Week 16 Homework Submission File: Penetration Testing 1

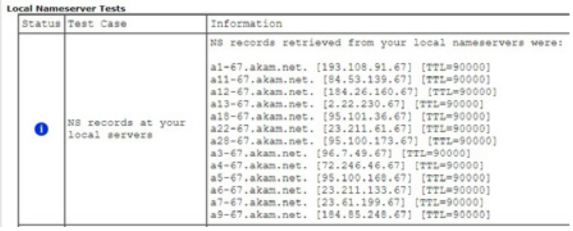
Step 1: Google Dorking

- Using Google, can you identify who the Chief Executive Officer of Altoro Mutual is: `Karl Fitzgerald`
- How can this information be helpful to an attacker: `This can be helpful to an attacker to do Spear Phishing, especially Whaling the CEO`

Step 2: DNS and Domain Discovery

Enter the IP address for `demo.testfire.net` into Domain Dossier and answer the following questions based on the results:

1. Where is the company located: `Sunnyvale, CA 94085`
2. What is the NetRange IP address: `NetRange: 65.61.137.64 - 65.61.137.127`
3. What is the company they use to store their infrastructure: `Rackspace Backbone Engineering`
4. What is the IP address of the DNS server: ----------> `*See Screenshots in appended pages`



Local Nameserver Tests

Status	Test Case	Information
●	NS records at your local servers	NS records retrieved from your local nameservers were: a1-67.akam.net. [193.108.91.67] [TTL=90000] a11-67.akam.net. [84.53.139.67] [TTL=90000] a12-67.akam.net. [184.26.160.67] [TTL=90000] a13-67.akam.net. [2.22.230.67] [TTL=90000] a18-67.akam.net. [95.101.36.67] [TTL=90000] a22-67.akam.net. [23.211.61.67] [TTL=90000] a28-67.akam.net. [95.100.173.67] [TTL=90000] a3-67.akam.net. [96.7.49.67] [TTL=90000] a4-67.akam.net. [72.246.46.67] [TTL=90000] a5-67.akam.net. [95.100.168.67] [TTL=90000] a6-67.akam.net. [23.211.133.67] [TTL=90000] a7-67.akam.net. [23.61.199.67] [TTL=90000] a9-67.akam.net. [184.85.248.67] [TTL=90000]

Step 3: Shodan

- What open ports and running services did Shodan find: `Open Ports: 80, 443, 8080`

Step 4: Recon-ng

- Install the Recon module `xssed`.
- Set the source to `demo.testfire.net`. `*See Screenshots in appended pages`
- Run the module.

Is Altoro Mutual vulnerable to XSS: `Yes, they are!`

Step 5: Zenmap

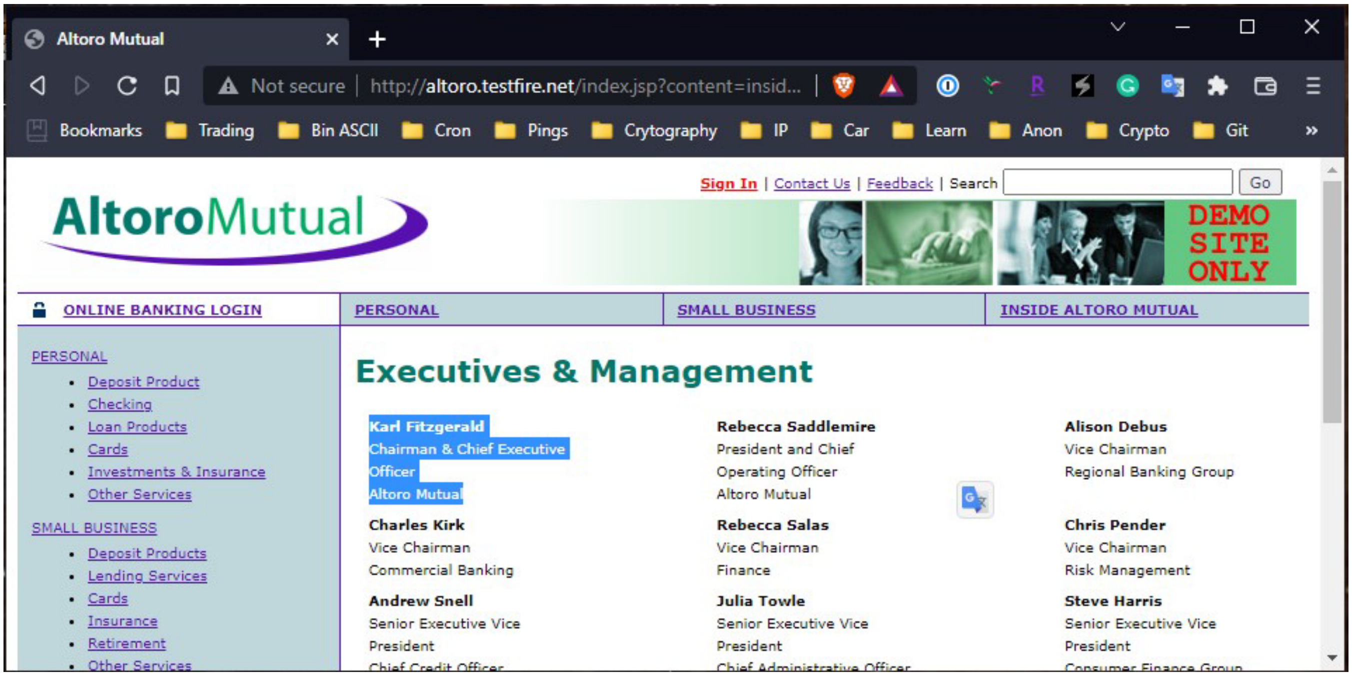
Your client has asked that you help identify any vulnerabilities with their file-sharing server.

Using the Metasploitable machine to act as your client's server, complete the following:

- Command for Zenmap to run a service scan against the Metasploitable machine:
  `nmap -v 192.168.0.10`
- Bonus command to output results into a new text file named `zenmapscan.txt` :
  `nmap -v -oN zenmapscan.txt 192.168.0.10`
- Zenmap vulnerability script command:
  `nmap -v -oN zenmapscan.txt --script samba-vuln-cve-2012-1182 192.168.0.10`
- Once you have identified this vulnerability, answer the following questions for your client:

1. What is the vulnerability: This vulnerability in the Samba software service that allows remote code execution as the “root” user from an annonymous connection.
2. Why is it dangerous: This is dangerous because it allows an unathenticated connection to the server with “root” priveleges for an annoymous user to control the entire system.
3. What mitigation strategies can you recommendations for the client to protect their server: A mitigation strategy for this vulnerability is to update and patch any Samba software versions 3.6.3 and previous immediately. Another is to disable to service completely if it is not something that is needed or used by the organization.

Appendix 1 - Google Dorking Screenshots



PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

Executives & Management

Karl Fitzgerald
Chairman & Chief Executive
Officer
Altoro Mutual

Rebecca Saddlemire
President and Chief
Operating Officer
Altoro Mutual

Alison Debus
Vice Chairman
Regional Banking Group

Charles Kirk
Vice Chairman
Commercial Banking

Rebecca Salas
Vice Chairman
Finance

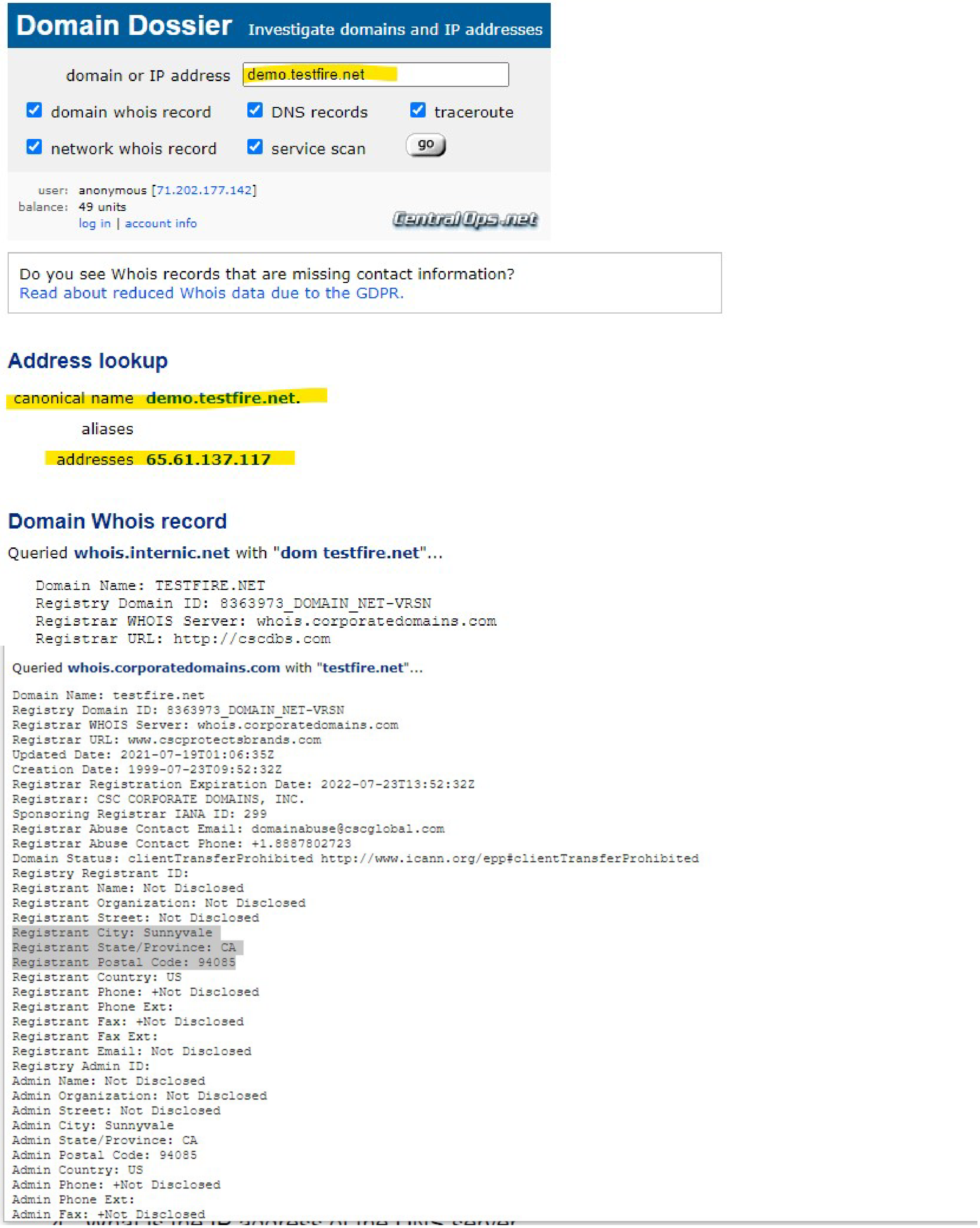
Chris Pender
Vice Chairman
Risk Management

Andrew Snell
Senior Executive Vice
President
Chief Credit Officer

Julia Towle
Senior Executive Vice
President
Chief Administrative Officer

Steve Harris
Senior Executive Vice
President
Consumer Finance Group

Appendix 2 - DNS and Domain Discovery Screenshots



domain or IP address demo.testfire.net

☑ domain whois record ☑ DNS records ☑ traceroute

☑ network whois record ☑ service scan

user: anonymous [71.202.177.142]
balance: 49 units
log in | account info

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name demo.testfire.net.

aliases

addresses 65.61.137.117

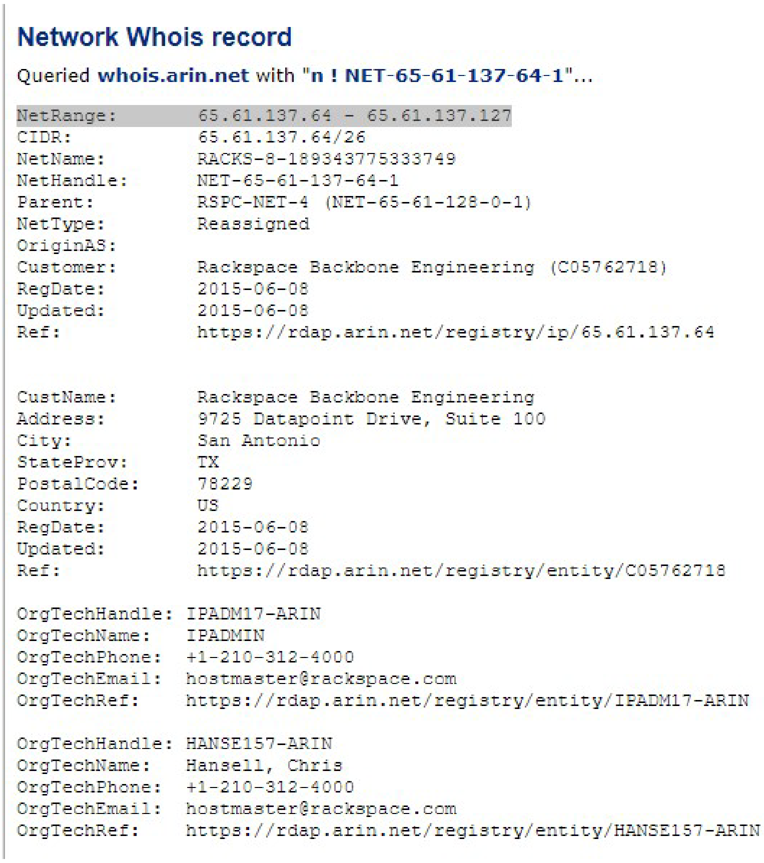
Domain Whois record

Queried **whois.internic.net** with "**dom testfire.net**"...

```
Domain Name: TESTFIRE.NET
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
```

Queried **whois.corporatedomains.com** with "**testfire.net**"...

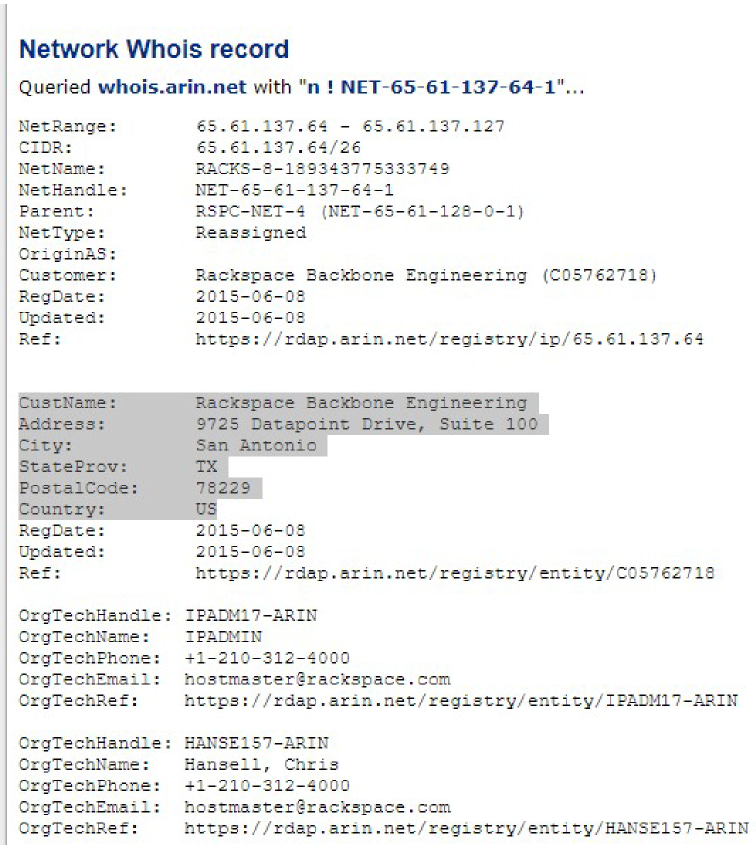
```
Domain Name: testfire.net
Registry Domain ID: 8363973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2021-07-19T01:06:35Z
Creation Date: 1999-07-23T09:52:32Z
Registrar Registration Expiration Date: 2022-07-23T13:52:32Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94085
Registrant Country: US
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
Registry Admin ID:
Admin Name: Not Disclosed
Admin Organization: Not Disclosed
Admin Street: Not Disclosed
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94085
Admin Country: US
Admin Phone: +Not Disclosed
Admin Phone Ext:
Admin Fax: +Not Disclosed
```



Network Whois record

Queried **whois.arin.net** with "**n ! NET-65-61-137-64-1**"...

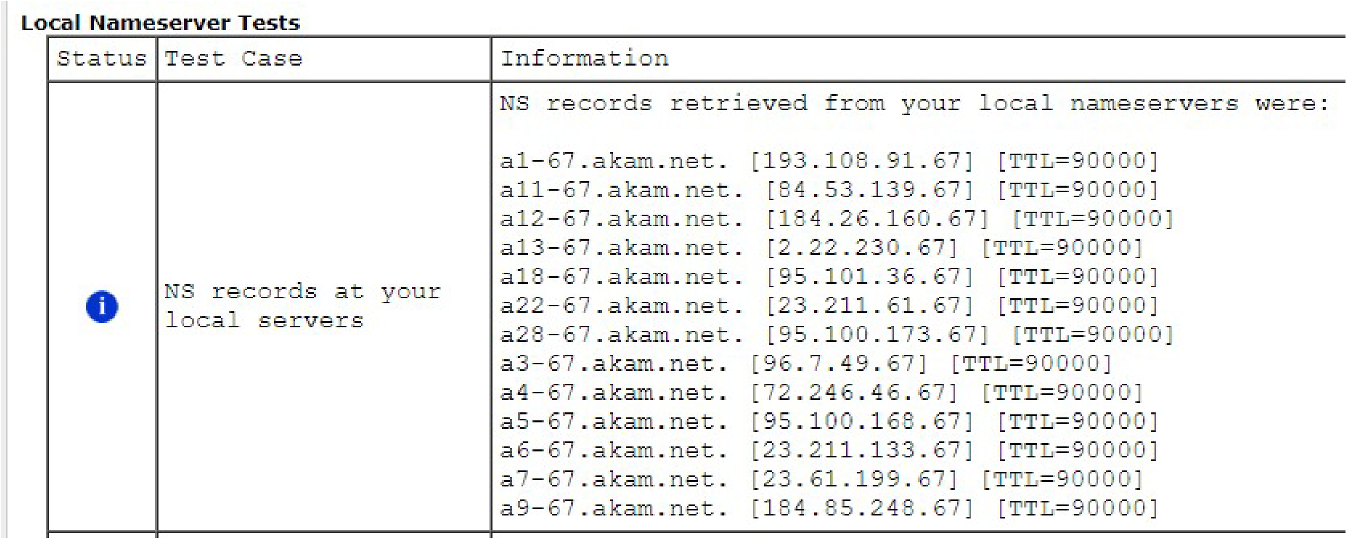
```
NetRange:       65.61.137.64 - 65.61.137.127
CIDR:           65.61.137.64/26
NetName:        RACKS-8-189343775333749
NetHandle:      NET-65-61-137-64-1
Parent:         RSPC-NET-4 (NET-65-61-128-0-1)
NetType:        Reassigned
OriginAS:
Customer:       Rackspace Backbone Engineering (C05762718)
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/ip/65.61.137.64


CustName:       Rackspace Backbone Engineering
Address:        9725 Datapoint Drive, Suite 100
City:           San Antonio
StateProv:      TX
PostalCode:     78229
Country:        US
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/entity/C05762718

OrgTechHandle: IPADM17-ARIN
OrgTechName:   IPADMIN
OrgTechPhone:  +1-210-312-4000
OrgTechEmail:  hostmaster@rackspace.com
OrgTechRef:    https://rdap.arin.net/registry/entity/IPADM17-ARIN

OrgTechHandle: HANSE157-ARIN
OrgTechName:   Hansell, Chris
OrgTechPhone:  +1-210-312-4000
OrgTechEmail:  hostmaster@rackspace.com
OrgTechRef:    https://rdap.arin.net/registry/entity/HANSE157-ARIN
```



Network Whois record

Queried **whois.arin.net** with "**n ! NET-65-61-137-64-1**"...

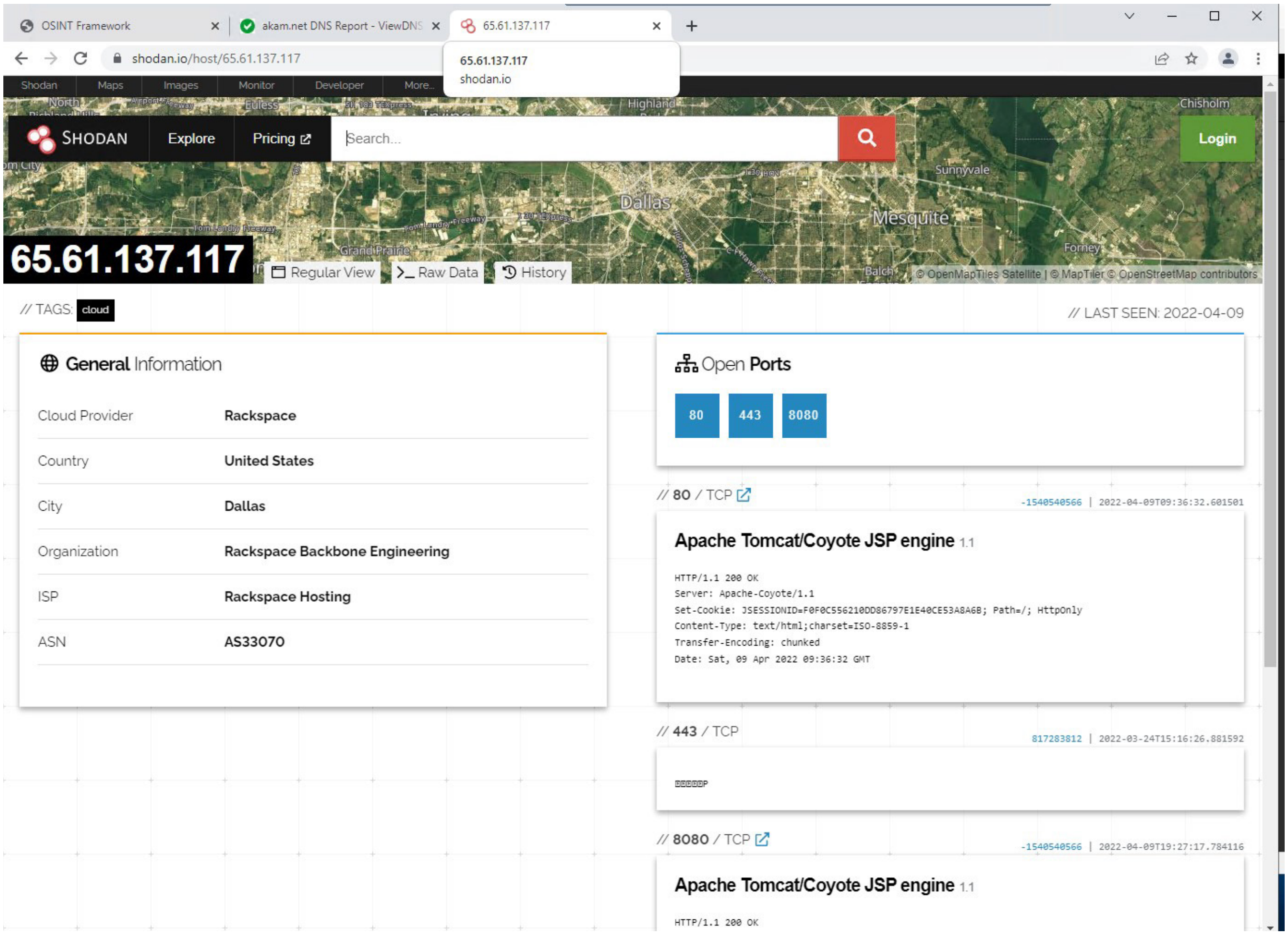
```
NetRange:       65.61.137.64 - 65.61.137.127
CIDR:           65.61.137.64/26
NetName:        RACKS-8-189343775333749
NetHandle:      NET-65-61-137-64-1
Parent:         RSPC-NET-4 (NET-65-61-128-0-1)
NetType:        Reassigned
OriginAS:
Customer:       Rackspace Backbone Engineering (C05762718)
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/ip/65.61.137.64


CustName:       Rackspace Backbone Engineering
Address:        9725 Datapoint Drive, Suite 100
City:           San Antonio
StateProv:      TX
PostalCode:     78229
Country:        US
RegDate:        2015-06-08
Updated:        2015-06-08
Ref:            https://rdap.arin.net/registry/entity/C05762718

OrgTechHandle: IPADM17-ARIN
OrgTechName:   IPADMIN
OrgTechPhone:  +1-210-312-4000
OrgTechEmail:  hostmaster@rackspace.com
OrgTechRef:    https://rdap.arin.net/registry/entity/IPADM17-ARIN

OrgTechHandle: HANSE157-ARIN
OrgTechName:   Hansell, Chris
OrgTechPhone:  +1-210-312-4000
OrgTechEmail:  hostmaster@rackspace.com
OrgTechRef:    https://rdap.arin.net/registry/entity/HANSE157-ARIN
```



Local Nameserver Tests

Status	Test Case	Information
ⓘ	NS records at your local servers	NS records retrieved from your local nameservers were: a1-67.akam.net. [193.108.91.67] [TTL=90000] a11-67.akam.net. [84.53.139.67] [TTL=90000] a12-67.akam.net. [184.26.160.67] [TTL=90000] a13-67.akam.net. [2.22.230.67] [TTL=90000] a18-67.akam.net. [95.101.36.67] [TTL=90000] a22-67.akam.net. [23.211.61.67] [TTL=90000] a28-67.akam.net. [95.100.173.67] [TTL=90000] a3-67.akam.net. [96.7.49.67] [TTL=90000] a4-67.akam.net. [72.246.46.67] [TTL=90000] a5-67.akam.net. [95.100.168.67] [TTL=90000] a6-67.akam.net. [23.211.133.67] [TTL=90000] a7-67.akam.net. [23.61.199.67] [TTL=90000] a9-67.akam.net. [184.85.248.67] [TTL=90000]

Appendix 3 - Shodan Screenshots



65.61.137.117

// TAGS: cloud

// LAST SEEN: 2022-04-09

General Information

Cloud Provider	Rackspace
Country	United States
City	Dallas
Organization	Rackspace Backbone Engineering
ISP	Rackspace Hosting
ASN	AS33070

Open Ports

80 443 8080

// 80 / TCP — -1540540566 | 2022-04-09T09:36:32.601501

Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=F0F0C556210DD86797E1E40CE53A8A6B; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sat, 09 Apr 2022 09:36:32 GMT
```

// 443 / TCP — 817283812 | 2022-03-24T15:16:26.881592

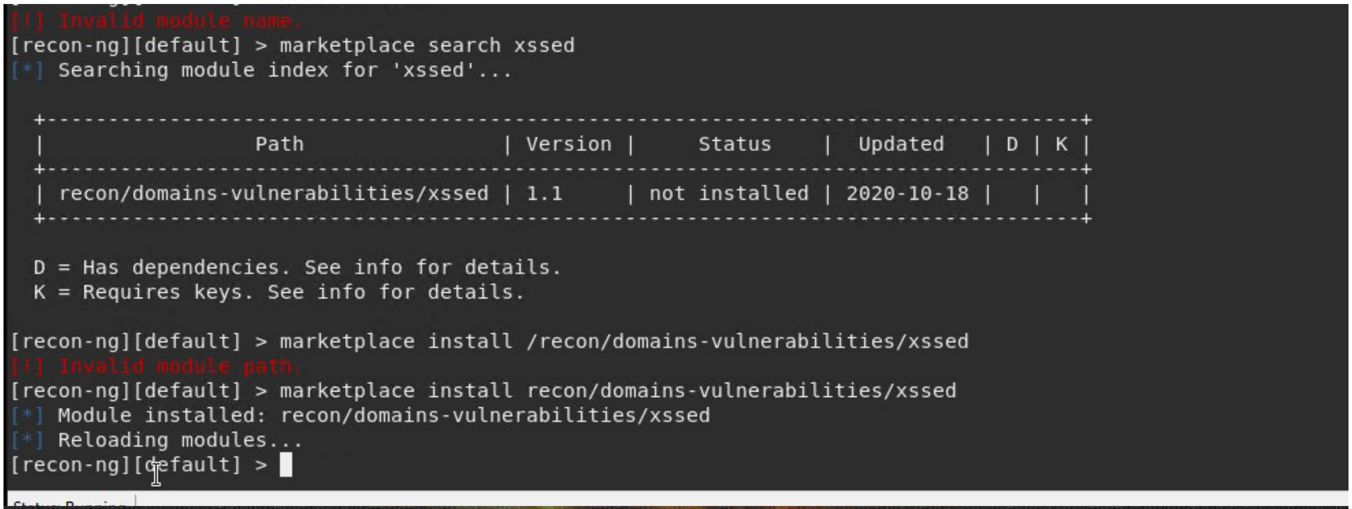
```
□□□□□P
```

// 8080 / TCP — -1540540566 | 2022-04-09T19:27:17.784116

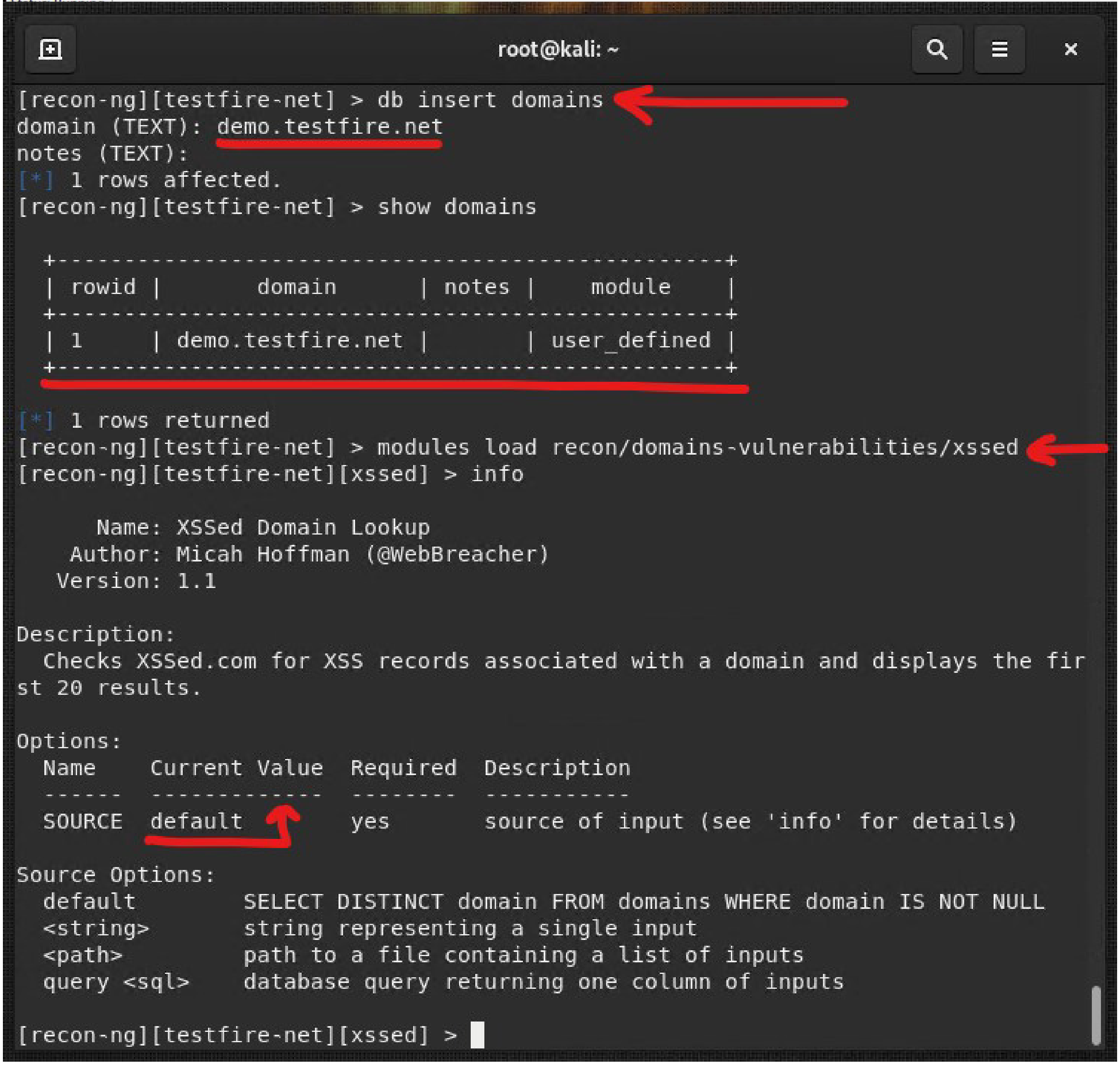
Apache Tomcat/Coyote JSP engine 1.1

```
HTTP/1.1 200 OK
```

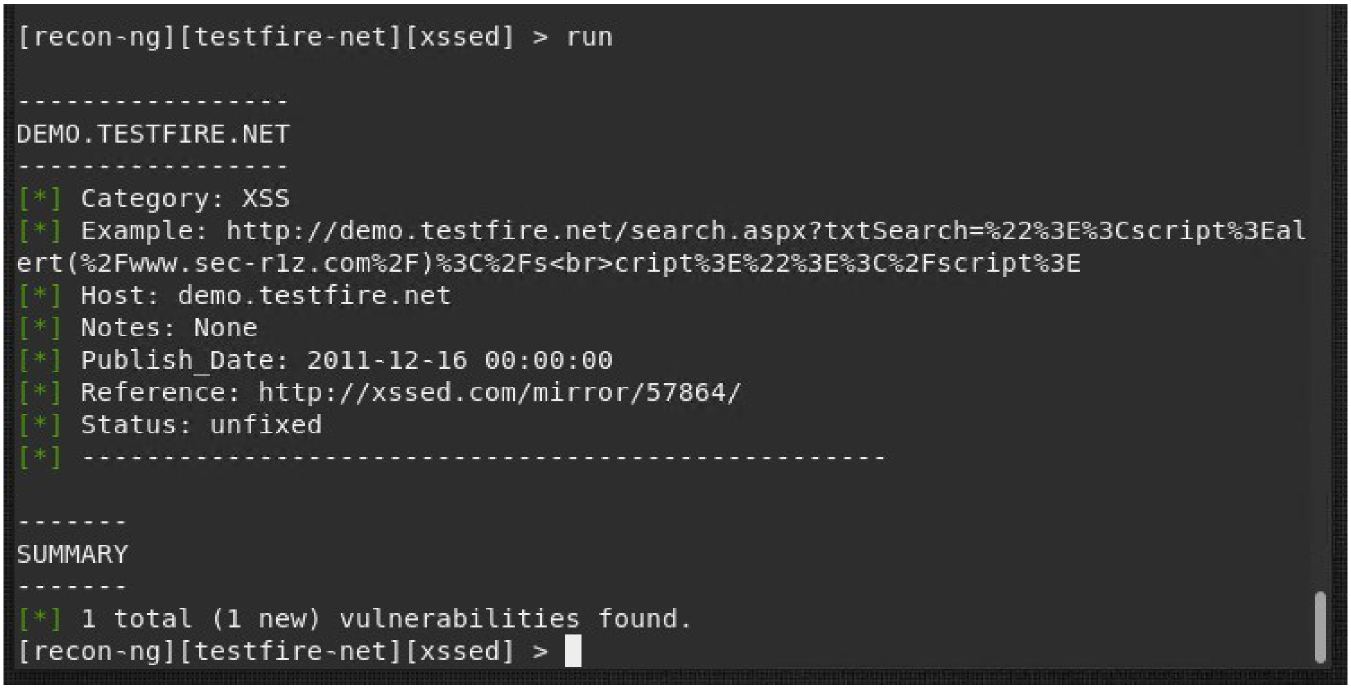
Appendix 4 - Recon-ng Screenshots



```
[!] Invalid module name.
[recon-ng][default] > marketplace search xssed
[*] Searching module index for 'xssed'...

  +---------------------------------------------------------------------------------+
  |                Path                | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------+
  | recon/domains-vulnerabilities/xssed | 1.1     | not installed | 2020-10-18 |   |   |
  +---------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > marketplace install /recon/domains-vulnerabilities/xssed
[!] Invalid module path.
[recon-ng][default] > marketplace install recon/domains-vulnerabilities/xssed
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Reloading modules...
[recon-ng][default] > 
```

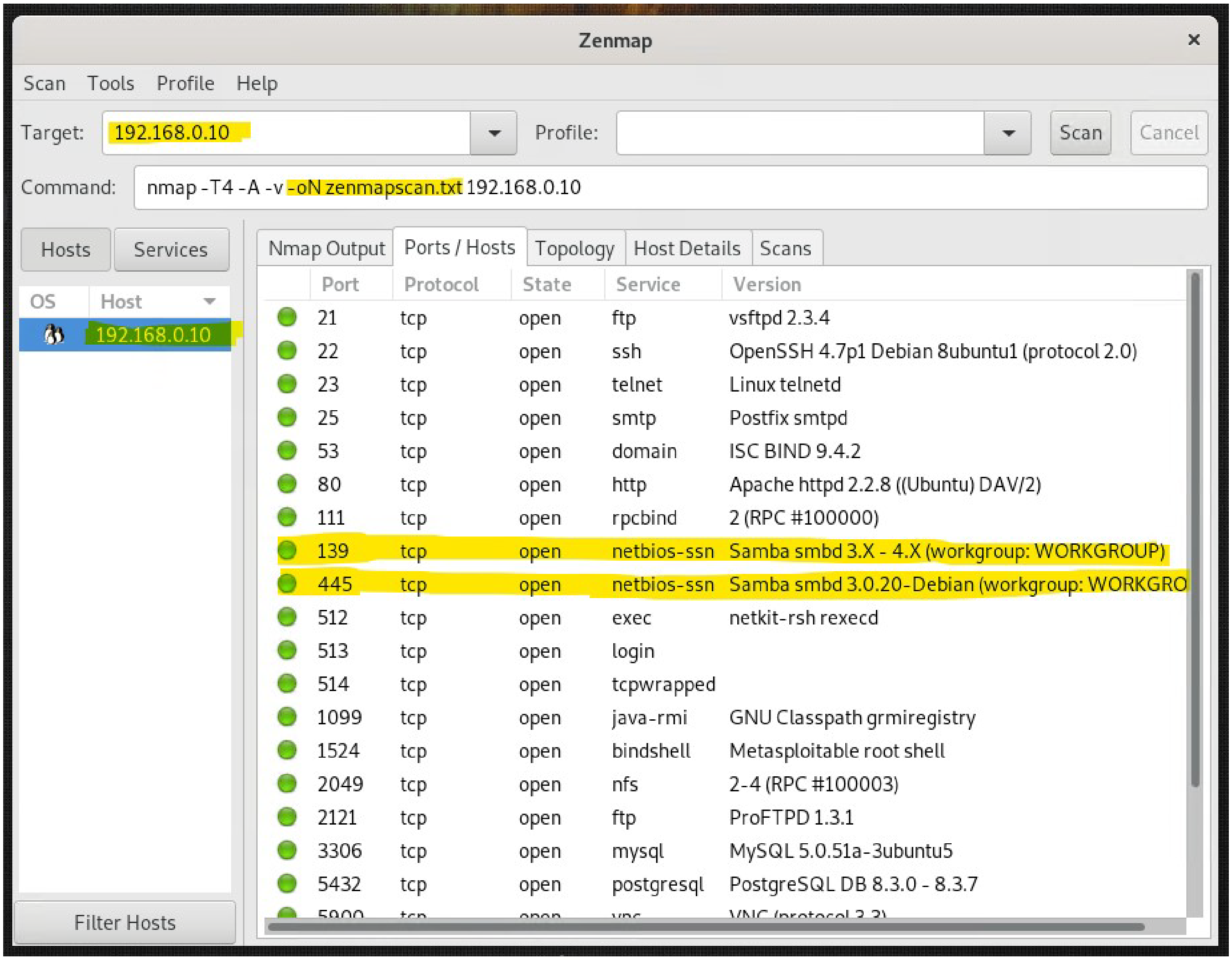


```
[recon-ng][testfire-net] > db insert domains
domain (TEXT): demo.testfire.net
notes (TEXT):
[*] 1 rows affected.
[recon-ng][testfire-net] > show domains

  +---------------------------------------------------+
  | rowid |        domain       | notes |    module    |
  +---------------------------------------------------+
  | 1     | demo.testfire.net |       | user_defined |
  +---------------------------------------------------+

[*] 1 rows returned
[recon-ng][testfire-net] > modules load recon/domains-vulnerabilities/xssed
[recon-ng][testfire-net][xssed] > info

      Name: XSSed Domain Lookup
    Author: Micah Hoffman (@WebBreacher)
   Version: 1.1

Description:
  Checks XSSed.com for XSS records associated with a domain and displays the fir
st 20 results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        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][testfire-net][xssed] > 
```



```
[recon-ng][testfire-net][xssed] > run

-----------------
DEMO.TESTFIRE.NET
-----------------
[*] Category: XSS
[*] Example: http://demo.testfire.net/search.aspx?txtSearch=%22%3E%3Cscript%3Eal
ert(%2Fwww.sec-r1z.com%2F)%3C%2Fs<br>cript%3E%22%3E%3C%2Fscript%3E
[*] Host: demo.testfire.net
[*] Notes: None
[*] Publish_Date: 2011-12-16 00:00:00
[*] Reference: http://xssed.com/mirror/57864/
[*] Status: unfixed
[*] --------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (1 new) vulnerabilities found.
[recon-ng][testfire-net][xssed] >
```

Appendix 5 - Zenmap Screenshots



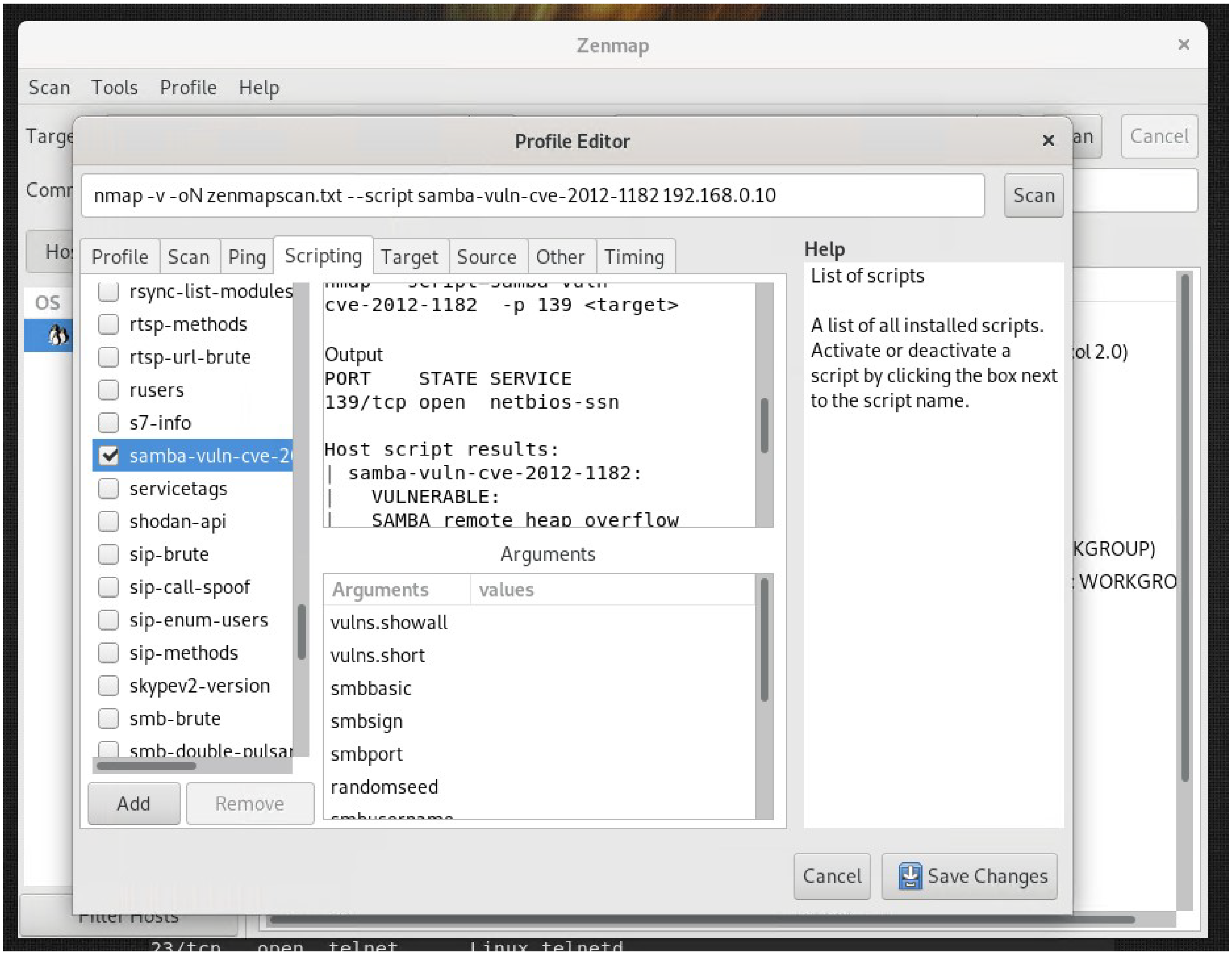
Target: 192.168.0.10

Profile:

Command: nmap -T4 -A -v -oN zenmapscan.txt 192.168.0.10

Host: 192.168.0.10

	Port	Protocol	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 3.0.20-Debian (workgroup: WORKGRO
●	512	tcp	open	exec	netkit-rsh rexecd
●	513	tcp	open	login	
●	514	tcp	open	tcpwrapped	
●	1099	tcp	open	java-rmi	GNU Classpath grmiregistry
●	1524	tcp	open	bindshell	Metasploitable root shell
●	2049	tcp	open	nfs	2-4 (RPC #100003)
●	2121	tcp	open	ftp	ProFTPD 1.3.1
●	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)



```
nmap -v -oN zenmapscan.txt --script samba-vuln-cve-2012-1182 192.168.0.10
```

- ☐ rsync-list-modules
- ☐ rtsp-methods
- ☐ rtsp-url-brute
- ☐ rusers
- ☐ s7-info
- ☑ samba-vuln-cve-2
- ☐ servicetags
- ☐ shodan-api
- ☐ sip-brute
- ☐ sip-call-spoof
- ☐ sip-enum-users
- ☐ sip-methods
- ☐ skypev2-version
- ☐ smb-brute
- ☐ smb-double-pulsar

```
nmap --script-samba-vuln-
cve-2012-1182  -p 139 <target>

Output
PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
| samba-vuln-cve-2012-1182:
|   VULNERABLE:
|   SAMBA remote heap overflow
```

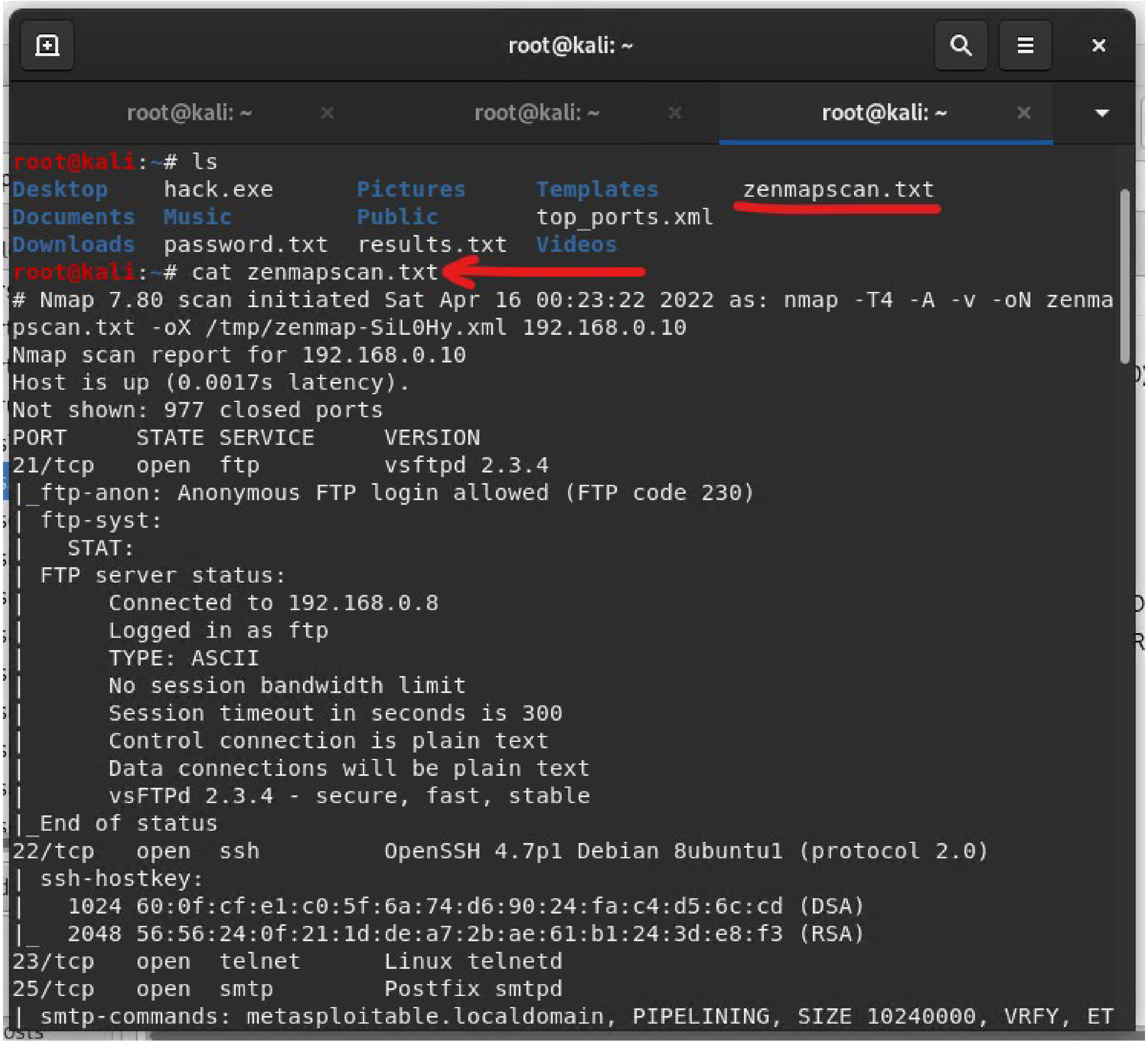
Arguments

Arguments	values
vulns.showall	
vulns.short	
smbbasic	
smbsign	
smbport	
randomseed	
smbusername	

Help

List of scripts

A list of all installed scripts. Activate or deactivate a script by clicking the box next to the script name.



```
root@kali:~# ls
Desktop    hack.exe      Pictures     Templates      zenmapscan.txt
Documents  Music         Public       top_ports.xml
Downloads  password.txt  results.txt  Videos
root@kali:~# cat zenmapscan.txt
# Nmap 7.80 scan initiated Sat Apr 16 00:23:22 2022 as: nmap -T4 -A -v -oN zenma
pscan.txt -oX /tmp/zenmap-SiL0Hy.xml 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.8
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ET
```