 Application version detection

```
root@kali:~# nmap -sV 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-02 09:11 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
servers
Nmap scan report for 192.168.56.105
Host is up (0.00017s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs          2-4 (RPC #100003)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:55:8B:8F (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, .metasploit.metasploitable,
/o:linux:linux_kernel
```

Figure 42

CONCLUSION AND LIST OF REFERENCES

A lot of important information companies or person publish online. In one example using passive information gathering I was able to gather information about card number, address, company and family structure, all that information was available online, everybody can use it. Otherwise, the main work of pen tester is active information gathering, the popularity of tools like nmap can be compare to medium known actor who played in twelve movies. Free tutorial on web or YouTube are crucial in self-education process, in this way the OSINT helps pen testers to improve ways collecting information, by giving them possibility to boost their skills.

References Portfolio 1

Anon., n.d. [Online]

Available at: <https://www.fillerworld.com/password/remind>

BMW, 2018. *NFORMATION*. [Online]

Available at:

https://static.bmw.com/content/dam/bmw/staticContent/static_bmw_com/bluetooth/updates/bmw/pdf/Readme_UPD05081_en.pdf

[Accessed 21 19 2019].

Eshbach, L., nd. *www.linkedin.com*. [Online]

Available at: <https://www.linkedin.com/in/laurel-eshbach-a41885b2>

[Accessed 06 12 2019].

Keeling, N., 2018. *Thieves are 'hacking' keyless cars. These are the models at risk - and the simple thing you can do to protect yourself.* [Online].

nd, 2016. *They CC are from Checker {x-blacks.com}*. [Online]

Available at: <http://ccwithmoney.blogspot.com/>

[Accessed 25 10 2019].

nd, 2017. *hack credit card number with -cvv-2019*. [Online]

Available at: <http://hack-credit-card2019.blogspot.com/2017/11/hack-credit-card-number-with-cvv-2019.html>

[Accessed 25 October 2019].

nd, 2018. *1824 Allen Ln.* [Online]

Available at: https://www.zillow.com/homedetails/1824-Allen-Ln-Abington-PA-19001/9890608_zpid/
[Accessed 05 12 2019].

nd, 2018. *Redfin Estimate for 1824 Allen Ln.* [Online]

Available at: <https://www.redfin.com/PA/Abington/1824-Allen-Ln-19001/home/38194890>
[Accessed 05 12 2019].

nd, n.d. *Telephone Directory of*. [Online].

nd, nd. *google.com*. [Online]

Available at:

https://www.google.com/search?rlz=1C1GCEA_enGB872GB872&biw=1028&bih=1079&tbo=isch&sa=1&ei=1xuzXfx8CP6V1fAP4uud6AQ&q=Laurel+Eshbach&oq=Laurel+Eshbach&gs_l=img.3...1569.1569..2312...0.0..0.44.44.1.....0....1..gws-wiz-img.GHrUu7deWcc&ved=0ahUKEwi1xL7c47flAh

[Accessed 06 12 2019].

Wikipedia, 2018. *https://en.wikipedia.org/*. [Online]

Available at: <https://en.wikipedia.org/wiki/ConnectedDrive>

wikipedia, 2019. *Eric Corley*. [Online].

PORTFOLIO 2

TECHNICAL REPORT VULNERABILITY ASSESSMENT - INTRODUCTION

Vulnerability assessment is an important step in system penetration testing. Pen tester need to assent gathered information because it wants vulnerabilities which can be exploited at later date. Nowadays, software and hardware rapidly change in that reason, companies produce a lot of updates and add new features to their products. Otherwise, today's update for yesterday's bugs is new opportunity for hacker to break into victim's system, also it can be seemed like an endless fight because tomorrow producent will publish new updates. Updates make changes in software, if developers did not enough test new update, it would make application unstable or vulnerable. For hackers each new line of code in application, which is changed in configurations or new hardware, is other opportunity to hack security system (CVE Team , 2019).

In the other hand, people use computer devices because they like to connect the internet, in that reason the devise need to provide online services. Also, they like to have many new applications for work or entertainment. The security of users is in cyber security specialists' hands. Like a policeman, cybersecurity specialist every day wakes up and starts new battle with cybercriminals. This is one huge never-ending war between white and red hats, because each day new vulnerabilities are found. Hackers theft a lot of money, in 2017 they stale more than 172.000.000.000\$ (Condilffe, 2018). They are very motivated and well-paid and will do everything to steal more. They are buying new hardware and testing all new feature in applications, even more they are organized like international enterprises (sophos, nd). The cybersecurity specialists must start preparing for it, they need a system which provide a vulnerability assessment. Like cogwheel in machine all computers in company have to work as long as possible. They cannot being update all the time. How to set which one vulnerability is the biggest risk? During the time the security lack are not updated the hackers can use them, in that reason time for security specialist is an enemy, but hackers using hackers' community faster than cybersecurity specialist. The crucial updates should be installed firs in that reasons pen testers need system of assessment vulnerabilities and databased with vulnerability, also hackers have a dark net dataset with collections of vulnerability, and often they know vulnerabilities before pen testers. In order to this problem this essay will present the step by step process how to asset vulnerabilities.

VULNERABILITY ASSESSMENT TOOL

In this example of vulnerability assessment would be demonstrated a Nmap. Nmap or the full name is 'Network scanner', it is a free and open source network scanner created by Gordon Lyon (wikipedia, 2019; nd, Introduction, nd). Pen testers use Nmap for task as network inventory, managing services upgrade schedules, and monitoring host or service uptime. Nmap is so popular even it was used in twelve movies one of them was The Matrix Reloaded, the popularity of this tool cause large user support community (nd, Introduction, nd). An example of standard scan is "nmap -sV [target's ip address]" and If pen tester uses Kali Linux, it does not need to install Nmap because Nmap is pre-installed. Nmap is simple for new user to star it out because to run a command in terminal is just needed to write "nmap", settings and target's ip address. Nmap is command line based, otherwise there are also programmes

which add graphic user interface to nmap for example Zen map. One of the Nmap advantages is portability, because most operating system are supported, for example Linux, Microsoft Windows and Mac Os. Nmap can scan thousands of machines, in that reason it can be used to build topology of huge networks.

Nmap has a few useful features:

1. Active port scanning
2. Host discovery
3. OS detection
4. Application version detection
5. Nmap-vulners

The Nmap-vulners script extends the functionality of Nmap by connecting to the CVE database to find information about vulnerabilities on a machine from security experts and this feature makes it the best tool to for vulnerability assessment (SECURITYTRAILS TEAM, 2018).

In this report will be scan machine with ip address 195.168.56.105, results can be seen on figure 5, figure 6, figure 7, figure 8. This machine very vulnerable, what is making it easy target for hackers. This tool require form user to download git repository with data about vulnerability, the repository can be updated and using nmap-vulners needs an intent connection, but all vulnerability are updated.

Figure 5 shows result of standard nmap scanning with –script nmap-vulners of ip address: 192.168.56.101. Port 80 services apache: http_server:2.2.14 and has the most dangerous vulnerability found in this part of scan - CVE-2010-0425, it has 10 point in CVSS version 2.

Figure 6 shows result of standard nmap scanning with –script nmap-vulners of ip address: 192.168.56.102. Port 53 is a domain service and it has the most dangerous vulnerability found in this part of scan - CVE-2012-1667, it has 8.5 point in CVSS version 2. Also, important information is open port 23 telnet which is a backdoor or can be used like backdoor, it gives full control on machines everybody who would connect using this port.

Figure 7 shows result of standard nmap scanning with –script nmap-vulners of ip address: 192.168.56.102. Port 80 services apache: http_server:2.2.8 and has the most dangerous vulnerability found in this part of scan - CVE-2010-0425, it has 10 point in CVSS version 2. This vulnerability is only for windows machines, there is no metasploit in Metasploit framework on Kali Machine dedicated for this CVE on Linux machine.

Figure 8 shows result of standard nmap scanning with –script nmap-vulners of ip address: 192.168.56.102. Port 5432 services PostgreSQL and it has the most dangerous vulnerability found in this part of scan - CVE-2013-1903, it has 10 point in CVSS version 2.

VULNERABILITY VALIDATION

Common vulnerabilities and Exposures (CVE) were stared in 1999 by MITRE (Armerding, 2017). An exposure is a developer's mistake that attacker can use to access to a system or network (Tunggal, 2019). MITRE is a not-for-profit company with mission to make a world

safer, MITRE solves problems with nation's safety or well-being, and it works across the government (MITRE, nd). CVE system's goal is to make easier to share data about vulnerability, in that reason CVE provides common names, CVSS, descriptions, validation and often countermeasures of vulnerabilities for publicly known problems (CVE Team , 2019).

The Common Vulnerability Scoring System is an open framework connect with CVE, the National Vulnerability Database (NVD) provides score for almost all CVE (NVD, nd). The target of CVSS is to show how danger a vulnerability is, it contains tree metric categories: Base, Temporal, and Environmental, where the base score is ranging from 0 to 10 as shown in Figure 1 (10.0 High). The name vulnerability as build form: 'CVE', discovery year and catalogue number, it is easy to figure out an age of vulnerability.

Screenshots below presents examples of CVE vulnerabilities, it can be seen how NVE presents the vulnerability. The inscription has information about date, description and resources with useful links which are there to help administrators to secure their system.

CVE-2010-0425

CVE-2010-0425 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Source: MITRE

[+View Analysis Description](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2010-0425

NVD Published Date:

03/05/2010

NVD Last Modified:

10/30/2018

Severity

[CVSS Version 3.x](#) [CVSS Version 2.0](#)

CVSS 2.0 Severity and Metrics:



NIST: NVD

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:L/I:C/A:C)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://httpd.apache.org/security/vulnerabilities_20.html	

Figure 43

CVE-2010-4478

CVE-2010-4478 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

Source: MITRE

[View Analysis Description](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2010-4478

NVD Published Date:

12/06/2010

NVD Last Modified:

09/18/2017

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 2.0 Severity and Metrics:



NIST: NVD

Base Score: 7.5 HIGH

Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10673	
http://seb.dlzteam.org/crypto/jpake-session-key-retrieval.pdf	Exploit
http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c#rev1.5	Patch
http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/jpake.c.diff?r1=1.4;r2=1.5;f=h	Patch
https://bugzilla.redhat.com/show_bug.cgi?id=659297	Patch
https://github.com/seb-m/jpake	
https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A12338	

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-287	Improper Authentication	NIST

Known Affected Software Configurations

Switch to CPE 2.2

[Configuration 1](#) ([hide](#))

Figure 44

CVE-2019-10210

CVSS Version 2.0

CVE-2019-10210 Detail

Current Description

Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.

Source: MITRE

[View Analysis Description](#)

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 2.0 Severity and Metrics:



NIST: NVD

Base Score: 1.9 LOW

Vector: (AV:L/AC:M/Au:N/C:P/I:N/A:N)

QUICK INFO

CVE Dictionary Entry:

CVE-2019-10210

NVD Published Date:

10/29/2019

NVD Last Modified:

11/01/2019

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10210	Issue Tracking
https://www.postgresql.org/about/news/1960/	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST
CWE-377	Insecure Temporary File	Red Hat, Inc.

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1 ([hide](#))

 cpe:2.3:a:postgresql:postgresql:**:**:**:*	Up to (excluding) 9.4.24
Show Matching CPE(s) ▾	

Figure 45

CVSS Version 3.x

CVE-2019-10210 Detail

Current Description

Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.

Source: MITRE

[View Analysis Description](#)

Severity

[CVSS Version 3.x](#) [CVSS Version 2.0](#)

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 7.0 HIGH

Vector:

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H



CNA: Red Hat, Inc.

Base Score: 6.7 MEDIUM

Vector:

CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

CVE-2019-10210

NVD Published Date:

10/29/2019

NVD Last Modified:

11/01/2019

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10210	Issue Tracking
https://www.postgresql.org/about/news/1960/	Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST
CWE-377	Insecure Temporary File	Red Hat, Inc.

Figure 46

CONCLUSION PORTFOLIO 2

The vulnerability assessment is a crucial part of security management. The web administrator take care about software update and keep all security update download and installed. Paradoxical data bases like CVE and NVD help both attackers and defenders. The hackers or red team learn from that data based what vulnerability to exploit firstly. Also, blue team know on which vulnerability should focus firstly update or reconfigure a system. Only the time matter, how will be first one who will exploit or update vulnerability.

APPENDICES PORTFOLIO 2

```
root@kali:~# nmap -sV --script nmap-vulners -p 192.168.56.101 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 10:23 EST of vulnerabilities! CVSS Score 8.7
Nmap scan report for 192.168.56.101
Host is up (1.0s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu1)
. )
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
n_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
| vulners:
|   Highlight different blocks
cpe:/a:apache:http_server:2.2.14:
  CVE-2010-0425  10.0  https://vulners.com/cve/CVE-2010-0425
  CVE-2011-3192  7.8   https://vulners.com/cve/CVE-2011-3192
  CVE-2017-7679  7.5   https://vulners.com/cve/CVE-2017-7679
  CVE-2017-7668  7.5   https://vulners.com/cve/CVE-2017-7668
  CVE-2017-3169  7.5   https://vulners.com/cve/CVE-2017-3169
  CVE-2017-3167  7.5   https://vulners.com/cve/CVE-2017-3167
  CVE-2013-2249  7.5   https://vulners.com/cve/CVE-2013-2249
  CVE-2012-0883  6.9   https://vulners.com/cve/CVE-2012-0883
  CVE-2018-1312  6.8   https://vulners.com/cve/CVE-2018-1312
  CVE-2013-1862  5.1   https://vulners.com/cve/CVE-2013-1862
  CVE-2014-0231  5.0   https://vulners.com/cve/CVE-2014-0231
  CVE-2014-0098  5.0   https://vulners.com/cve/CVE-2014-0098
  CVE-2013-6438  5.0   https://vulners.com/cve/CVE-2013-6438
  CVE-2012-4557  5.0   https://vulners.com/cve/CVE-2012-4557
  CVE-2011-3368  5.0   https://vulners.com/cve/CVE-2011-3368
  CVE-2010-2068  5.0   https://vulners.com/cve/CVE-2010-2068
  CVE-2010-1452  5.0   https://vulners.com/cve/CVE-2010-1452
  CVE-2010-0408  5.0   https://vulners.com/cve/CVE-2010-0408
  CVE-2012-0031  4.6   https://vulners.com/cve/CVE-2012-0031
  CVE-2011-3607  4.4   https://vulners.com/cve/CVE-2011-3607
  CVE-2016-4975  4.3   https://vulners.com/cve/CVE-2016-4975
  CVE-2013-1896  4.3   https://vulners.com/cve/CVE-2013-1896
  CVE-2012-4558  4.3   https://vulners.com/cve/CVE-2012-4558
  CVE-2012-3499  4.3   https://vulners.com/cve/CVE-2012-3499
  CVE-2012-0053  4.3   https://vulners.com/cve/CVE-2012-0053
  CVE-2011-4317  4.3   https://vulners.com/cve/CVE-2011-4317
  CVE-2011-3639  4.3   https://vulners.com/cve/CVE-2011-3639
  CVE-2011-3348  4.3   https://vulners.com/cve/CVE-2011-3348
  CVE-2011-0419  4.3   https://vulners.com/cve/CVE-2011-0419
  CVE-2010-0434  4.3   https://vulners.com/cve/CVE-2010-0434
  CVE-2016-8612  3.3   https://vulners.com/cve/CVE-2016-8612
  CVE-2012-2687  2.6   https://vulners.com/cve/CVE-2012-2687
  CVE-2011-4415  1.2   https://vulners.com/cve/CVE-2011-4415
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap       Courier Imapd (released 2008)
443/tcp  open  ssl/https?
```

Figure 47

```

root@kali:~# nmap --script nmap-vulners -sV 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-21 12:55 EST
Nmap scan report for 192.168.56.102
Host is up (1.0s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     CVE-2010-4478  7.5      https://vulners.com/cve/CVE-2010-4478
|     CVE-2017-15906 5.0      https://vulners.com/cve/CVE-2017-15906
|     CVE-2016-10708 5.0      https://vulners.com/cve/CVE-2016-10708
|     CVE-2010-4755  4.0      https://vulners.com/cve/CVE-2010-4755
|     CVE-2008-5161  2.6      https://vulners.com/cve/CVE-2008-5161
|_ 23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
|_ vulners:
|   cpe:/a:isc:bind:9.4.2:
|     CVE-2012-1667  8.5      https://vulners.com/cve/CVE-2012-1667
|     CVE-2014-8500  7.8      https://vulners.com/cve/CVE-2014-8500
|     CVE-2012-5166  7.8      https://vulners.com/cve/CVE-2012-5166
|     CVE-2012-4244  7.8      https://vulners.com/cve/CVE-2012-4244
|     CVE-2012-3817  7.8      https://vulners.com/cve/CVE-2012-3817
|     CVE-2008-4163  7.8      https://vulners.com/cve/CVE-2008-4163
|     CVE-2010-0382  7.6      https://vulners.com/cve/CVE-2010-0382
|     CVE-2017-3141  7.2      https://vulners.com/cve/CVE-2017-3141
|     CVE-2015-8461  7.1      https://vulners.com/cve/CVE-2015-8461
|     CVE-2015-8704  6.8      https://vulners.com/cve/CVE-2015-8704
|     CVE-2009-0025  6.8      https://vulners.com/cve/CVE-2009-0025
|     CVE-2015-8705  6.6      https://vulners.com/cve/CVE-2015-8705
|     CVE-2010-3614  6.4      https://vulners.com/cve/CVE-2010-3614
|     CVE-2017-3145  5.0      https://vulners.com/cve/CVE-2017-3145
|     CVE-2016-9444  5.0      https://vulners.com/cve/CVE-2016-9444
|     CVE-2016-9131  5.0      https://vulners.com/cve/CVE-2016-9131
|     CVE-2016-8864  5.0      https://vulners.com/cve/CVE-2016-8864
|     CVE-2016-2848  5.0      https://vulners.com/cve/CVE-2016-2848
|     CVE-2016-1286  5.0      https://vulners.com/cve/CVE-2016-1286
|     CVE-2015-8000  5.0      https://vulners.com/cve/CVE-2015-8000
|     CVE-2012-1033  5.0      https://vulners.com/cve/CVE-2012-1033
|     CVE-2011-4313  5.0      https://vulners.com/cve/CVE-2011-4313
|     CVE-2011-1910  5.0      https://vulners.com/cve/CVE-2011-1910
|     CVE-2009-0265  5.0      https://vulners.com/cve/CVE-2009-0265
|     CVE-2017-3143  4.3      https://vulners.com/cve/CVE-2017-3143
|     CVE-2017-3142  4.3      https://vulners.com/cve/CVE-2017-3142
|     CVE-2016-2775  4.3      https://vulners.com/cve/CVE-2016-2775
|     CVE-2016-1285  4.3      https://vulners.com/cve/CVE-2016-1285
|     CVE-2010-0097  4.3      https://vulners.com/cve/CVE-2010-0097
|     CVE-2009-0696  4.3      https://vulners.com/cve/CVE-2009-0696
|     CVE-2018-5741  4.0      https://vulners.com/cve/CVE-2018-5741
|     CVE-2016-6170  4.0      https://vulners.com/cve/CVE-2016-6170
|     CVE-2010-0290  4.0      https://vulners.com/cve/CVE-2010-0290
|     CVE-2009-4022  2.6      https://vulners.com/cve/CVE-2009-4022

```

Figure 48

```

80/tcp open http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
vulnerbs:
cpe:/a:apache:http_server:2.2.8:
  CVE-2010-0425  10.0  https://vulners.com/cve/CVE-2010-0425
  CVE-2011-3192  7.8   https://vulners.com/cve/CVE-2011-3192
  CVE-2017-7679  7.5   https://vulners.com/cve/CVE-2017-7679
  CVE-2013-2249  7.5   https://vulners.com/cve/CVE-2013-2249
  CVE-2009-1891  7.1   https://vulners.com/cve/CVE-2009-1891
  CVE-2009-1890  7.1   https://vulners.com/cve/CVE-2009-1890
  CVE-2012-0883  6.9   https://vulners.com/cve/CVE-2012-0883
  CVE-2018-1312  6.8   https://vulners.com/cve/CVE-2018-1312
  CVE-2013-1862  5.1   https://vulners.com/cve/CVE-2013-1862
  CVE-2014-0231  5.0   https://vulners.com/cve/CVE-2014-0231
  CVE-2014-0098  5.0   https://vulners.com/cve/CVE-2014-0098
  CVE-2013-6438  5.0   https://vulners.com/cve/CVE-2013-6438
  CVE-2011-3368  5.0   https://vulners.com/cve/CVE-2011-3368
  CVE-2010-1452  5.0   https://vulners.com/cve/CVE-2010-1452
  CVE-2010-0408  5.0   https://vulners.com/cve/CVE-2010-0408
  CVE-2009-2699  5.0   https://vulners.com/cve/CVE-2009-2699
  CVE-2008-2364  5.0   https://vulners.com/cve/CVE-2008-2364
  CVE-2007-6750  5.0   https://vulners.com/cve/CVE-2007-6750
  CVE-2009-1195  4.9   https://vulners.com/cve/CVE-2009-1195
  CVE-2012-0031  4.6   https://vulners.com/cve/CVE-2012-0031
  CVE-2011-3607  4.4   https://vulners.com/cve/CVE-2011-3607
  CVE-2016-4975  4.3   https://vulners.com/cve/CVE-2016-4975
  CVE-2013-1896  4.3   https://vulners.com/cve/CVE-2013-1896
  CVE-2012-4558  4.3   https://vulners.com/cve/CVE-2012-4558
  CVE-2012-3499  4.3   https://vulners.com/cve/CVE-2012-3499
  CVE-2012-0053  4.3   https://vulners.com/cve/CVE-2012-0053
  CVE-2011-4317  4.3   https://vulners.com/cve/CVE-2011-4317
  CVE-2011-3639  4.3   https://vulners.com/cve/CVE-2011-3639
  CVE-2011-3348  4.3   https://vulners.com/cve/CVE-2011-3348
  CVE-2011-0419  4.3   https://vulners.com/cve/CVE-2011-0419
  CVE-2010-0434  4.3   https://vulners.com/cve/CVE-2010-0434
  CVE-2008-2939  4.3   https://vulners.com/cve/CVE-2008-2939
  CVE-2016-8612  3.3   https://vulners.com/cve/CVE-2016-8612
  CVE-2012-2687  2.6   https://vulners.com/cve/CVE-2012-2687
  CVE-2011-4415  1.2   https://vulners.com/cve/CVE-2011-4415
111/tcp open rpcbind  2 (RPC #100000)
|_rpcinfo:
    program version  port/proto  service
    100000  2          111/tcp    rpcbind
    100000  2          111/udp    rpcbind
    100003  2,3,4      2049/tcp   nfs
    100003  2,3,4      2049/udp   nfs
    100005  1,2,3      41274/tcp  mountd
    100005  1,2,3      42222/udp mountd
    100021  1,3,4      49886/tcp  nlockmgr
    100021  1,3,4      55182/udp  nlockmgr
    100024  1          36910/udp  status
    100024  1          52510/tcp   status
|_vulnerbs: ERROR: Script execution failed (use -d to debug)

```

Figure 49

```

111/tcp open rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version port/proto  service
|     100000  2          111/tcp   rpcbind
|     100000  2          111/udp   rpcbind
|     100003  2,3,4     2049/tcp   nfs
|     100003  2,3,4     2049/udp   nfs
|     100005  1,2,3     41274/tcp  mountd
|     100005  1,2,3     42222/udp  mountd
|     100021  1,3,4     49886/tcp  nlockmgr
|     100021  1,3,4     55182/udp  nlockmgr
|     100024  1          36910/udp  status
|     100024  1          52510/tcp  status
|_vulners: ERROR: Script execution failed (use -d to debug)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec       netkit-rsh rexecd
513/tcp open login?
514/tcp open shell      Netkit rshd
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open bindshell  Bash shell (**BACKDOOR**; root shell)
2049/tcp open nfs       2-4 (RPC #100003)
|_vulners: ERROR: Script execution failed (use -d to debug)
3306/tcp open mysql     MySQL 5.0.51a-3ubuntu5
| vulners:
|   MySQL 5.0.51a-3ubuntu5:
|     NODEJS:602      0.0      https://vulners.com/nodejs/NODEJS:602
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| vulners:
|   cpe:/a:postgresql:postgresql:8.3:
|     CVE-2013-1903    10.0    https://vulners.com/cve/CVE-2013-1903
|     CVE-2013-1902    10.0    https://vulners.com/cve/CVE-2013-1902
|     CVE-2016-7048    9.3     https://vulners.com/cve/CVE-2016-7048
|     CVE-2010-1447    8.5     https://vulners.com/cve/CVE-2010-1447
|     CVE-2010-1169    8.5     https://vulners.com/cve/CVE-2010-1169
|     CVE-2019-10211   7.5     https://vulners.com/cve/CVE-2019-10211
|     CVE-2017-14798   6.9     https://vulners.com/cve/CVE-2017-14798
|     CVE-2013-0255   6.8     https://vulners.com/cve/CVE-2013-0255
|     CVE-2012-0868   6.8     https://vulners.com/cve/CVE-2012-0868
|     CVE-2009-3231   6.8     https://vulners.com/cve/CVE-2009-3231
|     CVE-2012-0866   6.5     https://vulners.com/cve/CVE-2012-0866
|     CVE-2010-4015   6.5     https://vulners.com/cve/CVE-2010-4015
|     CVE-2018-1115   6.4     https://vulners.com/cve/CVE-2018-1115
|     CVE-2010-3433   6.0     https://vulners.com/cve/CVE-2010-3433
|     CVE-2010-1170   6.0     https://vulners.com/cve/CVE-2010-1170
|     CVE-2010-1975   5.5     https://vulners.com/cve/CVE-2010-1975
|     CVE-2012-3488   4.9     https://vulners.com/cve/CVE-2012-3488
|     CVE-2012-2143   4.3     https://vulners.com/cve/CVE-2012-2143
|     CVE-2012-3489   4.0     https://vulners.com/cve/CVE-2012-3489
|     CVE-2012-2655   4.0     https://vulners.com/cve/CVE-2012-2655
|     CVE-2009-3229   4.0     https://vulners.com/cve/CVE-2009-3229
|     CVE-2010-0733   3.5     https://vulners.com/cve/CVE-2010-0733
|     CVE-2019-10210  1.9     https://vulners.com/cve/CVE-2019-10210

```

Figure 50

```

5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, localhost, .metasploitable.metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 47.47 seconds

```

Figure 51

CVE-ID
CVE-2013-1903 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description
PostgreSQL, possibly 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 incorrectly provides the superuser password to scripts related to "graphical installers for Linux and Mac OS X," which has unspecified impact and attack vectors.
References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.
<ul style="list-style-type: none"> • CONFIRM:http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html • CONFIRM:http://www.postgresql.org/about/news/1456/ • CONFIRM:http://www.postgresql.org/support/security/
Assigning CNA
Red Hat, Inc.
Date Entry Created
20130219 <small>Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.</small>
Phase (Legacy)
Assigned (20130219)
Votes (Legacy)
Comments (Legacy)
Proposed (Legacy)
N/A
This is an entry on the CVE List , which provides common identifiers for publicly known cybersecurity vulnerabilities.
SEARCH CVE USING KEYWORDS: <input type="text"/> <input type="button" value="Submit"/>
You can also search by reference using the CVE Reference Maps .
For More Information: CVE Request Web Form (select "Other" from dropdown)

Figure 52

REFERENCES

- Condiffe, J., 2018. *Hackers stole \$172 billion from people in 2017*. [Online] Available at: <https://www.technologyreview.com/f/610043/hackers-stole-172-billion-from-people-in-2017/> [Accessed 22 11 2019].
- CVE Team , 2019. *Frequently Asked Questions*. [Online] Available at: https://cve.mitre.org/about/faqs.html#what_is_cve [Accessed 22 11 2019].
- nd, nd. *Introduction*. [Online] Available at: <https://nmap.org/> [Accessed 7 12 2019].
- SECURITYTRAILS TEAM, 2018. *Top 5 Best Port Scanners*. [Online] Available at: <https://securitytrails.com/blog/best-port-scanners> [Accessed 07 12 2019].
- sophos, nd. *When Malware Goes Mobile*. [Online] Available at: <https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx> [Accessed 7 12 2019].
- Tunggal, A. T., 2019. *What is CVE? Common Vulnerabilities and Exposures Explained*. [Online] Available at: <https://www.upguard.com/blog/cve> [Accessed 7 12 2019].
- wikipedia, 2019. *Nmap*. [Online] Available at: <https://en.wikipedia.org/wiki/Nmap> [Accessed 07 12 2019].

BIBLIOGRAPHY

<http://www.sussex.ac.uk/ei/internal/forstudents/engineeringdesign/studyguides/techreportwriting#1>

<https://ebookcentral.proquest.com/lib/edgehill/reader.action?docID=952079&query=>

<https://nostarch.com/metasploit>

<https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html>

<https://ieeexplore.ieee.org/abstract/document/4275642>

<https://nmap.org/book/osdetect-usage.html>

https://cve.mitre.org/about/faqs.html#what_is_cve

PORTFOLIO 3

This report focusses on applying the penetration testing framework to a virtual real-world environment and how a Penetration test can be carried out successfully. Revealing vulnerabilities can help to ensure that a network can be as secure as possible from many hackers.

The Penetration Testing Framework consists of seven phases:

1. Information Discovery – Various sources will be used by the pentester to gather vital information about a corporation, network or website. Most information found is publicly available, this is known as open-source intelligence, other information could include information regarding the systems which have been provided by enterprises.

Web crawlers are used for an automated gathering of information on the internet, and this can provide information regarding the targets without the need of querying enterprise employees.

2. Target Scanning – This can require the pentester to send probes out to the network targeted, this can collect preliminary information which can be used to allow the probe to further gain input for extra information. Other forms of target scanning include searching ports, services, operating systems and IP addresses on a network using various tools such as Nmap and OpenVAS.
3. Vulnerability Assessment – The outcome of vulnerability assessments usually come in a form of CVE codes with severity scores to accompany it. These codes allow a pentester to understand what vulnerabilities are on the network and how to possibly exploit them and or fix them. Examples of vulnerabilities that can be identified include remote-code execution, XSS, SQL injection and HeartBleed.
4. Exploiting Weakness – As per the previous phase, once vulnerabilities are discovered, they can be exploited however not all of them can be so easy, there might be a firewall in place, or other aspects that remain outside the scope of the penetration test. Vulnerabilities which are focused on the most are once which can be exploited to gain access to a target system.
5. Privilege Escalation – A pentester, for a penetration test to be completed, needs to be able to exploit the system to gain higher privileges, this can be in form of gaining access as a standard user to gaining administrative rights. This can help a pentester to gain confidential information, deploy malware and to run commands which only admins could run. This can cause serious damage to a network (Banach, 2019).
6. Retaining Access – Retaining access can allow a pentester to keep access to a system or network even after it has been reset, modified or rebooted.
7. Covering Tracks – Within this final phase, a pentester will clear all changes made within the system compromised, whilst doing this, they will return the previously compromised systems to their original configurations before penetration testing took place (Narwal & Gupta, 2015).

Phases 1-4 and 6 (RedLegg, 2019).

This report as mentioned previously shall go into detail with a demonstration of how a penetration test is conducted with examples. These examples follow the case study scenario within the appendix where the pentester is “The HackBay Pvt Ltd” and the network which is being tested is the “The Happy Shop Inc”. The “Happy Shop” networks consist of a Database server, Web server, Windows 7 machine, and a Windows XP machine, the software suite within KaliLinux will be used to carry out the penetration test.

PREPARATION PHASE

XSS

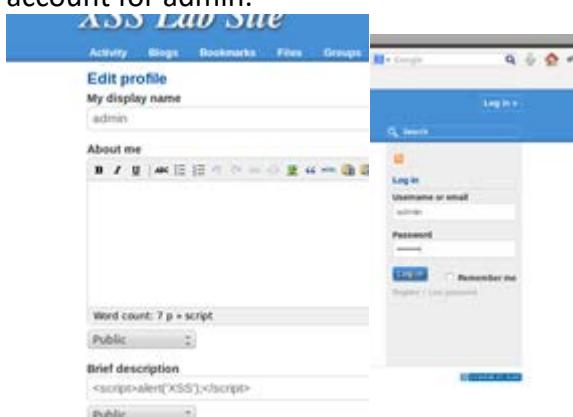
XSS stands for Cross-Site Scripting and is known to be one of the top exploits used in many modern web applications. According to Gupta & Gupta (2017), XSS attacks allow for an attacker to execute malicious scripts on the victim's web browser, this can lead to compromises in data integrity, the loss of cookies, passwords and credit card details amongst other crucial private and confidential information. To further back up the statement that XSS is one of the top exploits, Rodríguez, Torres, Flores & Benavides (2019) analyse the results of the 2018 Cisco Security Report noting that all web applications which have been analysed have at least one attack with XSS making up 40% of all attack attempts.

According to Ruiz (2019), the main vulnerability that can be exploited with XSS would be full control over browsers which is one of the most important pieces of computer software. Typically, as mentioned before, the malicious scripts may contain HTML and JavaScript, they may even manipulate the DOM-node. One last vulnerability that comes from the attack includes the use of downloads including trojans and keyloggers being download on the client-side machine (Ruiz, 2019).

The screenshots below illustrate a typical XSS scenario.



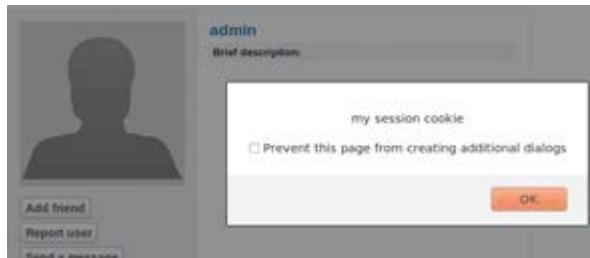
The first screenshot shows the webserver being booted, this webserver hosts www.xsslablegg.com which is a social media web application. There are multiple user accounts on this network which can be exploited. The example used in this scenario is the account for admin.



With the screenshot above, a malicious script has been entered in the place of the "brief description" for the user, this could also be entered into the "about me" section with the same outcome. What the script aims to do is create a pop-up box for when a user clicks on the admin account. The pop-up box is known as an alert. This is shown in the screenshot below:



The two screenshots below demonstrate a script which displays cookies to a user who may be viewing the admin account.



The screenshot shows the "Edit profile" page for the "admin" user on the "XSS Lab Site".

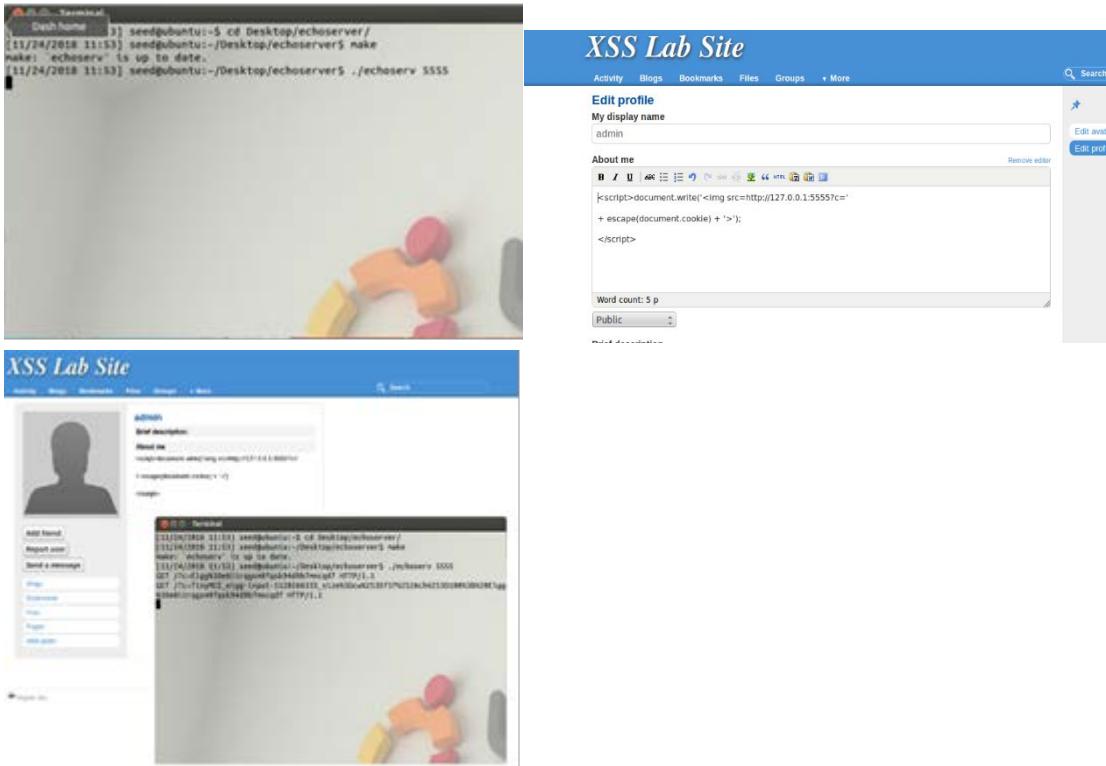
- My display name:** admin
- About me:** (Contains the following script)

```
<script>
alert(document.cookie);
alert('my session cookie');
</script>
```
- Brief description:** <><script>alert('XSS')</script>

The script demonstrates how cookies are stolen. Previously, users could see their cookies however the attacker could not.

For cookies to become visible to the attacker, an HTTP request to the server is required. The hacker's port number is 5555, this is being listened to by a TCP server. An HTTP GET request is then initiated. An HTTP GET request allows a client to “get” a piece of information from an HTTP server (Singh, 2017).

The TCP server being used is the echoserver which allows for a client and a server to connect, this is shown in the second screenshot. Once configured the cookies are displayed as shown in the third screenshot.



According to Ruiz (2019), a countermeasure which proves quite effective would be the use of a firewall such as “Sucuri”, this firewall is specially designed to mitigate XSS attacks. Methods that work well alongside this countermeasure includes escaping untrusted HTTP requests based on the HTML output, context-sensitive encoding being modified to fight against DOM XSS attacks as well as enabling the Content Security Policy, this method is best used if no other vulnerabilities exist in relation to use of malicious code. Further countermeasures may include integrity checks of digital signatures on serialized objects as well as isolating running code in low privileged environments (Ruiz, 2019).

Huang et al (2017) states that XSS countermeasures fall into three different categories, the first being secure implementation, then defence mechanism deployment and lastly penetration testing. With secure implementation, input validation and sanitization and proper use of a content security policy being enforced. This could stop XSS content from being stored. The XSS penetration test countermeasure involves white-hat testing which can help developers to locate system vulnerabilities (Huang et al, 2017).

SQL INJECTION

SQL injection involves injection of code where an SQL query is used for malicious purposes. SQL injections allow for attackers to gain unauthorised access to databases and can exploit any weaknesses within them to uncover sensitive information. Sensitive information includes confidential information which can lead to fraud (Halfond et al, 2006).

SQL injections are most lethal when a weak input validation technique has been placed on the database, the input validation technique would aim to filter database input so that certain queries cannot be used to cause an injection of malicious code. The most dangerous SQL injection would be when an attacker has the same privileges as an administrator by going through the victim's back end system. This can lead to disastrous SQL injections. (Atoum & Qaralleh, 2014).

Page Break

Below is an example of SQL injection:

1. Guessing the email and password does not work, the log shows that no user was found with the matching credentials.

The diagram illustrates a SQL injection attack on a bank's login application. On the left, a text box contains instructions: "Go ahead and try logging in with the following credentials:" followed by "Email user@email.com" and "Password password". An arrow points from this text box to a login form on the right. The login form has fields for "Email" containing "user@email.com" and "Password" containing "password". A green "Log in" button is to the right of the password field. Below the form, the text "Trust us with your money" and "Our website is totally secure and almost never gets hacked." is displayed. On the far left, a "LOGS" section shows the log entry "Rendering login page.".

APPLICATION

Okay, so guessing the password didn't work. Let's try adding a quote character after the password:

Email user@email.com
Password password'

Unknown email or password.

user@email.com Enter your password **Log in**

Trust us with your money
Our website is totally secure and almost never gets hacked.

LOGS

```
Rendering login page.
Checking supplied authentication details for user@email.com.
Finding user in database.
No such user, report this to the user (invalid credentials?).
Rendering login page.
```

2. Same email is used but SQL syntax has been entered into the password box. The password entered this time is “password”. This determines whether the password box allows special characters. The results below show that special characters are not acceptable.

The second screenshot below, showcases that the query had been terminated early, this showcases that the application is vulnerable to SQL injections.

APPLICATION

Hmmm. The application crashed with an unexpected error. What could that mean? →

BANK

An unexpected error occurred.

user.email.com Enter your password **Log in**

Trust us with your money
Our website is totally secure and almost never gets hacked.

LOGS

```
Rendering login page.
Checking supplied authentication details for user.email.com.
Finding user in database.
An error occurred: PG::SyntaxError: ERROR: unterminated quoted string at or near "'password'" limit 1" LINE 1: ...ers where email =
'user.email.com' and password = 'password'... ^ : select * from users where email = 'user.email.com' and password = 'password' limit 1.
Unable to login this user due to unexpected error.
Rendering login page.
```

CODE

```
SELECT *
  FROM users
 WHERE email = 'user.email.com'
   AND pass  = 'password' LIMIT 1
```

Entering in ' or 1=1—allowed for unauthorised access to the bank account using SQL injection.

The screenshot shows a web application interface for a bank. On the left, a message box says: "And we are in! We successfully gained access to the application without having to guess the password, using SQL INJECTION." The main page title is "BANK". On the right, there is a "Log out" link. Below the title, it says "Bank Accounts". A table shows account details:

Account	Available Balance	Present Balance
Checking	\$16,100.44	\$16,100.44
Savings	\$50,895.96	\$50,895.96

A green button labeled "Transfer Funds!" is visible. At the bottom, there are two panels: "LOGS" and "CODE". The "LOGS" panel shows the following log entries:

```

users where email = 'user.email.com' and password = '' limit 1.
Unable to login this user due to unexpected error.
Rendering login page.
Checking supplied authentication details for user.email.com.
Finding user in database.
Authentication details confirmed, establishing session for this
user.

```

The "CODE" panel shows the SQL query used for the exploit:

```

SELECT *
FROM users
WHERE email = 'user.email.com'
AND pass = '' OR 1=1-- LIMIT 1

```

According to Ruiz (2018), preventing SQL injection code depends on the technology used behind the website. An example of this would be the use of WordPress, SQL injection can be avoided by keeping the number of plugins and themes used to a minimum. Ruiz (2018) goes on to discuss the OWASP's technical recommendations which can help to prevent SQL injections, the first being that API's need to be chosen carefully so that any use of the interpreter can be avoided. The next countermeasure which is discussed would be to whitelist server-side input validation which limits input however it is not perfect being that some applications use special characters which could bypass this. Using Limit and other SQL controls within written queries can help to prevent disclosure of records on a database.

HEARTBLEED

Within the OpenSSL cryptographic software library, there is a vulnerability known as the Heartbleed bug. This allows for information which is protected to be stolen, the information could be encrypted by either SSL or TLS. Vulnerable versions of the OpenSSL software can have the memory of their system read by any capable internet user. A compromised component would be secret keys which encrypt network traffic and keeps service providers identities hidden. Other very important vulnerabilities exploited include names and passwords of users who are on the network. What this allows attackers to do is to monitor the various network communications and steal data directly from the services discovered (Heartbleed.com, 2014).

According to Banks (2015), computer servers are quite like a human body in that OpenSSL has a heartbeat. When two servers talk to each other the encryption acts as a heart, each beat communicates connectivity and validation.

The vulnerability code for Heartbleed is **CVE-2014-0160** as can be seen on screen shot below the NVE inform about that attacker can use leak of memory to steal cryptographic keys and passwords.

CVE-2014-0160 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Source: MITRE

[+View Analysis Description](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2014-0160

NVD Published Date:

04/07/2014

NVD Last Modified:

10/09/2019

Severity

[CVSS Version 3.x](#) [CVSS Version 2.0](#)

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **7.5 HIGH**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Evaluator Impact

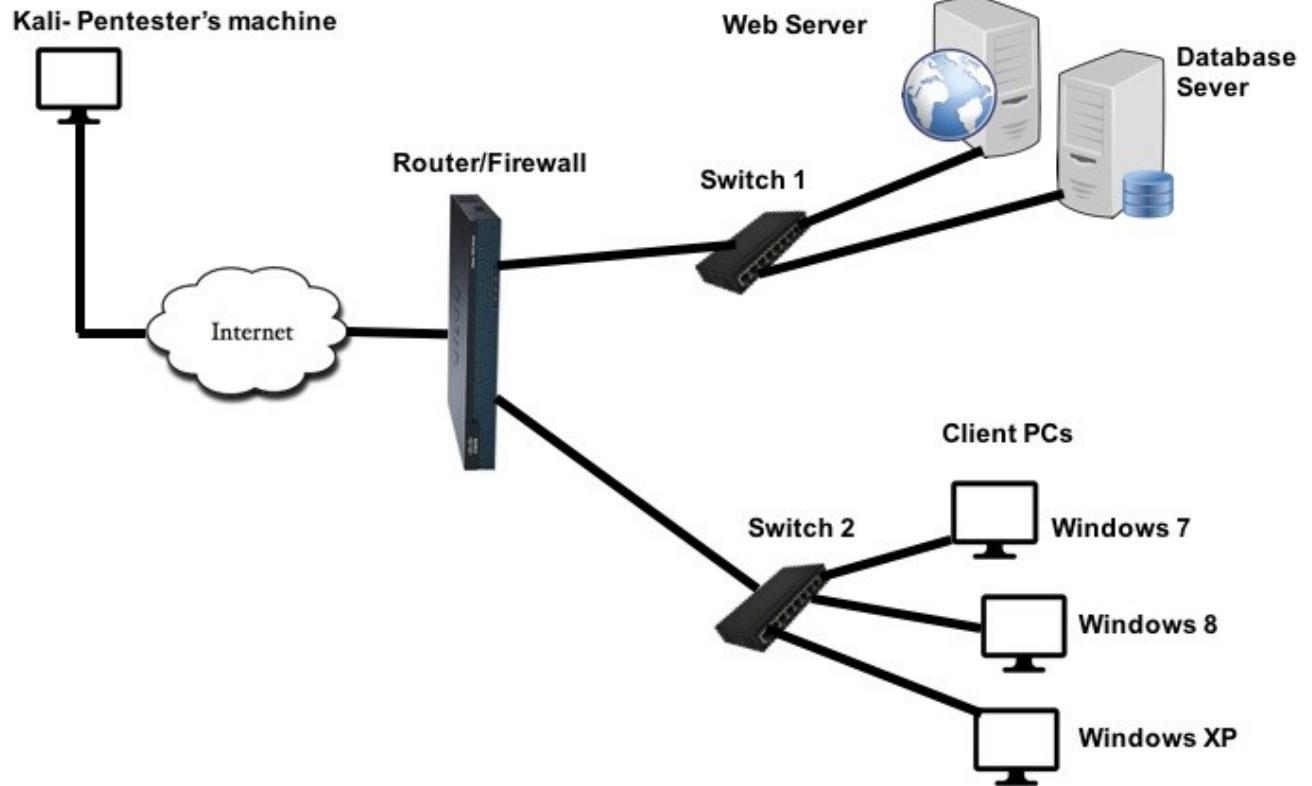
CVSS V2 scoring evaluates the impact of the vulnerability on the host where the vulnerability is located. When evaluating the impact of this vulnerability to your organization, take into account the nature of the data that is being protected and act according to your organization's risk acceptance. While CVE-2014-0160 does not allow unrestricted access to memory on the targeted host, a successful exploit does leak information from memory locations which have the potential to contain particularly sensitive information, e.g., cryptographic keys and passwords. Theft of this information could enable other attacks on the information system, the impact of which would depend on the sensitivity of the data and functions of that system.

There is a limitation of Heartbleed which limits attackers to request 64-kilobyte chunks of memory through a single “heartbeat” however there is no limit to how many attacks can be carried out. For example, the attacker may send out multiple heartbeats aka they try to reconnect or maintain an active TLS connection to gain enough memory content until the satisfactory amount of secrets are revealed (Heartbleed.com, 2014).

Heartbleed could have been avoided by validating message length and ignoring all Heartbeat requests as they come through, these requests ask for more data than what payloads require (Gajawada, 2016). According to Fruhlinger (2017), the easiest fix for preventing Heartbleed is for servers to have the latest version of OpenSSL which has fixes within the code.

PEN TESTING PHASE AND RECOMMENDATION PHASE

Happy Shop Inc – Network diagram



STEP 1: BUILD THE HAPPY SHOP NETWORK ON VIRTUAL BOX AND GATHER BASIC INFORMATION

File Machine Help

Tools

New Settings Discard Show

General

Name: JS-KALI
Operating System: Ubuntu (64-bit)
Settings File Location: C:\Users\24325457\VirtualBox VMs\JS-KALI

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE

Virtual Box Set Up

Portfolio 3 required a computer network to be built, this very network represents HappyShop online. The Virtual Box has features which help users to set up a computer network using only one computer for testing purposes. This virtual network contains two servers “Js-metasploitable” which is the Database server (metasploitable Linux 2.6.9 – 2.6.33) and “web_server” (Ubuntu) which is the web server. Also, it contains two Windows machine, the first one being Js-windows7 (Windows 7) and Js-WINDOWSXP (Windows XP). To scan a network and finding vulnerabilities another virtual machine was set up, this machine is JS-KALI which uses Kali Linux.

STEP 2: TARGET SCANNING/PROBING

Machine	IP Address	MAC Address	Open Ports
Web Server	192.168.56.101	08:00:27:ef:6f:9a	22, 80, 139, 143
Database Server	192.168.56.105	08:00:27:66:8b:8f	21, 22, 23, 25, 53, 80, 111, 139, 3306
Windows 7	192.168.56.103	08:00:27:6e:63:dd	135, 139, 445
Windows XP	192.168.56.104	08:00:27:bo:e2:0f	135, 139, 445

Netdiscover -i eth0

The “netdiscover” command lists all IP addresses and MAC Addresses that are connected to the network, this is how we got the results shown in the table above, however, this command does not list all the ports found on each machine, the command for that information would be the “nmap -sV” command as shown below.

Figure 1

```
Currently scanning: 192.168.0/16 | Screen View: Unique Hosts  
6 Captured ARP Req/Rep packets, from 6 hosts. Total size: 360
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
<hr/>				
192.168.56.1	0a:00:27:00:00:05	1	60	Unknown vendor
192.168.56.100	08:00:27:14:e3:35	1	60	PCS Systemtechnik GmbH
192.168.56.101	08:00:27:ef:6f:9a	1	60	PCS Systemtechnik GmbH
192.168.56.103	08:00:27:6e:63:dd	1	60	PCS Systemtechnik GmbH
192.168.56.104	08:00:27:b0:e2:0f	1	60	PCS Systemtechnik GmbH
192.168.56.105	08:00:27:55:8b:8f	1	60	PCS Systemtechnik GmbH

Nmap -sV (IP Address)

As seen in the screenshots below, the “nmap -sV” command lists all the ports on the selected IP address, it even gives the generalised version of each service used on each port. It is useful for finding all ports on the IP address as well as finding out which ports are open.

Figure 2

```
root@kali:~# nmap -sV 192.168.56.103  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:33 EST  
Nmap scan report for 192.168.56.103  
Host is up (1.3s latency).  
Not shown: 990 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-  
P)  
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/U  
49152/tcp  open  msrpc        Microsoft Windows RPC  
49153/tcp  open  msrpc        Microsoft Windows RPC  
49154/tcp  open  msrpc        Microsoft Windows RPC  
49155/tcp  open  msrpc        Microsoft Windows RPC  
49156/tcp  open  msrpc        Microsoft Windows RPC  
49157/tcp  open  msrpc        Microsoft Windows RPC  
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:  
  
Service detection performed. Please report any incorrect results  
bmit/.  
Nmap done: 1 IP address (1 host up) scanned in 66.53 seconds
```

Figure 3

```
root@kali:~# nmap -sV 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:31 EST
Nmap scan report for 192.168.56.101
Host is up (1.1s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14
           OpenSSL...)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/https?
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-rmi    Java RMI
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5001-TCP:V=7.70%I=7%D=11/29%Time=5DE15617%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4,"\\xac\\xed\\0\\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 4

```
root@kali:~# nmap -sV 192.168.56.104
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:34 EST
Nmap scan report for 192.168.56.104
Host is up (1.1s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:win
:windows_xp

Service detection performed. Please report any incorrect results
bmit/ .

Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
```

Figure 5

```
Nmap scan report for 192.168.56.105
Host is up (1.1s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs          2-4 (RPC #100003)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
3180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, localhost, .metasploitable, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

STEP 3: OPERATING SYSTEM DETECTION AND BANNER GRABBING

Machine	Operating System	Names of services	Versions of Service
Web Server	Linux 2.6.17 – 2.6.36	ssh, http, netbios-ssn, imap	OpenSSH 5.3p1 (Ubuntu Linux; protocol 2.0), Apache httpd 2.2.14, Samba smbd 3.X – 4.X, Courier Imapd (2008)
Database Server	Linux 2.6.9 – 2.6.33	ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, mysql	vsftpd 2.3.4, OpenSSH 4.7p1, Linux telnetd, Postfix smpd, ISC BIND 9.4.2, Apache httpd 2.2.8, 2, Samba smbd 3.X – 4.X, MySQL 5.0.51a

Nmap -O (IP Address)

This command brings back the version of the operating system which each machine linked to each IP address runs on. For example, when used with the IP address 192.168.56.101, the version brought back by the web server is Linux 2.6.X with a range of 2.6.17 – 2.6.36 which shows that the command is not the most accurate. The use of this command is useful for checking if an operating system is out of date which could lead to further vulnerabilities.

Figure 6

```
root@kali:~# nmap -O 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 08:46 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
Nmap scan report for 192.168.56.101
Host is up (0.00035s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  commplex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
MAC Address: 08:00:27:EF:6F:9A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Network Distance: 1 hop
```

Figure 7

```
root@kali:~# nmap -O 192.168.56.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:52 EST
Nmap scan report for 192.168.56.103
Host is up (0.067s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (94%), Cisco embedded (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:cisco:css_11501
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (94%), Cisco CSS11501 switch (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org
.
Nmap done: 1 IP address (1 host up) scanned in 19.71 seconds
```

No Bluetooth Found

Figure 8

```
root@kali:~# nmap -O 192.168.56.104
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 08:47 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
Nmap scan report for 192.168.56.104
Host is up (0.00054s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 08:00:27:B0:E2:0F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
```

Nmap -sV -sT (IP Address)

Using this command brought back the services and service versions. Using this command allows for a clear understanding of whether there are any outdated versions of services, with this, there might be possible vulnerabilities that could be exploited that newer versions have fixed. The “-sT” portion of the command specifies for ports with TCP to be scanned for services.

Figure 9

```
root@kali:~# nmap -sV -sT 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:38 EST
Nmap scan report for 192.168.56.101
Host is up (1.0s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.6.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.6.5 OpenSSL/1.0.2f-fips)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Courier Imapd (released 2008)
443/tcp   open  ssl/https?
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp  open  java-rmi    Java RMI
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http         Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/version
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-se
SF-Port5001-TCP:V=7.70%I=7%D=11/29%Time=5DE1581E%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4,"\\xac\\xed\\0\\x05");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.64 seconds
```

Figure 10

```
root@kali:~# nmap -sV -sT 192.168.56.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:42 EST
Nmap scan report for 192.168.56.103
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.45 seconds
```

Figure 11

```
root@kali:~# nmap -sV -sT 192.168.56.104
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 12:46 EST
Nmap scan report for 192.168.56.104
Host is up (1.0s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Service
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:
:windows_xp

Service detection performed. Please report any incorrect results at https://nma
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.76 seconds
```

Figure 12

```
Nmap scan report for 192.168.56.105
Host is up (1.0s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smt
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs          2-4 (RPC #100003)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, localhost, .metasploit.metasploitable, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

STEP 4: VULNERABILITY ASSESSMENT

Machine	Vulnerability	Brief Description
Web Server	CVE-2010-0425 CVE-2017-7679 CVE-2015-1452 CVE-2012-0031 CVE-2011-4415	<p>CVE-2010-0425 modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned call-back pointers." (Nvd.nist.gov, 2019).</p> <p>This score under version 2 is 10 however with version 3 there is no score assigned, this could be due to the age of the CVE code, with version 3 being too new for any valuable data.</p> <p>CVE-2017-7679 In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header (Nvd.nist.gov, 2019).</p> <p>This CVE scores 9.8 and 7.5 depending on the version of apache version 3 or above is 9.8 and version 2 is 7.5.</p> <p>CVE-2015-1452 The Control and Provisioning of Wireless Access Points (CAPWAP) daemon in Fortinet FortiOS 5.0 Patch 7 build 4457 allows remote attackers to cause a denial of service (locked CAPWAP Access Controller) via many ClientHello DTLS messages. This CVE only has one score at this moment in time but has been identified across two versions however only one version has a score (Nvd.nist.gov, 2019).</p> <p>The version that has current score of 7.8 is version 2. Version 3 does not have a score assigned to it.</p> <p>CVE-2012-0031</p>

		<p>scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function (Nvd.nist.gov, 2019).</p> <p>This CVE has score 4.6 on version 2 for version three there is no score applied.</p> <p>CVE-2011-4415</p> <p>The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607 (Nvd.nist.gov, 2019).</p> <p>The score of this on version 2 is 1.2 version 3 has no score assigned.</p>
Database Server	CVE-2012-1667 CVE-2008-4163 CVE-2016-1286 CVE-2016-1285 CVE-2010-0290	<p>CVE-2012-1667</p> <p>ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 8.5 version 2 for version 3 has no score applied to it.</p> <p>CVE-2008-4163</p> <p>Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via</p>

		<p>unknown vectors. (Nvd.nist.gov, 2019). This CVE has a score of 7.8 version 2 for version 3 has no score applied to it.</p> <p>CVE-2016-1286</p> <p>named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c. (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 5.0 version 2 for version 3 has a score 7.8 applied to it.</p> <p>CVE-2016-1285</p> <p>named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c. (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 4.3 version 2 for version 3 has a score 6.8 applied to it.</p> <p>CVE-2010-0290</p> <p>Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching, aka Bug 20737. NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4022 (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 4.0 version 2 for version 3 has no score applied to it.</p>
Windows 7	No vulnerabilities discovered	No vulnerabilities where found when scanning windows with Nmap and Vulners.

	using nmap-vulners. See screenshot in Figure	
Windows XP	No vulnerabilities discovered using nmap-vulners. See screenshot in Figure	No vulnerabilities were found when scanning windows with Nmap and Vulners.

VULNERS FOR CVE FOR WEB SERVER (192.168.56.101)

Figure 13

```
root@kali:~# nmap -sV --script nmap-vulners -p 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 10:23 EST
Nmap scan report for 192.168.56.101
Host is up (1.0s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu1.9)
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
n_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
| vulners:
|   cpe:/a:apache:http_server:2.2.14:
|     CVE-2010-0425  10.0  https://vulners.com/cve/CVE-2010-0425
|     CVE-2011-3192  7.8   https://vulners.com/cve/CVE-2011-3192
|     CVE-2017-7679  7.5   https://vulners.com/cve/CVE-2017-7679
|     CVE-2017-7668  7.5   https://vulners.com/cve/CVE-2017-7668
|     CVE-2017-3169  7.5   https://vulners.com/cve/CVE-2017-3169
|     CVE-2017-3167  7.5   https://vulners.com/cve/CVE-2017-3167
|     CVE-2013-2249  7.5   https://vulners.com/cve/CVE-2013-2249
|     CVE-2012-0883  6.9   https://vulners.com/cve/CVE-2012-0883
|     CVE-2018-1312  6.8   https://vulners.com/cve/CVE-2018-1312
|     CVE-2013-1862  5.1   https://vulners.com/cve/CVE-2013-1862
|     CVE-2014-0231  5.0   https://vulners.com/cve/CVE-2014-0231
|     CVE-2014-0098  5.0   https://vulners.com/cve/CVE-2014-0098
|     CVE-2013-6438  5.0   https://vulners.com/cve/CVE-2013-6438
|     CVE-2012-4557  5.0   https://vulners.com/cve/CVE-2012-4557
|     CVE-2011-3368  5.0   https://vulners.com/cve/CVE-2011-3368
|     CVE-2010-2068  5.0   https://vulners.com/cve/CVE-2010-2068
|     CVE-2010-1452  5.0   https://vulners.com/cve/CVE-2010-1452
|     CVE-2010-0408  5.0   https://vulners.com/cve/CVE-2010-0408
|     CVE-2012-0031  4.6   https://vulners.com/cve/CVE-2012-0031
|     CVE-2011-3607  4.4   https://vulners.com/cve/CVE-2011-3607
|     CVE-2016-4975  4.3   https://vulners.com/cve/CVE-2016-4975
|     CVE-2013-1896  4.3   https://vulners.com/cve/CVE-2013-1896
|     CVE-2012-4558  4.3   https://vulners.com/cve/CVE-2012-4558
|     CVE-2012-3499  4.3   https://vulners.com/cve/CVE-2012-3499
|     CVE-2012-0053  4.3   https://vulners.com/cve/CVE-2012-0053
|     CVE-2011-4317  4.3   https://vulners.com/cve/CVE-2011-4317
|     CVE-2011-3639  4.3   https://vulners.com/cve/CVE-2011-3639
|     CVE-2011-3348  4.3   https://vulners.com/cve/CVE-2011-3348
|     CVE-2011-0419  4.3   https://vulners.com/cve/CVE-2011-0419
|     CVE-2010-0434  4.3   https://vulners.com/cve/CVE-2010-0434
|     CVE-2016-8612  3.3   https://vulners.com/cve/CVE-2016-8612
|     CVE-2012-2687  2.6   https://vulners.com/cve/CVE-2012-2687
|     CVE-2011-4415  1.2   https://vulners.com/cve/CVE-2011-4415
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap       Courier Imapd (released 2008)
443/tcp  open  ssl/https?
```

DATABASE SERVER (192.168.56.105)

Figure 14

```
root@kali:/usr/share/nmap/scripts# nmap -sV --script nmap-vulners 192.168.56.105
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 14:41 EST
Nmap scan report for 192.168.56.105
Host is up (1.0s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     CVE-2010-4478  7.5      https://vulners.com/cve/CVE-2010-4478
|     CVE-2017-15906 5.0      https://vulners.com/cve/CVE-2017-15906
|     CVE-2016-10708 5.0      https://vulners.com/cve/CVE-2016-10708
|     CVE-2010-4755  4.0      https://vulners.com/cve/CVE-2010-4755
|     CVE-2008-5161  2.6      https://vulners.com/cve/CVE-2008-5161
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
|_ vulners:
|   cpe:/a:isc:bind:9.4.2:
|     CVE-2012-1667  8.5      https://vulners.com/cve/CVE-2012-1667
|     CVE-2014-8500  7.8      https://vulners.com/cve/CVE-2014-8500
|     CVE-2012-5166  7.8      https://vulners.com/cve/CVE-2012-5166
|     CVE-2012-4244  7.8      https://vulners.com/cve/CVE-2012-4244
|     CVE-2012-3817  7.8      https://vulners.com/cve/CVE-2012-3817
|     CVE-2008-4163  7.8      https://vulners.com/cve/CVE-2008-4163
|     CVE-2010-0382  7.6      https://vulners.com/cve/CVE-2010-0382
|     CVE-2017-3141  7.2      https://vulners.com/cve/CVE-2017-3141
|     CVE-2015-8461  7.1      https://vulners.com/cve/CVE-2015-8461
|     CVE-2015-8704  6.8      https://vulners.com/cve/CVE-2015-8704
|     CVE-2009-0025  6.8      https://vulners.com/cve/CVE-2009-0025
|     CVE-2015-8705  6.6      https://vulners.com/cve/CVE-2015-8705
|     CVE-2010-3614  6.4      https://vulners.com/cve/CVE-2010-3614
|     CVE-2017-3145  5.0      https://vulners.com/cve/CVE-2017-3145
|     CVE-2016-9444  5.0      https://vulners.com/cve/CVE-2016-9444
|     CVE-2016-9131  5.0      https://vulners.com/cve/CVE-2016-9131
|     CVE-2016-8864  5.0      https://vulners.com/cve/CVE-2016-8864
|     CVE-2016-2848  5.0      https://vulners.com/cve/CVE-2016-2848
|     CVE-2016-1286  5.0      https://vulners.com/cve/CVE-2016-1286
|     CVE-2015-8000  5.0      https://vulners.com/cve/CVE-2015-8000
|     CVE-2012-1033  5.0      https://vulners.com/cve/CVE-2012-1033
|     CVE-2011-4313  5.0      https://vulners.com/cve/CVE-2011-4313
|     CVE-2011-1910  5.0      https://vulners.com/cve/CVE-2011-1910
|     CVE-2009-0265  5.0      https://vulners.com/cve/CVE-2009-0265
|     CVE-2017-3143  4.3      https://vulners.com/cve/CVE-2017-3143
|     CVE-2017-3142  4.3      https://vulners.com/cve/CVE-2017-3142
|     CVE-2016-2775  4.3      https://vulners.com/cve/CVE-2016-2775
|     CVE-2016-1285  4.3      https://vulners.com/cve/CVE-2016-1285
|     CVE-2010-0097  4.3      https://vulners.com/cve/CVE-2010-0097
|     CVE-2009-0696  4.3      https://vulners.com/cve/CVE-2009-0696
|     CVE-2018-5741  4.0      https://vulners.com/cve/CVE-2018-5741
|     CVE-2016-6170  4.0      https://vulners.com/cve/CVE-2016-6170
|     CVE-2010-0290  4.0      https://vulners.com/cve/CVE-2010-0290
```

WINDOWS 7 (192.168.56.103)

Figure 15

```
root@kali:~# nmap -sV --script nmap-vulners 192.168.56.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 12:39 EST
Nmap scan report for 192.168.56.103
Host is up (1.0s latency).

Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: workgroup)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/bug.html
Nmap done: 1 IP address (1 host up) scanned in 65.07 seconds
```

WINDOWS XP (192.168.56.104)

Figure 16

```
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to
^Croot@kali:~# nmap -sV --script nmap-vulners 192.168.56.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-18 12:58 EST
Nmap scan report for 192.168.56.103
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: ADMIN-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.81 seconds
```

STEP 5: VULNERABILITY ASSESSMENT OF WEB SERVER

The information within this table can be found within figure 13 above.

Vulnerability	Brief Description	Vendor Fix
CVE-2017-7668	<p>“The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token to return an incorrect value.” (Nvd.nist.gov, 2019).</p> <p>This CVE has two scores version 2 is a score of 7.5 and version 3 is a score of 9.8</p>	The fix for this was apache version 2.2.32 patch or upgrade to version 2.2.33. An update was released on 19th June 2017.
CVE-2017-3169	<p>“In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score under version 2 of 7.5 and a score of 9.8 on version 3.</p>	The fix for this was apache version 2.2.32 patch or upgrade to version 2.2.33 an update was released on 19th June 2017
CVE-2011-3368	<p>“The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. This CVE has a score of 4.3 on version 2 and no</p>	No fix or patch could be found

	<p>score applied for version 3.” (Nvd.nist.gov, 2019).</p> <p>This CVE exists because “NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.”.</p>	
CVE-2016-8612	<p>“Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.” (Nvd.nist.gov, 2019).</p> <p>The score for this CVE is 3.3 for version 2 and a score of 4.3 for version 3.</p>	No fix or patch could be found.
CVE-2012-2687	<p>“Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score on version 2 of 2.6 on version 2 and for version 3 there is no score applied.</p>	This affects versions 2.4.2 and 2.4.1 an update was released to patch this on 21st August 2012

All references within the brief description relate to vendor fix.

Step 5.1: Vulnerability Assessment of Database Server

Vulnerability	Brief Description	Vendor Fix
Database Server	CVE-2012-1667 <p>“ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-</p>	Workarounds are currently being investigated, but none are currently known.

	<p>length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 8.5 version 2 for version 3 has no score applied to it.</p>	
Database Server	<p>CVE-2008-4163</p> <p>“Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 7.8 version 2 for version 3 has no score applied to it.</p>	Apply update from the vendor, newer versions fix this vulnerability.
Database Server	<p>CVE-2016-1286</p> <p>“named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 5.0 version 2 for version 3 has a score 7.8 applied to it.</p>	Apply latest update from the vendor.
Database Server	<p>CVE-2016-1285</p> <p>“named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related</p>	Apply latest update from the vendor.

	<p>to alist.c and sexpr.c.” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 4.3 version 2 for version 3 has a score 6.8 applied to it.</p>	
Database Server	<p>CVE-2010-0290</p> <p>“Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching, aka Bug 20737. NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4022” (Nvd.nist.gov, 2019).</p> <p>This CVE has a score of 4.0 version 2 for version 3 has no score applied to it.</p>	Apply latest update from the vendor.

All references within the brief description relate to vendor fix.

NIKTO —HOST IP_ADDRESS —PORT 80

Figure 17

```
root@kali:~# nikto -host 192.168.56.101
- Nikto v2.1.6

+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2019-11-18 08:58:13 (GMT-5)

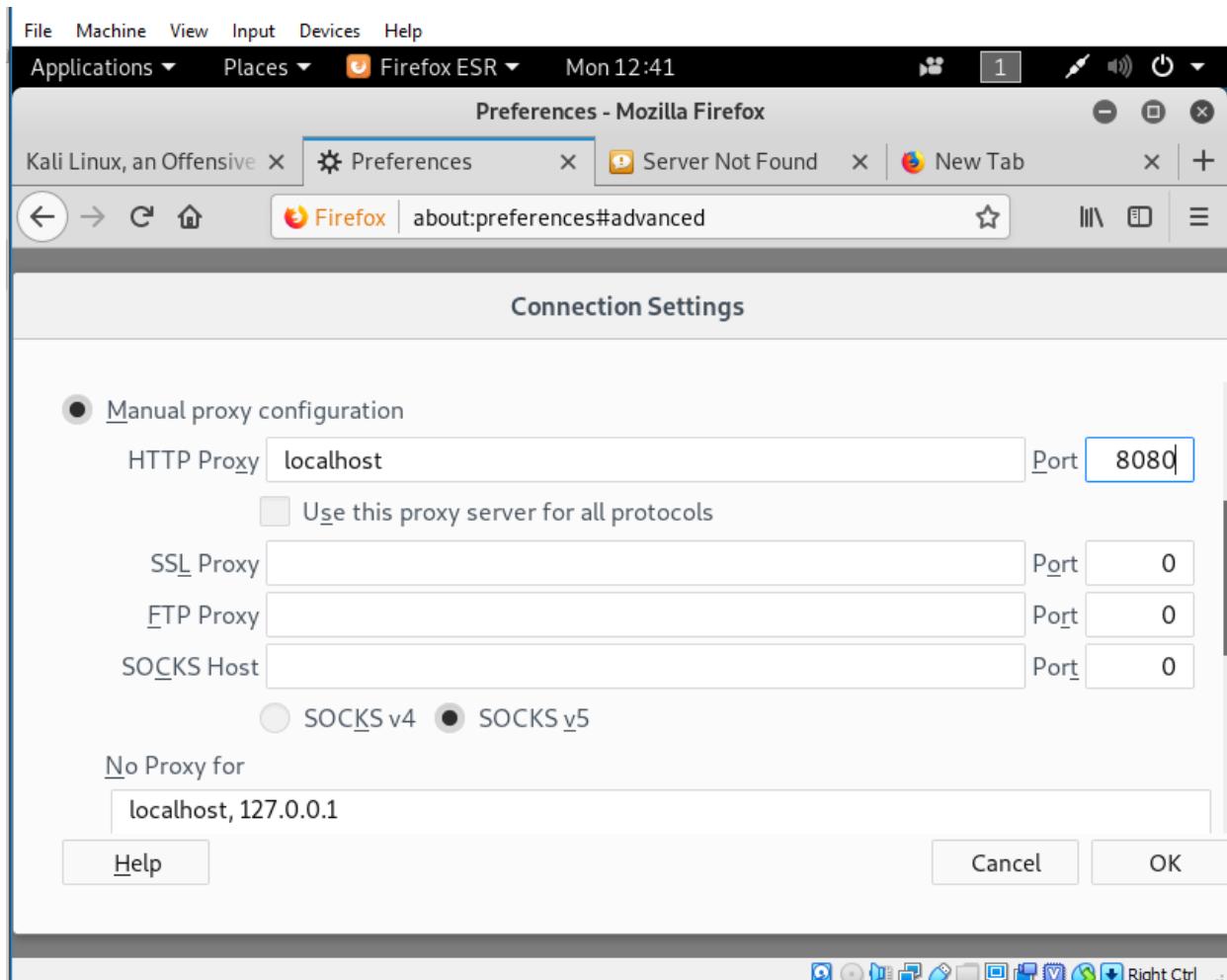
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Server leaks inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 22:55:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different way
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-injection-via-OpenSSL-0.9.8k.html
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Phusion Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.5)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The header found was: Content-Type: application/x-ms-application; Content-Length: 0; Content-Disposition: inline; Content-Location: /images
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://httpd.apache.org/docs/2.4/mod/mod_negotiation.html
+ OSVDB-3092: /index/ index.css, index.html
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower are vulnerable to CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ Cookie phpb2owaspbwa_data created without the httponly flag
+ Cookie phpb2owaspbwa_sid created without the httponly flag
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to trusted users
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3092: /cgi-bin/: This might be interesting... possibly a system shell found.
+ OSVDB-3093: /.bash_history: A user's home directory may be set to the web root, the shell history was retrieved. This is a security risk.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found
```

STEP 6: BURP SUITE PROXY

In this section Burp Suite has been used to carry out an SQL Injection Attack. This application is built into Kali Linux but also has two versions, the free edition and the professional edition. The free version has features allowing a user to discover and exploit the SQL Injection.

CONFIGURING BURP SITE FREE EDITION

Figure 18



After using the “netdiscover” and “nikto -host” command, the web server IP address was given back. The IP address is 192.168.56.101. After this, <http://192.168.56.x/bWAPP> was opened on a web browser, using the username “bee” and entering in “bug” as the password allowed for the SQL Injection page in Burp Suite to open.

Figure 19

The screenshot shows a search interface for movies. A search bar at the top has the placeholder "Search for a movie:". Below it is a table header with columns: Title, Release, Character, Genre, and IMDb. The table body contains a single row with the following data: Title (containing 'OR 1=1'), Release (2012), Character (Scarlett Johansson), Genre (Romantic), and IMDb (8.2). A message at the bottom of the table says: "Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' at line 1".

In the “Search for a movie” box, a single quota was written to return the below results.

In the place where the single quota was placed a script is written using SQL Injection. Below in figures 19 and 20, it shows queries being changed within the database using Burp, after this more information is required to be gathered.

Figure 20

154	http://192.168.56.101	GET	/bWAPP	301	673	F
155	http://192.168.56.101	GET	/bWAPP/	302	422	F
156	http://192.168.56.101	GET	/bWAPP/portal.php	302	616	F
157	http://192.168.56.101	GET	/bWAPP/login.php	200	3419	F
159	http://192.168.56.101	GET	/bWAPP/js/html5.js	200	2871	S

Using command below it gathered version of the host server.

1' UNION SELECT 1,2,3,4, version(),6,7--

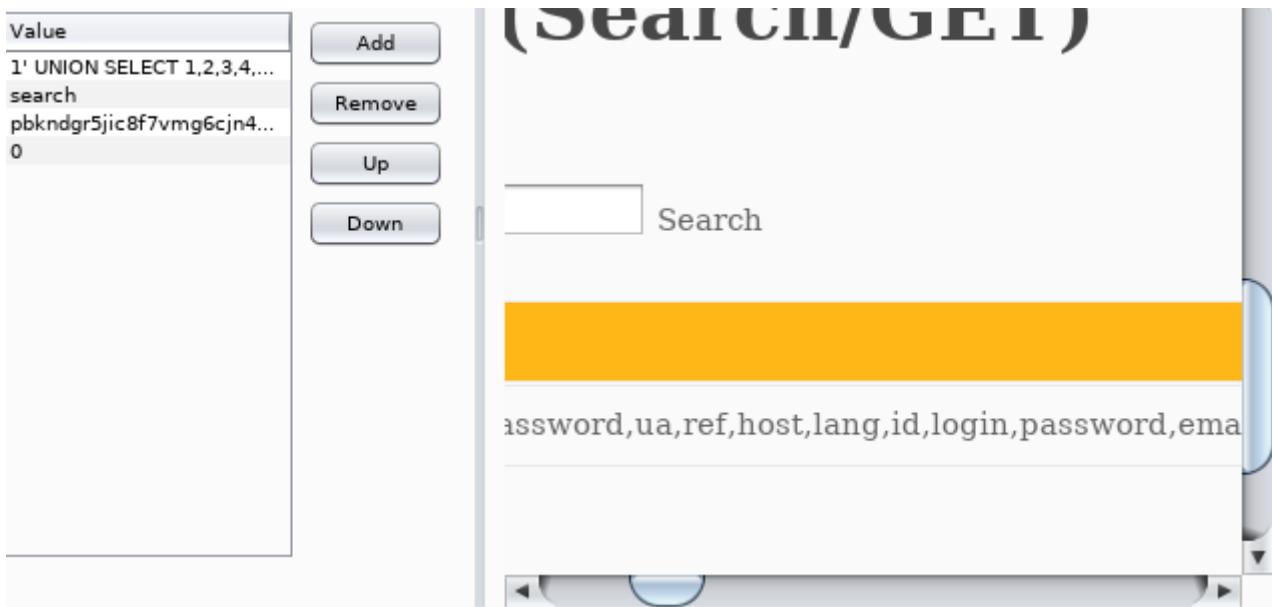
Figure 21

The screenshot shows the Burp Suite interface. On the left, under the 'Value' field, there is a text input containing the SQL injection payload: '1' UNION SELECT 1,2,3,4,...'. To the right, the 'Response' tab is selected, showing the raw response from the server. The word 'Release' is highlighted in yellow, indicating a potential point of interest or a keyword related to the current analysis.

Next step is look for lack of database security. With this there can be set queries which allow the database to search the table GROUP_CONCAT(table_name). An attacker can use this type of command to get to know the structure of databases.

1' UNION SELECT 1,2,3,4, GROUP_CONCAT(table_name),6,7 FROM information_schema.tables WHERE table_schema = DATABASE()--+

Figure 22



The next step in exploiting a database with SQL Injection is stealing information from the service. The crucial information in this case would be login and passwords. In more advanced cases it can also steal financial information or more valuable data. The screenshot below shows the password hash.

1' UNION SELECT 1,2,3,4, GROUP_CONCAT(login,password),6,7 FROM users--+

Figure 23

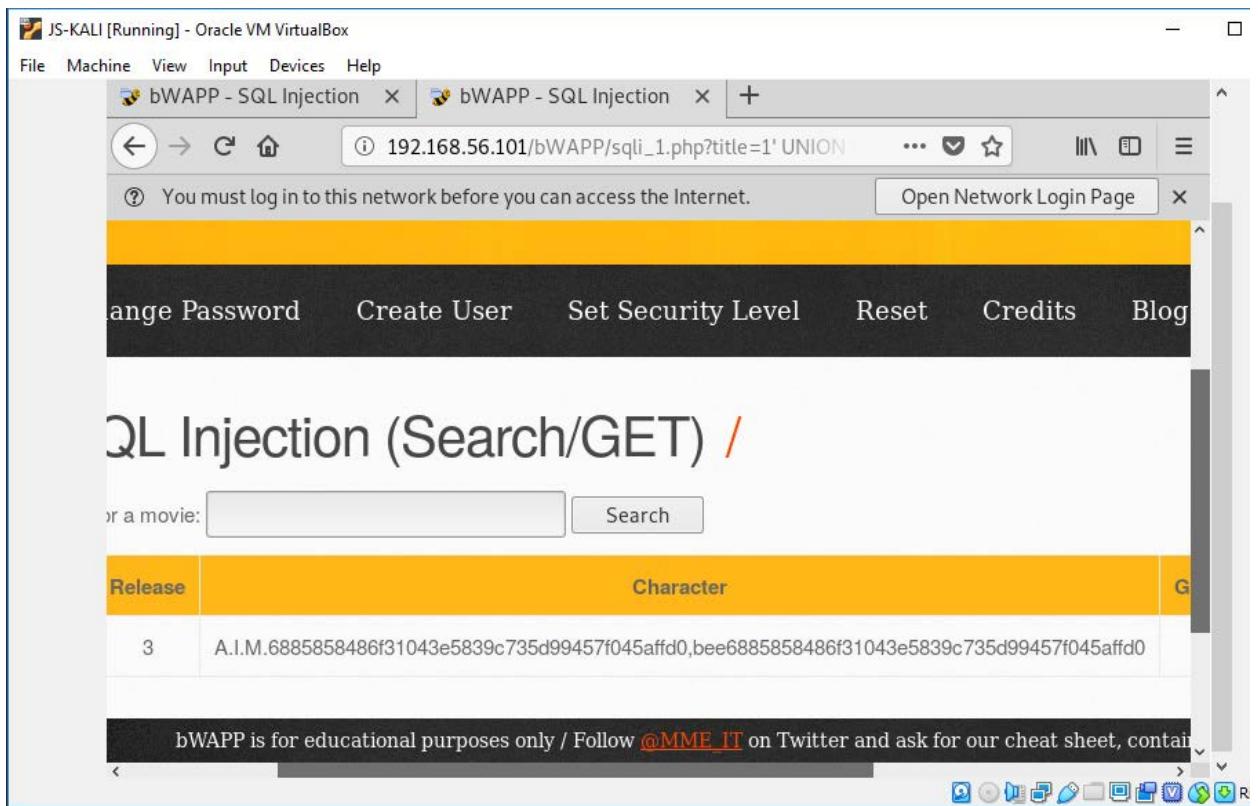


Figure 24 shows the hashed password decrypted. By copying the discovered hash password into the text box which cracks it, it comes back with a green match which indicates that the password was decrypted successfully.

Figure 24

The screenshot shows a web browser window for crackstation.net. In the address bar, the URL 'crackstation.net' is visible. Below the address bar, there is a text input field with the placeholder 'Enter up to 20 non-salted hashes, one per line:' followed by a single hash value: '6885858486f31043e5839c735d99457f045affd0'. To the right of the input field is a reCAPTCHA interface with the text 'I'm not a robot' and the reCAPTCHA logo. Below the input field is a button labeled 'Crack Hashes'. Underneath the input field, there is a note about supported hash types: 'Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+(sha1(bin)), QubesV3.1BackupDefaults'. Below this, there is a table with three columns: 'Hash', 'Type', and 'Result'. The first row in the table contains the hash '6885858486f31043e5839c735d99457f045affd0', its type 'sha1', and its result 'bug'. A color legend at the bottom left of the table area states: 'Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.'

Hash	Type	Result
6885858486f31043e5839c735d99457f045affd0	sha1	bug

Page Break

CONCLUSION

Within the portfolio, the network needed to be set up before penetration testing could commence. The network for The Happy Shop Inc consisted of a database server, a web server, a Windows 7 machine and an old but usable Windows XP machine. It was uncertain if the servers and machines were secure and free from vulnerabilities so HackBay Pvt Ltd, the team being posed as undertook a penetration test. Using port-scanning as seen in figures 2-12, allowed for all open ports of each machine on the network to be identified as well as the operating systems they use. This gives an idea of how vulnerable a system or entire network might be.

Nmap Vulners was used to identify the vulnerabilities within the network on each machine, it was suspected that Windows XP would be the most vulnerable due to being unsupported, this was not the case. Multiple vulnerabilities were found on both the database and web server, they had multiple CVE codes related to them, these were investigated, and multiple fixes were identified. If these vulnerabilities were not discovered, the servers could have been easily hacked in the future which would have led to both confidential and sensitive information being leaked. Most of the vulnerabilities could be resolved through updating the services and operating systems alike, this could be done through an Active Directory with an admin in control where these can be deployed seamlessly.

The rule of thumb to come from this conclusion is that anything can be vulnerable, the only real solution is to rely on services having a newer version available and keeping systems up to date, sometimes an older version may not have any vulnerabilities, but it is still best to keep updated.

REFERENCES PORTFOLIO 3

- ATOUM, J.O. AND QARALLEH, A.J., 2014. A hybrid technique for SQL injection attacks detection and prevention. International Journal of Database Management Systems, 6(1), p.21.
- BALOCH, R., 2014. Ethical Hacking and Penetration Testing Guide.
- BANKS, J., 2015, "The Heartbleed bug: Insecurity repackaged, rebranded and resold", Crime, Media, Culture: An International Journal, vol. 11, no. 3, pp. 259-279.
- FRUHLINGER, J., 2017. What is the Heartbleed bug, how does it work and how was it fixed?. [online] CSO Online. Available at: <https://www.csionline.com/article/3223203/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html> [Accessed 18 Nov. 2019].
- GAJAWADA, A., 2016. Heartbleed bug: How it works and how to avoid similar bugs. [online] Software Integrity Blog. Available at: <https://www.synopsys.com/blogs/software-security/heartbleed-bug/> [Accessed 18 Nov. 2019].
- GUPTA, S. & GUPTA, B.B. 2017, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art", International Journal of System Assurance Engineering and Management, vol. 8, no. S1, pp. 512-530.
- HALFOND, W.G., VIEGAS, J. AND ORSO, A., 2006, March. A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE International Symposium on Secure Software Engineering (Vol. 1, pp. 13-15). IEEE.
- Heartbleed.com., 2014. Heartbleed Bug. [online] Available at: <http://heartbleed.com/> [Accessed 18 Nov. 2019].
- HUANG, H., ZHANG, Z., CHENG, H. & SHIEH, S.W. 2017, "Web Application Security: Threats, Countermeasures, and Pitfalls", Computer, vol. 50, no. 6, pp. 81-85
- RODRÍGUEZ, G.E., TORRES, J.G., FLORES, P. & BENAVIDES, D.E. 2019, "Cross-Site Scripting (XSS) Attacks And Mitigation: A Survey", Computer Networks, , pp. 106960.
- RUIZ, G., 2018. OWASP Top 10 Security Risks – Part I. [online] Blog.sucuri.net. Available at: <https://blog.sucuri.net/2018/10/owasp-top-10-security-risks-part-i.html> [Accessed 25 Nov. 2019].
- RUIZ, G., 2019. OWASP Top 10 Security Risks – Part IV. Blog.sucuri.net [online]. Available from: <https://blog.sucuri.net/2019/01/owasp-top-10-security-risks-part-iv.html> [Accessed 16 November 2019].
- SINGH, V., 2017. What is HTTP Request, Request Line, Request Header & Request Body?. TOOLSQA [online]. Available from: <https://www.toolsqa.com/client-server/http-request/> [Accessed 17 November 2019].
- Group, D. (2019). *httpd 2.4 vulnerabilities - The Apache HTTP Server Project*. [online]
- Nvd.nist.gov. (2019). NVD - Home. [online] Available at: <https://nvd.nist.gov/> [Accessed 27 Nov. 2019].
- Nvd.nist.gov, 2019. NVD - CVE-2008-4163. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2008-4163> [Accessed 29 Nov. 2019].
- Nvd.nist.gov. (2019). NVD - CVE-2010-0290. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2010-0290> [Accessed 29 Nov. 2019].
- Nvd.nist.gov. (2019). NVD - CVE-2010-0425. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2010-0425> [Accessed 27 Nov. 2019].

- Nvd.nist.gov. (2019). *NVD - CVE-2011-4317*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2011-4317> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2011-4415*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2011-4415> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2012-0031*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2012-0031> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2012-1667*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2012-1667> [Accessed 29 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2015-1452*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2015-1452> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2016-1285*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2016-1285> [Accessed 29 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2016-1286*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2016-1286> [Accessed 29 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2016-8612*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2016-8612> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2017-3169*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2017-3169> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2017-7668*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2017-7668> [Accessed 27 Nov. 2019].
- Nvd.nist.gov. (2019). *NVD - CVE-2017-7679*. [online] Available at: <https://nvd.nist.gov/vuln/detail/CVE-2017-7679> [Accessed 27 Nov. 2019].