Indian Institute of Technology, Kanpur

Digital India
Power To Empower

ELECTRONICS INDIA
Billion Needs Million Chips

GOVERNMENT OF INDIA
Ministry of Electronics and Information Technology (MeitY)

IITK –ICT Summer Term Program (Cyber Security with Linux and Networking) 2020

Project – Penetration Testing On Web Servers

Submitted by- Anubhav Miller

Guided By- Mr. Rahul Gupta Sir

Project :- **Penetration Testing on Web Server**

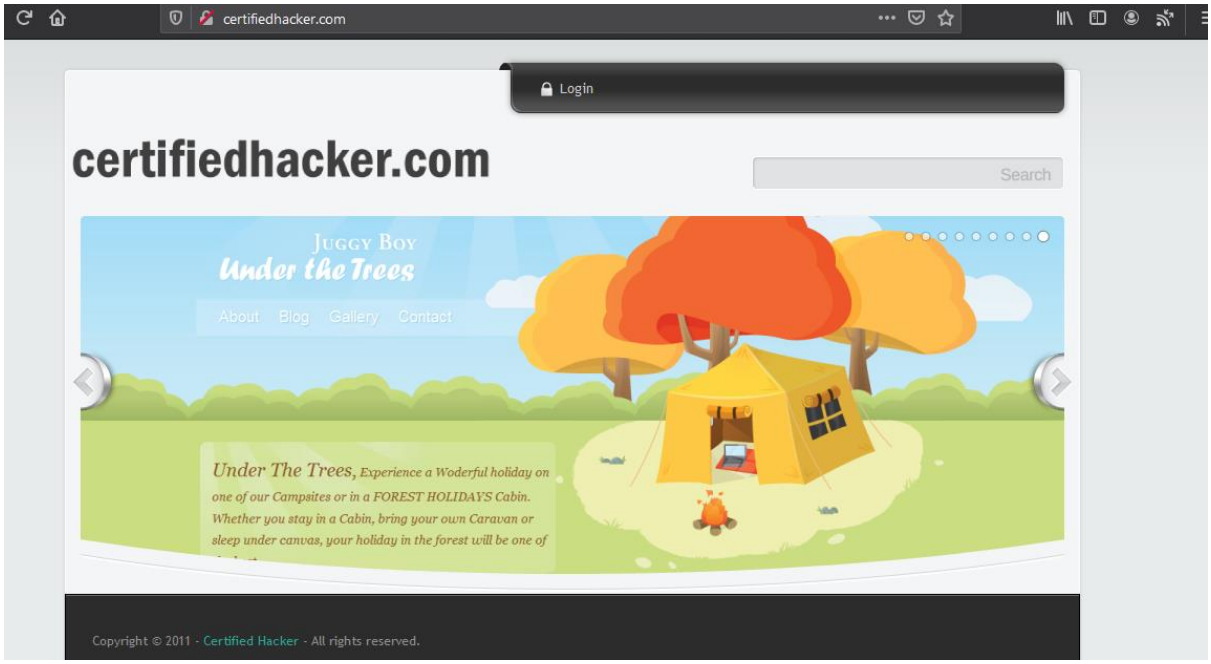
Website: www.certifiedhacker.com

Project Summary

- You have to harden the security of company website and also secure employees from being social engineered. That requires a lot of Footprinting and reconnaissance and hacking techniques. So, you have to penetrate the website and report all findings. Footprinting and Reconnaissance

1. About company
2. IP address of Website
3. Location of server
4. Operating System of server
5. Web server technology and version
6. Built in technology
7. When website first seen
8. Previous technology used by website
9. Which ISP IP range server is using
10. Do any other domains are on same server, if yes domain names

11. Ports open on Webserver
12. Registrar information of domain
13. Email ID of some employees of company
14. Social Networking Profiles of employees
15. LinkedIn Search for profiles with company name
16. Address of company
17. Director/CEO of company
18. Check firewall and load balancer presence
19. Check directory listing, if enabled write the directory structure
20. Check for files such as robots.txt and sites.xml



- **IP of website- Here we used CMD (i.e command promt) of windows OS to get the IP address of the given website.**

  By using the ping command.

```
C:\Users\HP>ping certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=302ms TTL=47
Reply from 162.241.216.11: bytes=32 time=295ms TTL=47
Reply from 162.241.216.11: bytes=32 time=299ms TTL=47
Reply from 162.241.216.11: bytes=32 time=310ms TTL=47

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 295ms, Maximum = 310ms, Average = 301ms
```

- **This command sends the packet of a default size to that website and get a response from there is the website is live and the packet size if accepted.**

2-Getting the max size of the packet that can be send over that website through my IP.

By using ping command.

```
C:\Users\HP>ping  -f -l 1472 certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=353ms TTL=47
Reply from 162.241.216.11: bytes=1472 time=328ms TTL=47
Reply from 162.241.216.11: bytes=1472 time=543ms TTL=47
Reply from 162.241.216.11: bytes=1472 time=358ms TTL=47

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 328ms, Maximum = 543ms, Average = 395ms
```

BY the above command we found that size of 1472 bytes can be send over there from my IP(It's not same all the time it varries)

3-Getting the pathway how many IP it will travel to get our requested things to us by tracert command in CMD.(It also gives the roundtrip time)

```
C:\Users\HP>tracert certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1     1 ms     9 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    61 ms    55 ms    51 ms  10.40.19.125
  4    60 ms    53 ms    45 ms  10.50.73.185
  5    58 ms    50 ms    49 ms  dsl-tn-dynamic-145.222.22.125.airtelbroadband.in [125.22.222.145]
  6   149 ms   165 ms   159 ms  182.79.134.112
  7   155 ms   159 ms   174 ms  mei-b3-link.telia.net [62.115.42.118]
  8   302 ms   301 ms   296 ms  prs-bb3-link.telia.net [62.115.118.94]
  9   298 ms   300 ms   285 ms  ash-bb2-link.telia.net [62.115.112.242]
 10   296 ms   296 ms   281 ms  atl-b24-link.telia.net [62.115.125.128]
 11   310 ms   299 ms   299 ms  hou-b1-link.telia.net [62.115.116.46]
 12   300 ms   298 ms   292 ms  cyrusone-svc067800-lag002969.c.telia.net [62.115.184.145]
 13   293 ms   300 ms   304 ms  72-250-192-6.cyrusone.com [72.250.192.6]
 14   300 ms   287 ms   290 ms  po101.router2a.hou1.net.unifiedlayer.com [162.241.0.7]
 15   293 ms   291 ms   292 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
 16   294 ms   299 ms   298 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.
```

Or as alternate we can use pathping command that is a combination of ping+tracert command

Getting more information about that website by its IP address (https://bgp.he.net/ip/162.241.216.11#_ipinfo)

BY bgp.he.net – Its gives info like the DNS,Whois,Other associated host etc

bgp.he.net/ip/162.241.216.11#_ipinfo

Apps | Welcome to Indian... | IRCTC Next Generat... | Image resize, edit, a... | jhsir

HURRICANE ELECTRIC
INTERNET SERVICES

Search

162.241.216.11

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

IP Info | Whois | DNS | RBL

162.241.216.11 (box5331.bluehost.com)

Announced By		
Origin AS	**Announcement**	**Description**
AS46606	162.240.0.0/15	Unified Layer
AS46606	162.241.0.0/16	Unified Layer

Address has 1448 hosts associated with it.

Updated 16 Jun 2020 01:36 PST © 2020

Whois info-

HURRICANE ELECTRIC
INTERNET SERVICES

Search

162.241.216.11

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

IP Info | Whois | DNS | RBL

```
NetRange:       162.240.0.0 - 162.241.255.255
CIDR:           162.240.0.0/15
NetName:        UNIFIEDLAYER-NETWORK-16
NetHandle:      NET-162-240-0-0-1
Parent:         NET162 (NET-162-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS46606
Organization:   Unified Layer (BLUEH-2)
RegDate:        2013-08-22
Updated:        2013-08-22
Ref:            https://rdap.arin.net/registry/ip/162.240.0.0

OrgName:        Unified Layer
OrgId:          BLUEH-2
Address:        1958 South 950 East
City:           Provo
StateProv:      UT
PostalCode:     84606
Country:        US
RegDate:        2006-08-08
Updated:        2020-01-31
Ref:            https://rdap.arin.net/registry/entity/BLUEH-2

ReferralServer:  rwhois://rwhois.unifiedlayer.com:4321

OrgTechHandle: ENO74-ARIN
OrgTechName:   EIG Network Operations
OrgTechPhone:  +1-877-659-6181
OrgTechEmail:  eig-noc@endurance.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ENO74-ARIN
```

For DNS we can also use the CMD by nslookup command.

```
C:\Users\HP>nslookup certifiedhacker.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
```

Getting information about some of its background, network, hosting history by netcraft.com (https://sitereport.netcraft.com/?url=http://certifiedhacker.com/)

Background

Site title	Not Acceptable!	Date first seen	December 2002
Site rank	42895	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	http://certifiedhacker.com	Domain registrar	networksolutions.com
Netblock Owner	Unified Layer	Nameserver organisation	whois.domain.com
Domain	certifiedhacker.com	Organisation	5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
Nameserver	ns1.bluehost.com		
IP address	162.241.216.11 (VirusTotal)	Hosting company	Endurance International Group
DNS admin	dnsadmin@box5331.bluehost.com	Top Level Domain	Commercial entities (.com)
IPv6 address	Not Present	DNS Security Extensions	unknown
Reverse DNS	box5331.bluehost.com	Hosting country	US

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	15-Jun-2020
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	29-May-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Nov-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	-	nginx/1.12.1	5-Nov-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	17-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.1	6-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.0	28-May-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.2	15-Apr-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.1	19-Oct-2016

- **Getting information of OS of server , Technology used Ports and services over that website,we are using shodan.io(https://www.shodan.io/host/162.241.216.11)**

162.241.216.11 box5331.bluehost.com

starttls Database

Country	**United States**
Organization	**Unified Layer**
ISP	**Unified Layer**
Last Update	**2020-06-16T16:10:37.001659**
Hostnames	**box5331.bluehost.com**
ASN	**AS46606**

Web Technologies

- Google Font API
- jQuery
- jQuery Migrate
- MySQL
- NextGEN Gallery
- PHP
- WordPress
- Yoast SEO

Ports

22 53 80 110 443 465 587 993 2082

2086 2087 2096 2222 3306 5432

Services

22
tcp
ssh

OpenSSH Version: 5.3

```
SSH-2.0-OpenSSH_5.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAzWY7a5YXkotfyVQXp4K/w/3qkPREhYS6b8Cf89YCCYYuIPyV
THfRdZ12PybQq/1Cr57qi/csGcY98DjWI3xpYcDAHgr6uTPprJJvF6WBbPxwU6gyb8m2XjX40VeH
MOhCBIh//36817BiLQRy71APuUgcnh3wIsjz+sObd1rlvRAdzLVk0Ru+JmioWCon83IPqnwLsWKY
f35N7olSdzwEQXfGDtgd2BHr9fnMeXKEBCfyPCs/DZ7dd6xPBmqFzaQZQLua4+L/EuOHRFGwgN5v
04fyusL321Zw1B3u2MkUoh6Zz6DDlQqXhaWyrzSHPwb9i1ucUT0RvK+PP8gLwpj6iw==
Fingerprint: c5:65:11:7c:5b:03:60:8e:be:13:1e:d9:b6:8d:80:ac

Kex Algorithms:
        diffie-hellman-group-exchange-sha256

Server Host Key Algorithms:
        ssh-rsa
        ssh-dss

Encryption Algorithms:
        aes256-ctr
        aes192-ctr
        aes128-ctr

MAC Algorithms:
        hmac-sha2-512
        hmac-sha2-256
        hmac-ripemd160
        hmac-ripemd160@openssh.com

Compression Algorithms:
        none
        zlib@openssh.com
```

53
tcp
dns-tcp

```
9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.4
```

53
udp
dns-udp

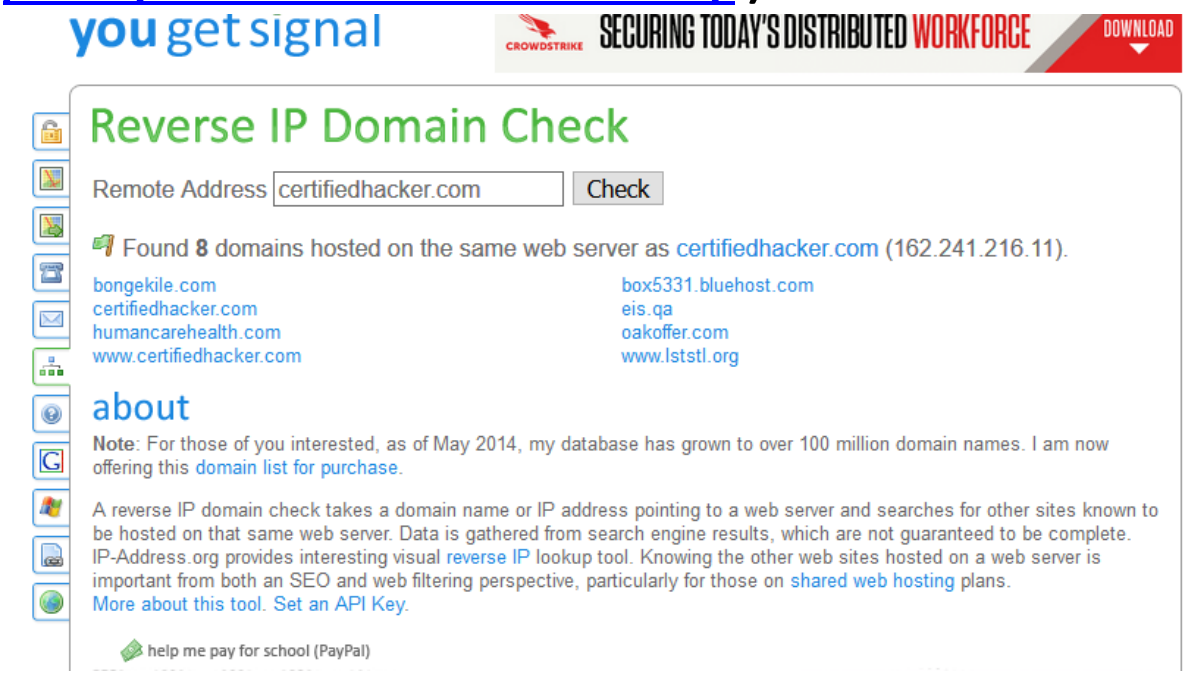
```
9.8.2rc1-RedHat-9.8.2-0.62.rc1.el6_9.4
```

80
tcp
http

Apache httpd

```
HTTP/1.1 404 Not Found
Date: Fri, 12 Jun 2020 22:04:36 GMT
Server: Apache
Content-Length: 315
Content-Type: text/html; charset=iso-8859-1
```

- **Checking for domain hosted on the same webserver as certifiedhacker.com by using website yougetsignal.com(https://www.yougetsignal.com/tools/web-sites-on-web-server/)**



- **Previous technology used and previous view of that website we can get this info by archive.org(https://web.archive.org/web/*/http://certifiedhacker.com/)**

https://web.archive.org/web/*/http://certifiedhacker.com/

See what's new with book lending at the Internet Archive

INTERNET ARCHIVE WEB BOOKS VIDEO AUDIO SOFTWARE IMAGES SIGN UP | LOG IN UPLOAD Search

ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE

DONATE

INTERNET ARCHIVE WayBackMachine

Explore more than 446 billion web pages saved over time

http://certifiedhacker.com/

Calendar · Collections beta · Changes beta · Summary · Site Map

Saved **212 times** between March 25, 2004 and February 27, 2020.

Explore captures for this URL

1997 1998 1999 2000 2001 2002 2003 2004 2005 **2006** 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 **2020**

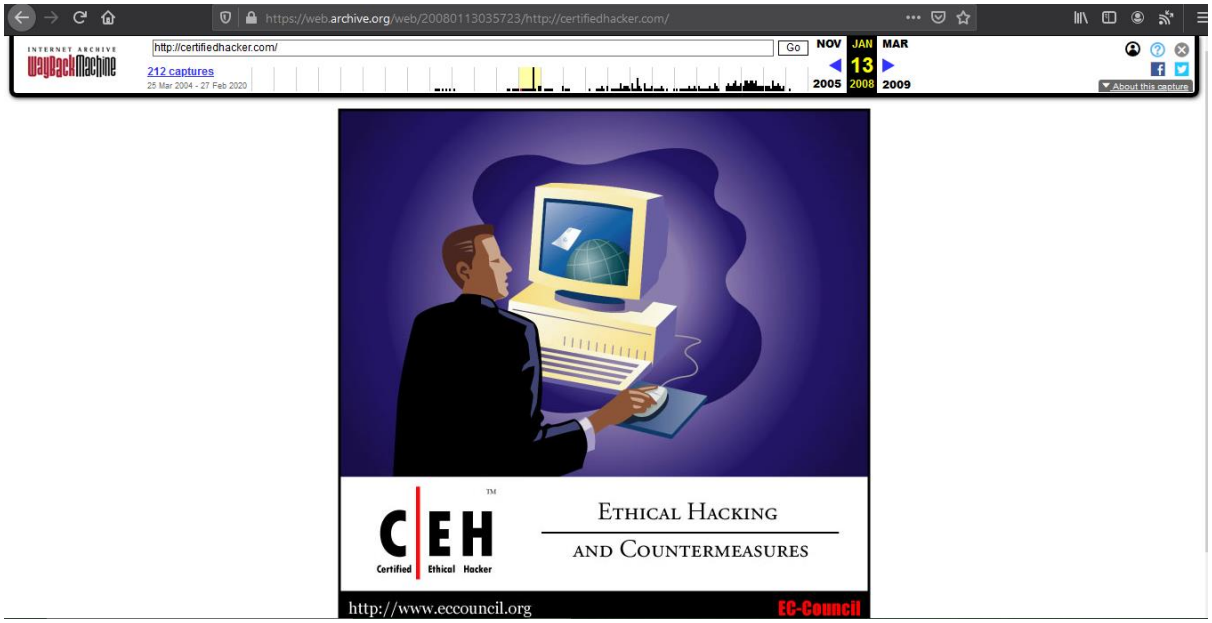
JAN							FEB							MAR							APR						
			1	2	3	4							1	1	2	3	4	5	6	7				1	2	3	4
5	6	7	8	9	10	11	2	3	4	5	6	7	8	8	9	10	11	12	13	14	5	6	7	8	9	10	11
12	13	14	15	16	17	18	9	10	11	12	13	14	15	15	16	17	18	19	20	21	12	13	14	15	16	17	18

Saved **212 times** between March 25, 2004 and February 27, 2020.

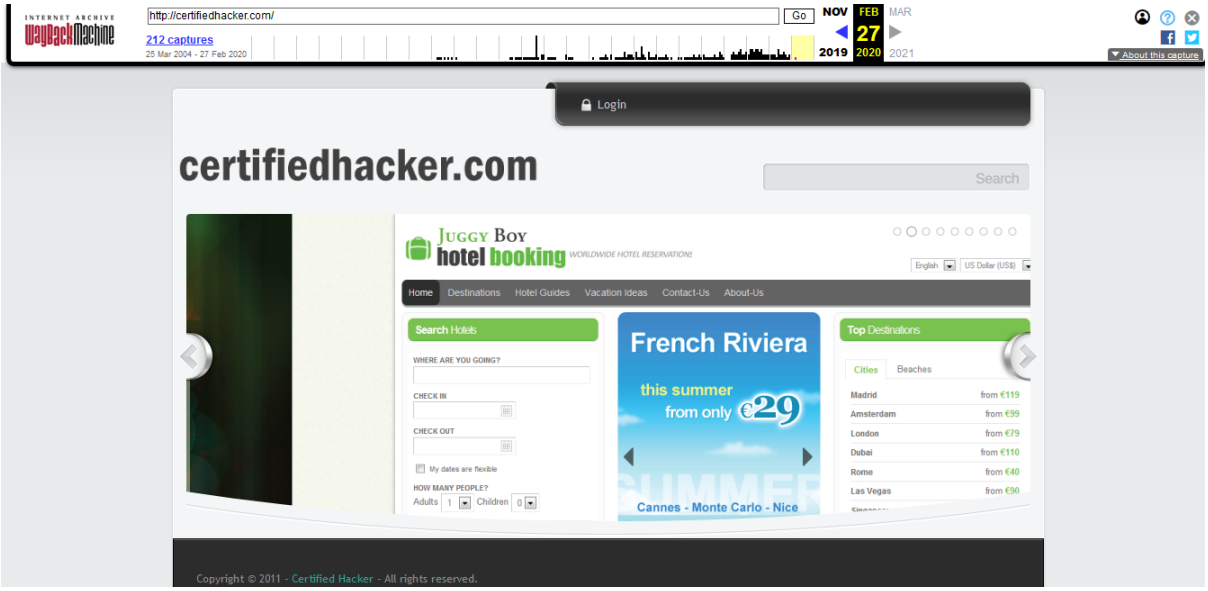
1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 **2020**

JAN							FEB							MAR							APR						
			1	2	3	4							1	1	2	3	4	5	6	7				1	2	3	4
5	6	7	8	9	10	11	2	3	4	5	6	7	8	8	9	10	11	12	13	14	5	6	7	8	9	10	11
12	13	14	15	16	17	18	9	10	11	12	13	14	15	15	16	17	18	19	20	21	12	13	14	15	16	17	18
19	20	21	22	23	24	25	16	17	18	19	20	21	22	22	23	24	25	26	27	28	19	20	21	22	23	24	25
26	27	28	29	30	31		23	24	25	26	27	28	29	29	30	31					26	27	28	29	30		

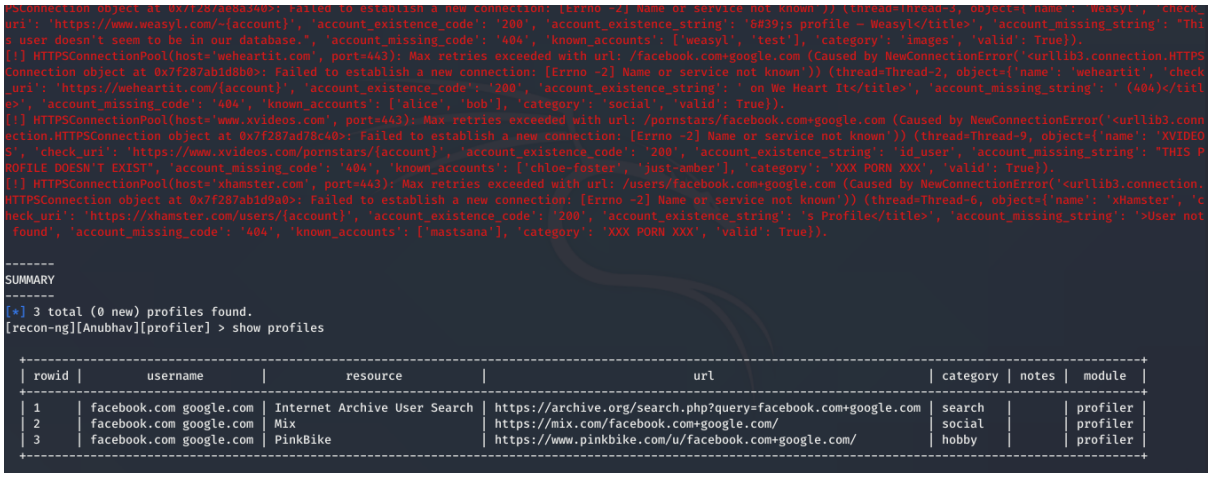
MAY							JUN							JUL							AUG						
					1	2		1	2	3	4	5	6				1	2	3	4							1
3	4	5	6	7	8	9	7	8	9	10	11	12	13	5	6	7	8	9	10	11	2	3	4	5	6	7	8
10	11	12	13	14	15	16	14	15	16	17	18	19	20	12	13	14	15	16	17	18	9	10	11	12	13	14	15
17	18	19	20	21	22	23	21	22	23	24	25	26	27	19	20	21	22	23	24	25	16	17	18	19	20	21	22
24	25	26	27	28	29	30	28	29	30					26	27	28	29	30	31		23	24	25	26	27	28	29
31																					30	31					


https://web.archive.org/web/20080113035723/http://certifiedhacker.com/
http://certifiedhacker.com/
Go
212 captures
25 Mar 2004 - 27 Feb 2020
NOV
JAN
MAR
13
2005
2008
2009
About this capture
CEH
Certified Ethical Hacker
Ethical Hacking
and Countermeasures
http://www.eccouncil.org
EC-Council


https://web.archive.org/web/20110814120054/http://www.certifiedhacker.com/
http://www.certifiedhacker.com/
Go
212 captures
25 Mar 2004 - 27 Feb 2020
JUN
AUG
SEP
14
2010
2011
2012
About this capture
Login
certifiedhacker.com
Search
JuggyBoy
Corporate.web
Learning Resources
Homepage
About us
Services
Articles
FAQ
Support
Contact us
Welcome to our website
Corporate learning resources has never been closer to the rest of the world. Online communications and advances in international transport mean local institutions and industries can easily participate in world markets. Our passion for experiencing other cultures and countries has earned the reputation of being best.
Vision :
This innovative thinking is reflected in the way we teach and learn. Our education system encourages inventive thinking and teaching techniques that reach far
Most popular schools
USA
Charter School
more details
California
High School
Copyright © 2011 - Certified Hacker - All rights reserved.



- **E-mail id of some employee or contacts and profiles related to that website using Kali linux recon-ng tool.**



```
PSConnection object at 0x7f287aeba340>: Failed to establish a new connection: [Errno -2] Name or service not known')) (thread=Thread-3, object={'name': 'weasyl', 'check_
uri': 'https://www.weasyl.com/~{account}', 'account_existence_code': '200', 'account_existence_string': '&#39;s profile — Weasyl</title>', 'account_missing_string': "Thi
s user doesn't seem to be in our database.", 'account_missing_code': '404', 'known_accounts': ['weasyl', 'test'], 'category': 'images', 'valid': True}).
[!] HTTPSConnectionPool(host='weheartit.com', port=443): Max retries exceeded with url: /facebook.com+google.com (Caused by NewConnectionError('<urllib3.connection.HTTPS
Connection object at 0x7f287ab1d8b0>: Failed to establish a new connection: [Errno -2] Name or service not known')) (thread=Thread-2, object={'name': 'weheartit', 'check
_uri': 'https://weheartit.com/{account}', 'account_existence_code': '200', 'account_existence_string': ' on We Heart It</title>', 'account_missing_string': ' (404)</titl
e>', 'account_missing_code': '404', 'known_accounts': ['alice', 'bob'], 'category': 'social', 'valid': True}).
[!] HTTPSConnectionPool(host='www.xvideos.com', port=443): Max retries exceeded with url: /pornstars/facebook.com+google.com (Caused by NewConnectionError('<urllib3.conn
ection.HTTPSConnection object at 0x7f287ad78c40>: Failed to establish a new connection: [Errno -2] Name or service not known')) (thread=Thread-9, object={'name': 'XVIDEO
S', 'check_uri': 'https://www.xvideos.com/pornstars/{account}', 'account_existence_code': '200', 'account_existence_string': 'id_user', 'account_missing_string': "THIS P
ROFILE DOESN'T EXIST", 'account_missing_code': '404', 'known_accounts': ['chloe-foster', 'just-amber'], 'category': 'XXX PORN XXX', 'valid': True}).
[!] HTTPSConnectionPool(host='xhamster.com', port=443): Max retries exceeded with url: /users/facebook.com+google.com (Caused by NewConnectionError('<urllib3.connection.
HTTPSConnection object at 0x7f287ab1d9a0>: Failed to establish a new connection: [Errno -2] Name or service not known')) (thread=Thread-6, object={'name': 'xHamster', 'c
heck_uri': 'https://xhamster.com/users/{account}', 'account_existence_code': '200', 'account_existence_string': 's Profile</title>', 'account_missing_string': '>User not
 found', 'account_missing_code': '404', 'known_accounts': ['mastsana'], 'category': 'XXX PORN XXX', 'valid': True}).

-------
SUMMARY
-------
[*] 3 total (0 new) profiles found.
[recon-ng][Anubhav][profiler] > show profiles

  +-----------------------------------------------------------------------------------------------------------------------------------------+
  | rowid |         username         |          resource          |                          url                          | category | notes |  module  |
  +-----------------------------------------------------------------------------------------------------------------------------------------+
  | 1     | facebook.com google.com | Internet Archive User Search | https://archive.org/search.php?query=facebook.com+google.com | search   |       | profiler |
  | 2     | facebook.com google.com | Mix                          | https://mix.com/facebook.com+google.com/                     | social   |       | profiler |
  | 3     | facebook.com google.com | PinkBike                     | https://www.pinkbike.com/u/facebook.com+google.com/          | hobby    |       | profiler |
  +-----------------------------------------------------------------------------------------------------------------------------------------+
```

```
[recon-ng][Anubhav][whois_pocs] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][Anubhav][whois_pocs] > info

      Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
  'contacts' table with the results.

Options:
  Name    Current Value        Required  Description
  ------  -------------        --------  -----------
  SOURCE  certifiedhacker.com  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][Anubhav][whois_pocs] > run

------------------
CERTIFIEDHACKER.COM
------------------
[*] URL: http://whois.arin.net/rest/pocs;domain=certifiedhacker.com
[*] No contacts found.
[recon-ng][Anubhav][whois_pocs] > modules load recons
```

- **Checking the open ports of the website using the dmitry tool in kali linux**

```
root@kali:~# dmitry -p -f certifiedhacker.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:162.241.216.11
HostName:certifiedhacker.com

Gathered TCP Port information for 162.241.216.11
---------------------------------

 Port           State

21/tcp          open
22/tcp          open
25/tcp          open
26/tcp          open
53/tcp          open
80/tcp          open
110/tcp         open
143/tcp         open

Portscan Finished: Scanned 150 ports, 141 ports were in state closed


All scans completed, exiting
root@kali:~#
```

More details about DNS and Domain by Dmitry .

```
root@kali:~# dmitry -w -f -p certifiedhacker.com -o host.txt
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to 'host.txt.txt'

HostIP:162.241.216.11
HostName:certifiedhacker.com

Gathered Inic-whois information for certifiedhacker.com
---------------------------------
   Domain Name: CERTIFIEDHACKER.COM
   Registry Domain ID: 88849376_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2016-03-16T12:38:41Z
   Creation Date: 2002-07-30T00:32:00Z
   Registry Expiry Date: 2021-07-30T00:32:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-06-17T07:58:05Z <<<
```

Using the OSR framework to find some more information about that website using the command of usufy on klai linux .

```
Coded with ♥ by Yaiza Rubio & Félix Brezo

 -- With 'phonefy' you can guess if a given phone number is linked to spam. --

      Usufy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2020

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

2020-06-17 04:32:13.563452      Starting search in 3 platform(s)... Relax!

        Press <Ctrl + C> to stop...
```

```
orted.
  warnings.warn(
Objects recovered (2020-6-17_4h36m).:
+-----------------------------------------------------+-------------------+----------------------+
|                  com.i3visio.URI                    | com.i3visio.Alias | com.i3visio.Platform |
+=====================================================+===================+======================+
| http://twitter.com/certifiedhacker                  | certifiedhacker   | Twitter              |
+-----------------------------------------------------+-------------------+----------------------+
| https://www.youtube.com/user/certifiedhacker/about  | certifiedhacker   | Youtube              |
+-----------------------------------------------------+-------------------+----------------------+
| http://www.instagram.com/certifiedhacker            | certifiedhacker   | Instagram            |
+-----------------------------------------------------+-------------------+----------------------+

2020-06-17 04:36:38.706640      You can find all the information here:
        ./profiles.csv

2020-06-17 04:36:38.706920      Finishing execution...

Total time consumed:    0:04:25.143468
Average seconds/query:  88.38115599999999 seconds


Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
    https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

```
  warnings.warn(
Objects recovered (2020-6-17_5h20m).:
+----------------------+-------------------+-----------------------------------------------------+
| com.i3visio.Platform | com.i3visio.Alias |                   com.i3visio.URI                   |
+======================+===================+=====================================================+
| Youtube              | CertifiedxHacker  | https://www.youtube.com/user/CertifiedxHacker/about |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | MrPanthers893417  | https://www.youtube.com/user/MrPanthers893417/about |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | IanTraceur5       | https://www.youtube.com/user/IanTraceur5/about      |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | RobsTechTips      | https://www.youtube.com/user/RobsTechTips/about     |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | dtwazere          | https://www.youtube.com/user/dtwazere/about         |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | starduel          | https://www.youtube.com/user/starduel/about         |
+----------------------+-------------------+-----------------------------------------------------+
| Youtube              | chinmaybhat123    | https://www.youtube.com/user/chinmaybhat123/about   |
+----------------------+-------------------+-----------------------------------------------------+

2020-06-17 05:20:33.270234      You can find all the information collected in the following files:
        ./profiles.csv

2020-06-17 05:20:33.270508      Finishing execution...

Total time used:        0:32:49.829591
Average seconds/query:  1969.829591 seconds


Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
```

- **Checking for load balancer on the website certified hacker**

```
root@kali: ~        root@kali: ~        root@kali: ~

root@kali:~# lbd certifiedhacker.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.


Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 Apache
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 09:10:37, 09:10:38, 09:10:38, 09:10:39, 09:10:40, 09:10:41, 09:10:41, 09:10:42, 09:10:43, 09:10:44, 09:10:45, 09:10:45, 09:10:46,
 09:10:47, 09:10:48, 09:10:49, 09:10:50, 09:10:51, 09:10:52, 09:10:53, 09:10:54, 09:10:54, 09:10:55, 09:10:56, 09:10:57, 09:10:58, 09:10:58, 09:11:00, 09:11:01, 09:11:01
, 09:11:02, 09:11:03, 09:11:04, 09:11:05, 09:11:06, 09:11:07, 09:11:08, 09:11:09, 09:11:10, 09:11:10, 09:11:11, 09:11:12, 09:11:13, 09:11:14, 09:11:15, 09:11:16, 09:11:1
7, 09:11:17, 09:11:18, 09:11:19, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

certifiedhacker.com does NOT use Load-balancing.
```

By using the lbd command in kali linux terminal

- **Checking firewall at the website using wafw00f tool**

```
root@kali: ~
bash: waf00f: command not found
root@kali:~# wafw00f http://certifiedhacker.com/

                    ______
                   /      \
                  (  W00f! )
                   \  ____/
                   ,,    __           404 Hack Not Found
              |`-.__   / /                    __     __
              /"  _/  /_/                     \ \   / /
             *====*    /                       \ \_/ /  405 Not Allowed
            /     )__//                         \   /
       /|  /     /---`                      403 Forbidden
       \\/`   \ |                                / _ \
       `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
         `    ``_`                              /_/   \_\
         -----

                         ~ WAFW00F : v2.1.0 ~
          The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://certifiedhacker.com/
[+] The site http://certifiedhacker.com/ is behind ModSecurity (SpiderLabs) WAF.
[~] Number of requests: 2
root@kali:~#
```

```
root@kali:~# wafw00f -a -v  http://certifiedhacker.com/

                    ______
                   /      \
                  (  W00f! )
                   \  ____/
                   ,,    __           404 Hack Not Found
              |`-.__   / /                    __     __
              /"  _/  /_/                     \ \   / /
             *====*    /                       \ \_/ /  405 Not Allowed
            /     )__//                         \   /
       /|  /     /---`                      403 Forbidden
       \\/`   \ |                                / _ \
       `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
         `    ``_`                              /_/   \_\
         -----

                         ~ WAFW00F : v2.1.0 ~
          The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://certifiedhacker.com/
[+] The site http://certifiedhacker.com/ is behind ModSecurity (SpiderLabs) WAF.
[+] Generic Detection results:
[*] The site http://certifiedhacker.com/ seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "406"
[~] Number of requests: 5
```

- **Using Who.is for getting the registrar information and other information regarding the website certifiedhacker.com**

certifiedhacker.com

whois information

Whois | DNS Records | Diagnostics

cache expires in 23 hours, 55 minutes and 25 seconds

Registrar Info	
Name	Network Solutions, LLC
Whois Server	whois.networksolutions.com
Referral URL	http://networksolutions.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates	
Expires On	2021-07-30
Registered On	2002-07-30
Updated On	2019-08-22

- **Information regarding the name servers and similar domains.**

Name Servers	
NS1.BLUEHOST.COM	162.159.24.80
NS2.BLUEHOST.COM	162.159.25.175

Similar Domains

certi-5oils.com | certi-air.eu | certi-api.org | certi-box.com | certi-bru.com | certi-bruxelles.net | certi-buy.com | certi-cable-1.com | certi-call.com | certi-camp.com | certi-camp.net | certi-car.com | certi-car.net | certi-care.com | certi-cares.com | certi-cars.com | certi-cast.com | certi-chain.com | certi-chef.com | certi-clean.com |

- **Registrar Information**

Registrar Data

We will display stored WHOIS data for up to 30 days.

Make Private Now

Registrant Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	nd2re72e6jz@networksolutionsprivateregistration.com

Administrative Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	nd2re72e6jz@networksolutionsprivateregistration.com

Technical Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	5335 Gate Parkway care of Network Solutions PO Box 459
City	Jacksonville
State / Province	FL
Postal Code	32256
Country	US
Phone	+1.5707088780
Email	nd2re72e6jz@networksolutionsprivateregistration.com