Reconnaissance Paper

Submitted by: Ira Tiwari

Course: Network Security Practices, Spring 2016

Executive Summary

Using the different tools specified in this document, a lot of information was found about the targeted organization, NDMC. Information about the internal workings of the organization through the documents, important contact details, e-mail addresses was found. Information about the network infrastructure, DNS lookups and IP addresses was also found. Details about monetary transactions occurring within NDMC, although old, were still available.

All the above information, when used together can be used to cause great harm by an attacker to the targeted organization. Security policies should specify how much information is publically available and employees should be made aware not to put up sensitive data on public servers. These measures may not guarantee the security of the organization, but certainly enhance it.

An introduction to the Organization: NDMC

NDMC, or the New Delhi Municipal Council is the municipal council of New Delhi. It is an urban administrative division with its own jurisdiction in a part of New Delhi. It is governed by a chairperson appointed by the government of India and also includes the Chief Minister of Delhi.

The NDMC area is approximately 16.8 square miles, a lot of it is part of “Lutyens’ Delhi”, the central area of Delhi, designed and built by the British architect, Edward Lutyens. Many of the prominent buildings and landmarks in Delhi are in this area.

The NDMC consists of 28 different departments, ranging from the Architecture department, IT department, to the Security and Training departments. They provide all these services to the residents and offices of this part of Delhi. Its headquarters are located in New Delhi.

I chose this organization because of my familiarity and closeness with it, my family (and me until last year) has resided in this area for almost 9 years now. I also chose it because it fits the criteria described, it is a small organization that is not in the Fortune 500 with an online presence, but as per my guess; lacking the resources and time to spend on reconnaissance.

Registered domains of the organization:

The domains I found until now were as follows:

ndmc.gov.in; ccb.ndmc.gov.in; ptis.ndmc.gov.in

Information gathered using various tools

1. Tool used: FOCA

How it gathers information:

Fingerprinting Organizations with Collected Archives works by first searching for and automatically downloading documents associated with an organization on Google and Bing. It then searches for “metadata” or information about the information, which may include users, creators, modifiers, paths of documents. We can also extract information about the organization’s network, servers, printers etc. using FOCA.

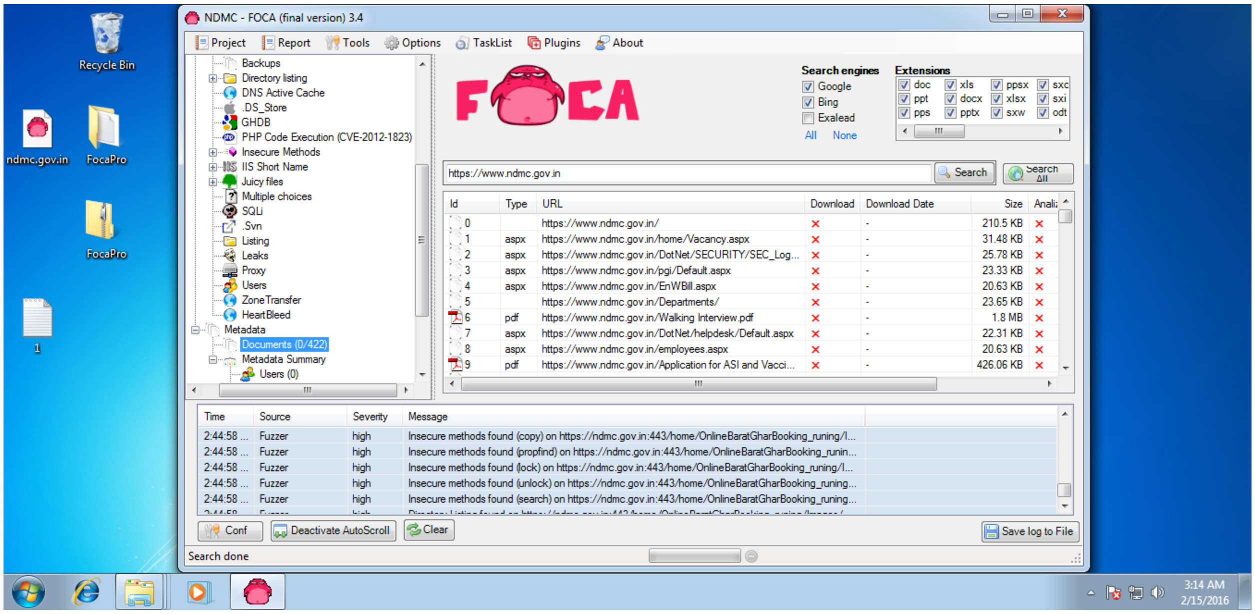
Information found:

The following were the details found through the tool:

1. Servers of the organization

2. Vulnerabilities, a vulnerability related to code execution was present

3. Metadata, 422 documents



https://www.ndmc.gov.in

Id	Type	URL	Download	Download Date	Size	Anali:
0		https://www.ndmc.gov.in/	✗	-	210.5 KB	✗
1	aspx	https://www.ndmc.gov.in/home/Vacancy.aspx	✗	-	31.48 KB	✗
2	aspx	https://www.ndmc.gov.in/DotNet/SECURITY/SEC_Log...	✗	-	25.78 KB	✗
3	aspx	https://www.ndmc.gov.in/pgi/Default.aspx	✗	-	23.33 KB	✗
4	aspx	https://www.ndmc.gov.in/EnWBill.aspx	✗	-	20.63 KB	✗
5		https://www.ndmc.gov.in/Departments/	✗	-	23.65 KB	✗
6	pdf	https://www.ndmc.gov.in/Walking Interview.pdf	✗	-	1.8 MB	✗
7	aspx	https://www.ndmc.gov.in/DotNet/helpdesk/Default.aspx	✗	-	22.31 KB	✗
8	aspx	https://www.ndmc.gov.in/employees.aspx	✗	-	20.63 KB	✗
9	pdf	https://www.ndmc.gov.in/Application for ASI and Vacci...	✗	-	426.06 KB	✗

```
Time        Source   Severity  Message
2:44:58 ... Fuzzer   high      Insecure methods found (copy) on https://ndmc.gov.in:443/home/OnlineBaratGharBooking_runing/I...
2:44:58 ... Fuzzer   high      Insecure methods found (propfind) on https://ndmc.gov.in:443/home/OnlineBaratGharBooking_runin...
2:44:58 ... Fuzzer   high      Insecure methods found (lock) on https://ndmc.gov.in:443/home/OnlineBaratGharBooking_runing/I...
2:44:58 ... Fuzzer   high      Insecure methods found (unlock) on https://ndmc.gov.in:443/home/OnlineBaratGharBooking_runing...
2:44:58 ... Fuzzer   high      Insecure methods found (search) on https://ndmc.gov.in:443/home/OnlineBaratGharBooking_runing...
```

Search done

How the information can be used by attacker

An attacker can perform active scanning once they get to know about the servers of the organization. This in turn can be used to exploit any vulnerabilities found. The vulnerability related to code execution can be utilized to perform an attack on the system. Metadata found about documents can reveal the important e-mails, e-mail formats and contact details of the organization. The attacker can use any or all of these in order to use social engineering attacks.

Suggested Controls

To avoid reconnaissance done through analyzing metadata, an organization should put policies in place as to what information can be placed in documents and on the website. Care should be taken that sensitive details such as contact information and e-mail information is not given out in a way that an attacker can use it to their advantage. Employees should also be careful not to post information about the organization on public forums which can be utilized by an attacker.

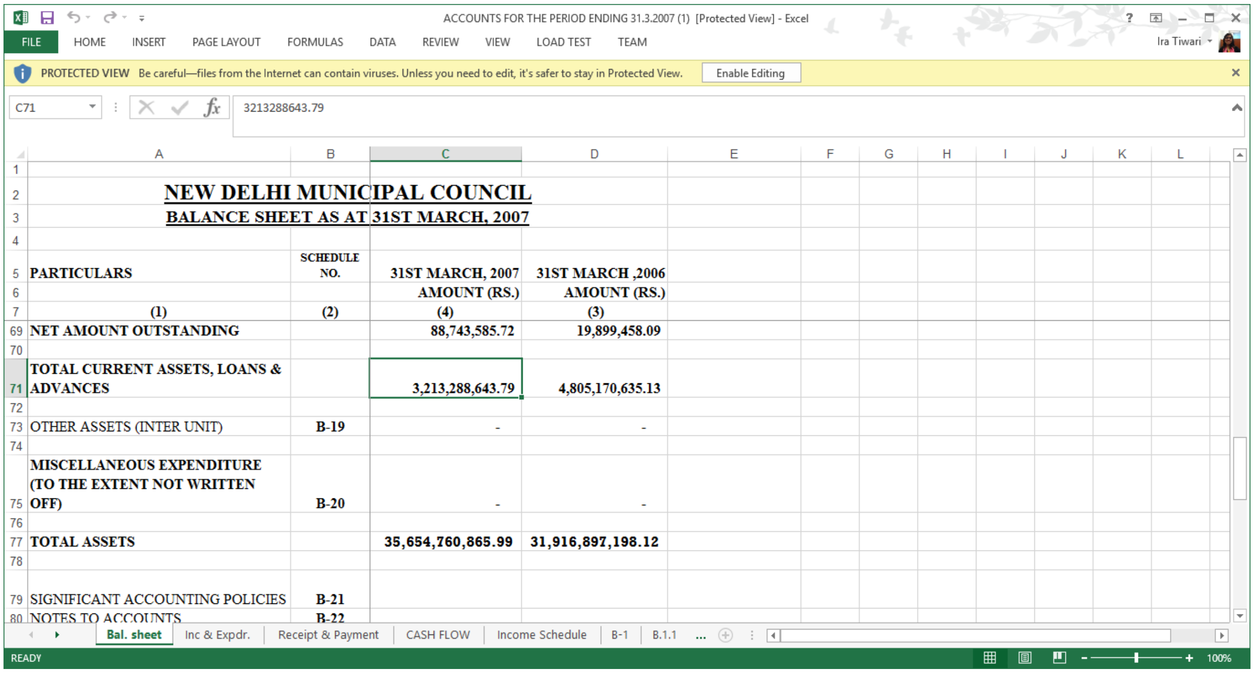
2. Tool used: Google – functions

How it gathers information

Google search has targeted functions such as “site” and “document” which when added to the search, returns more targeted results. For example typing site:neu.edu filetype: pdf will return pdf files associated with neu.edu.

Information found:

Excel sheets containing employee details, pdf documents related to NDMC were found. There were about 4000 results for the pdf documents, which included documents relating to work done by the organization. For example, construction tenders, water supply details for customers. A balance sheet containing details of funds and monetary transactions was found.



ACCOUNTS FOR THE PERIOD ENDING 31.3.2007 (1) [Protected View] - Excel

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

C71 3213288643.79

	A	B	C	D
1				
2	NEW DELHI MUNICIPAL COUNCIL			
3	BALANCE SHEET AS AT 31ST MARCH, 2007			
4				
5	PARTICULARS	SCHEDULE NO.	31ST MARCH, 2007	31ST MARCH ,2006
6			AMOUNT (RS.)	AMOUNT (RS.)
7	(1)	(2)	(4)	(3)
69	NET AMOUNT OUTSTANDING		88,743,585.72	19,899,458.09
70				
71	TOTAL CURRENT ASSETS, LOANS & ADVANCES		3,213,288,643.79	4,805,170,635.13
72				
73	OTHER ASSETS (INTER UNIT)	B-19	-	-
74				
75	MISCELLANEOUS EXPENDITURE (TO THE EXTENT NOT WRITTEN OFF)	B-20	-	-
76				
77	TOTAL ASSETS		35,654,760,865.99	31,916,897,198.12
78				
79	SIGNIFICANT ACCOUNTING POLICIES	B-21		
80	NOTES TO ACCOUNTS	B-22		

How the information can be used by an attacker

The attacker can know a lot about the internal workings of the organization using all this information. In addition to using this information for attacking via social engineering, the attacker can make up their own fake documents by noting the format in some of the search results. Depending on how much damage they want to cause, information about construction deals and tenders can be used to steal money. Information about an upcoming bid for a construction contract can be used by someone to bid to their advantage, or sabotage the bid.

Suggested Controls

The organization should have a stringent policy in place about the documents that are uploaded on the web server. Employees should not post such sensitive data anywhere on a public forum. They should take measures to remove this data and remove it from the google cache and index itself.

3. Tool used: Maltego

How it gathers information

Maltego visually demonstrates interconnected links between searched items. It provides the user with a more powerful search, giving us smarter results. It provides hidden results which may not otherwise be found by other tools.

Information found

E-mail addresses, domain names, IP addresses, contact details were found using Maltego. In addition to this, links between the information were found.

How the information can be used by an attacker

Information about contacts and e-mail addresses can be combined to later perform social engineering to know more about the internal working of the organization. Information about domain names and IP addresses of servers can be used to perform active scans and find vulnerabilities to perform the final attack.

Suggested Controls

A strict policy and guidelines on how much information can be made available to the public should be implemented. Security on the network should be implemented by putting up firewalls and blocking access as much as possible. Security through obscurity could also be implemented, using unusual ports which attackers may not be able to guess, hiding information about important contacts are other measures to protect the organization.

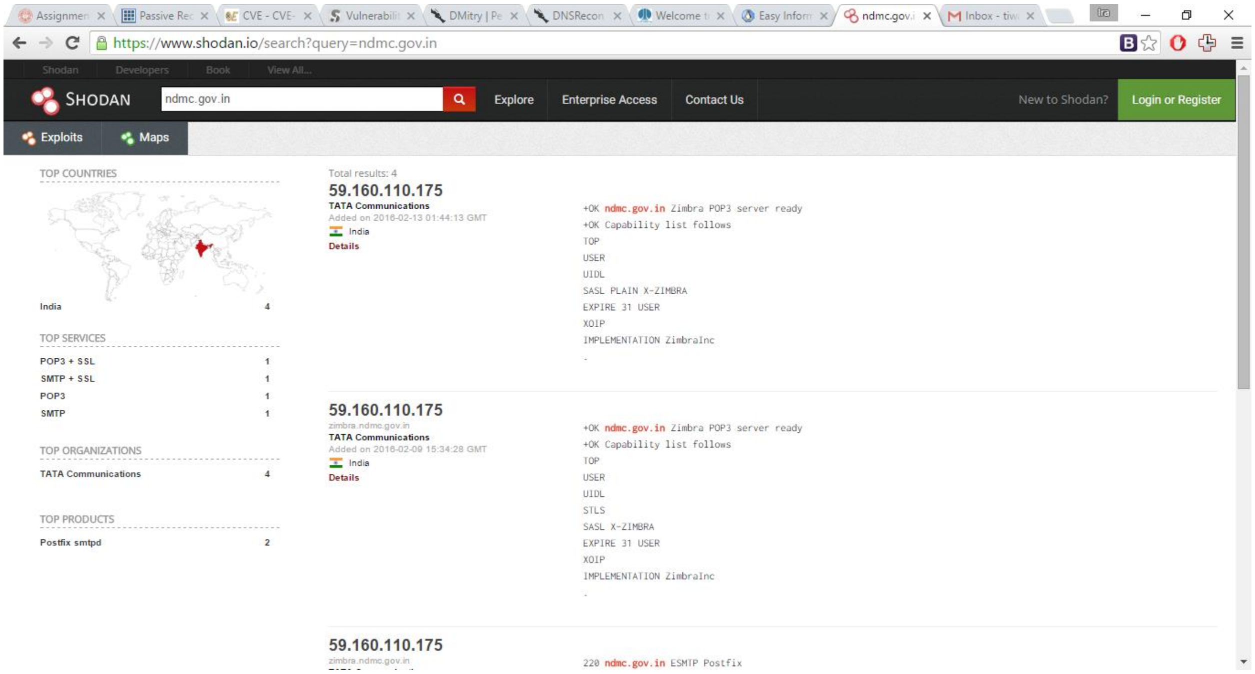
4. Tool used: Shodan

How it gathers information

Shodan is a search engine which specifically searches for devices connected to the Internet. Information about the server software can be found using this. It mostly collects data on web servers.

Information found

Information about the server, its location, protocols used and the owner of the server was found using Shodan.



https://www.shodan.io/search?query=ndmc.gov.in

ndmc.gov.in

TOP COUNTRIES

India	4

TOP SERVICES

POP3 + SSL	1
SMTP + SSL	1
POP3	1
SMTP	1

TOP ORGANIZATIONS

TATA Communications	4

TOP PRODUCTS

Postfix smtpd	2

Total results: 4

59.160.110.175
TATA Communications
Added on 2016-02-13 01:44:13 GMT
India
Details

```
+OK ndmc.gov.in Zimbra POP3 server ready
+OK Capability list follows
TOP
USER
UIDL
SASL PLAIN X-ZIMBRA
EXPIRE 31 USER
XOIP
IMPLEMENTATION ZimbraInc
.
```

59.160.110.175
zimbra.ndmc.gov.in
TATA Communications
Added on 2016-02-09 15:34:28 GMT
India
Details

```
+OK ndmc.gov.in Zimbra POP3 server ready
+OK Capability list follows
TOP
USER
UIDL
STLS
SASL X-ZIMBRA
EXPIRE 31 USER
XOIP
IMPLEMENTATION ZimbraInc
.
```

59.160.110.175
zimbra.ndmc.gov.in

```
220 ndmc.gov.in ESMTP Postfix
```

How the information can be used by an attacker

Information about the network infrastructure can be exploited by an attacker to perform active reconnaissance and the final attack using information found in the active recon.

Suggested Controls

Restricting the public facing servers and devices is one way to protect the organization’s servers from being detected by Shodan. Using VPN’s and IP filters for external access can also be used. Another method could be to run shodan against one’s own network

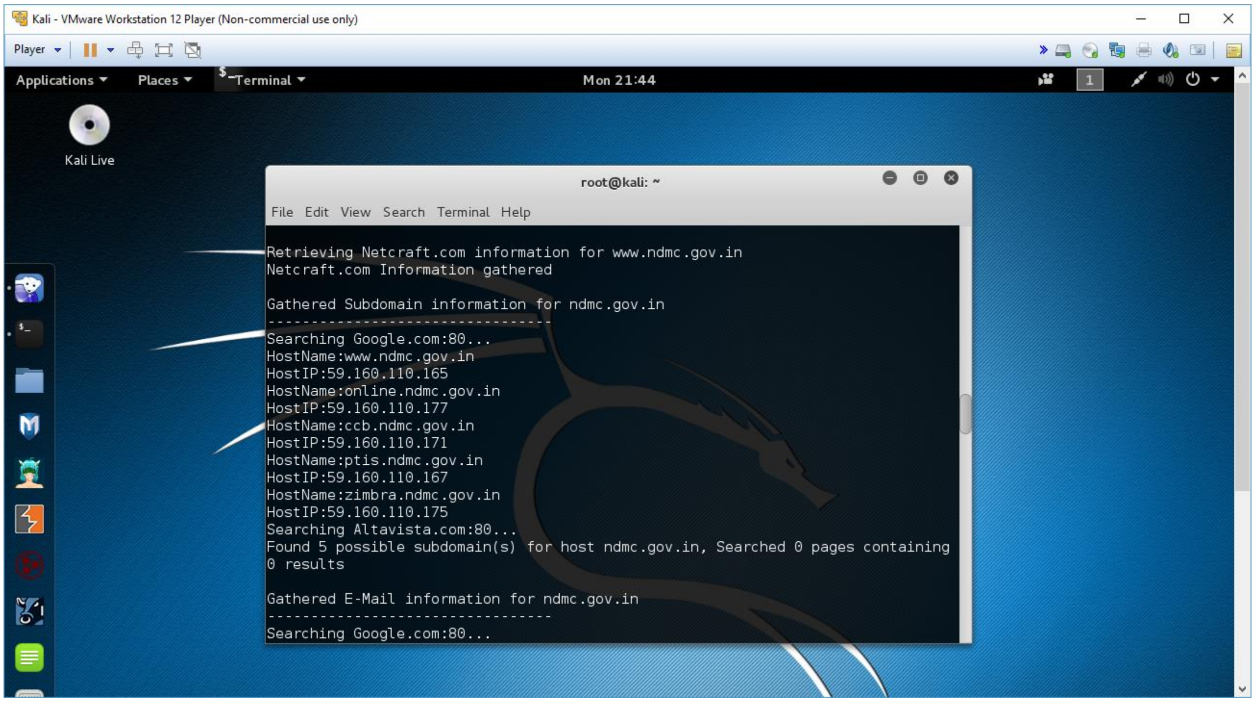
5. Tool used: Dmitry

How it gathers information

Dmitry is a built-in tool in Kali linux. It can perform a whois lookup on a domain, search for possible subdomains, e-mail addresses and even perform port scans on a given host. Except for port scanning, all other functionalities are passive reconnaissance techniques.

Information found

By using the whois lookup option, information about the registrant of the website and their contact information. Using the option for netcraft lookup, various host names and host IP addresses were found.


Kali - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Mon 21:44
Kali Live
root@kali: ~
File Edit View Search Terminal Help

```
Retrieving Netcraft.com information for www.ndmc.gov.in
Netcraft.com Information gathered

Gathered Subdomain information for ndmc.gov.in
---------------------------------
Searching Google.com:80...
HostName:www.ndmc.gov.in
HostIP:59.160.110.165
HostName:online.ndmc.gov.in
HostIP:59.160.110.177
HostName:ccb.ndmc.gov.in
HostIP:59.160.110.171
HostName:ptis.ndmc.gov.in
HostIP:59.160.110.167
HostName:zimbra.ndmc.gov.in
HostIP:59.160.110.175
Searching Altavista.com:80...
Found 5 possible subdomain(s) for host ndmc.gov.in, Searched 0 pages containing
0 results

Gathered E-Mail information for ndmc.gov.in
---------------------------------
Searching Google.com:80...
```

How the information can be used by an attacker

Knowing the contact details of the person who registered the website can be used by an attacker to perform a social engineering attack. Knowing the IP address the attacker can then actively scan using nmap and nessus.

Suggested Controls

Information about the registrant of the website can be obscured or hidden to prevent the attacker from using it. Putting up firewalls and using uncommon ports on hosts can be another safety measure.

6. Tool used: theharvester

How it gathers information

This tool is a built in tool of Kali Linux and gathers information about e-mail accounts, usernames and domains from various public sources, such as google, linkedin, googleprofiles, twitter, bing etc.

Information found

Information about the hostnames, domains and e-mails was found.

How the information can be used by an attacker

The information gathered using this tool showed the same hostnames and IP addressed obtained using Dmitry. The attacker would be able to confirm these addresses and hostnames and perform attacks on servers from each domain.

Suggested Controls

IP addresses of hosts can be found using many different methods. Protection against an active attack on a host can be done by strengthening the network, installing firewalls, using obscure ports.

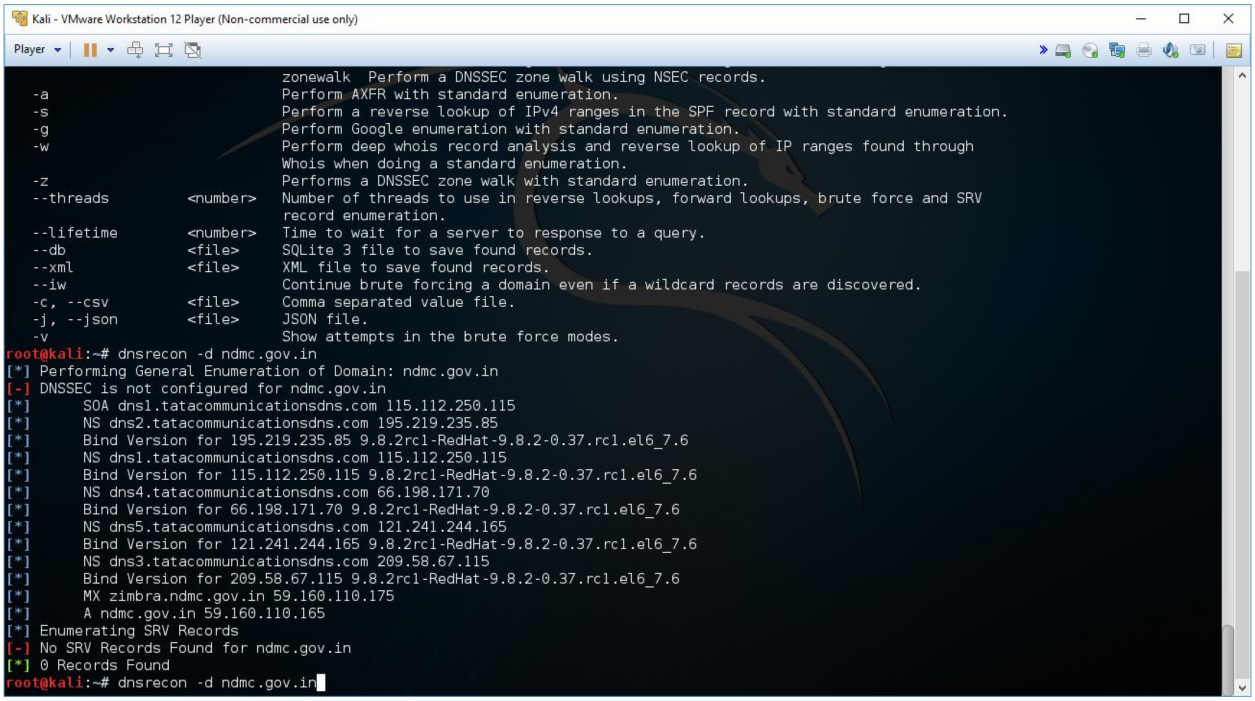
7. Tool used: dnsrecon

How it gathers information

The dnsrecon is a built-in tool in Kali linux, which performs DNS enumeration of the specified domain. It can reveal information about the company's network.

Information found

Information about the network servers and their domains, operating systems were found by specifying the domain for ndmc.gov.in.



Kali - VMware Workstation 12 Player (Non-commercial use only)
Player

```
                                 zonewalk  Perform a DNSSEC zone walk using NSEC records.
   -a                            Perform AXFR with standard enumeration.
   -s                            Perform a reverse lookup of IPv4 ranges in the SPF record with standard enumeration.
   -g                            Perform Google enumeration with standard enumeration.
   -w                            Perform deep whois record analysis and reverse lookup of IP ranges found through
                                 Whois when doing a standard enumeration.
   -z                            Performs a DNSSEC zone walk with standard enumeration.
   --threads          <number>   Number of threads to use in reverse lookups, forward lookups, brute force and SRV
                                 record enumeration.
   --lifetime         <number>   Time to wait for a server to response to a query.
   --db               <file>     SQLite 3 file to save found records.
   --xml              <file>     XML file to save found records.
   --iw                          Continue brute forcing a domain even if a wildcard records are discovered.
   -c, --csv          <file>     Comma separated value file.
   -j, --json         <file>     JSON file.
   -v                            Show attempts in the brute force modes.
root@kali:~# dnsrecon -d ndmc.gov.in
[*] Performing General Enumeration of Domain: ndmc.gov.in
[-] DNSSEC is not configured for ndmc.gov.in
[*]      SOA dns1.tatacommunicationsdns.com 115.112.250.115
[*]      NS dns2.tatacommunicationsdns.com 195.219.235.85
[*]      Bind Version for 195.219.235.85 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.6
[*]      NS dns1.tatacommunicationsdns.com 115.112.250.115
[*]      Bind Version for 115.112.250.115 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.6
[*]      NS dns4.tatacommunicationsdns.com 66.198.171.70
[*]      Bind Version for 66.198.171.70 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.6
[*]      NS dns5.tatacommunicationsdns.com 121.241.244.165
[*]      Bind Version for 121.241.244.165 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.6
[*]      NS dns3.tatacommunicationsdns.com 209.58.67.115
[*]      Bind Version for 209.58.67.115 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.6
[*]      MX zimbra.ndmc.gov.in 59.160.110.175
[*]      A ndmc.gov.in 59.160.110.165
[*] Enumerating SRV Records
[-] No SRV Records Found for ndmc.gov.in
[*] 0 Records Found
root@kali:~# dnsrecon -d ndmc.gov.in
```

How the information can be used by an attacker

Knowing the details of the network can be used to perform active exploits using nmap, nessus and penetration testing techniques.

Suggested Controls

Strengthening the network security and hiding the network details is recommended. The bind server operating system should not be made easily available for passive reconnaissance techniques.

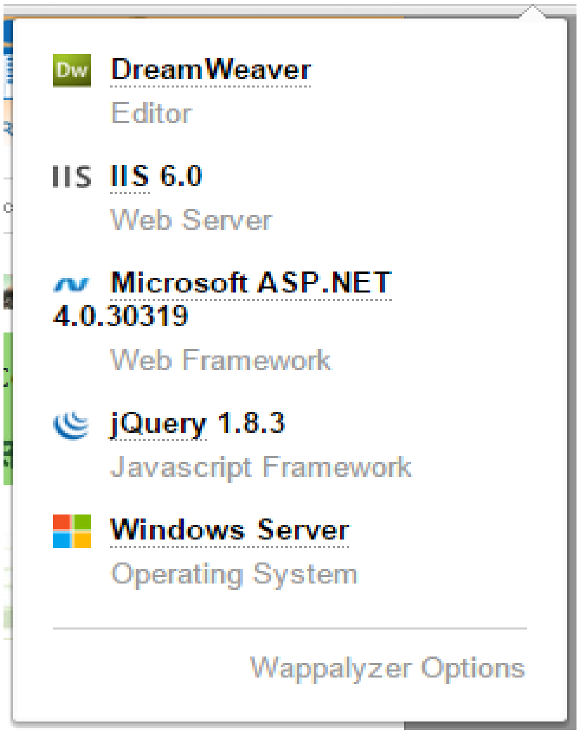
8. Tool used: wappalyzer

How it gathers information

Wappalyzer works as an extension on the browser being used. It identifies the software on a website. It can also identify the operating system, frameworks and technology being used on a website.

Information found

The operating system, framework and technology being used on ndmc.gov.in could be identified through wappalyzer.



DreamWeaver
Editor

IIS 6.0
Web Server

Microsoft ASP.NET 4.0.30319
Web Framework

jQuery 1.8.3
Javascript Framework

Windows Server
Operating System

How the information can be used by an attacker

An attacker can utilize information about the frameworks, technologies and operating system to launch targeted attacks.

Suggested Controls

Information about the operating system, technology etc. should be obscured so that the attacker is unable to see any of this. Apache and PHP can be configured to not display server information.