Home

Original Article: Dns Security: Comprenshive Guide How to Pull Data or DDos
Date: Sun/24 March, 2019
Refernces: 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

Hack

Policies, Guidelines and Firewalls

Final Words

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 methamtics 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 posioning 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 posioning 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 enteries 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 indsturies, 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

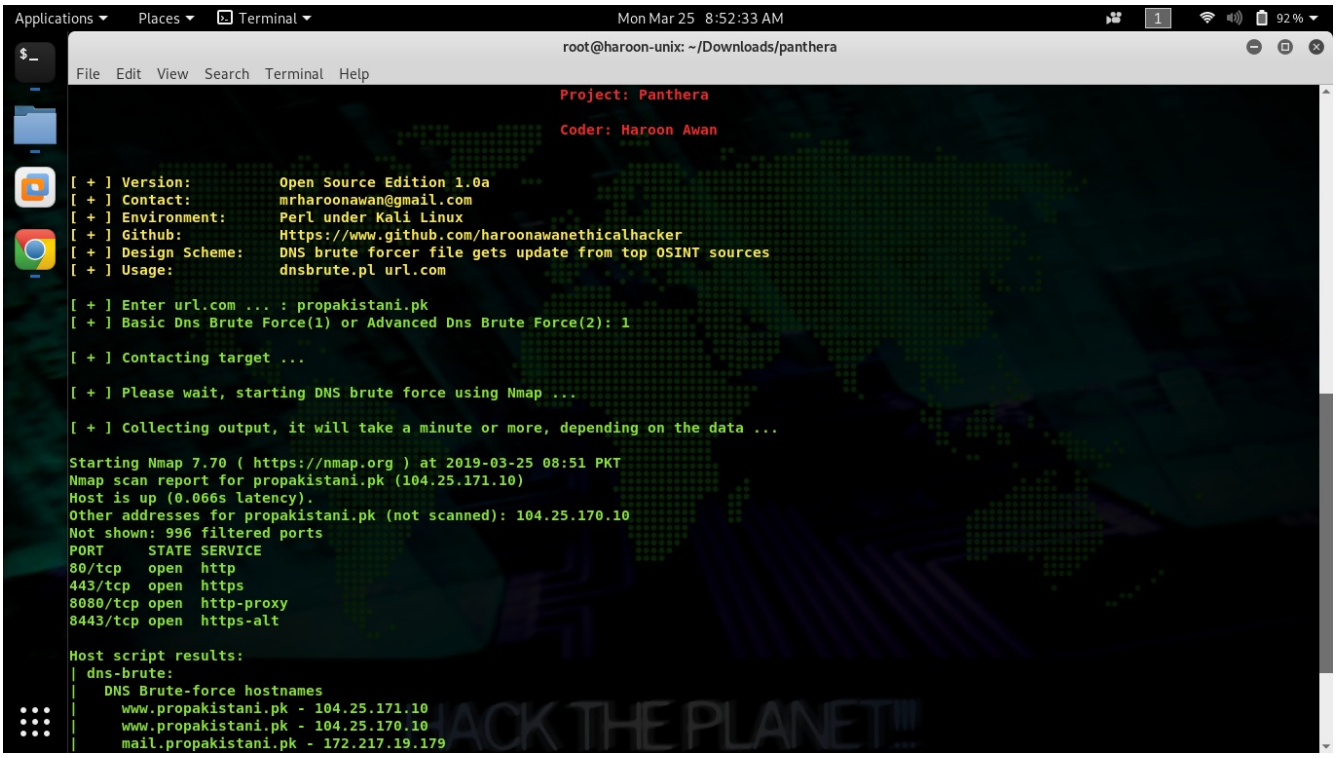
10a. Bugs like cache poisining, recursive, hijacking, hacking, ddos, amplify attacks, information leakage like how many domains point data from that DNS to other associated domains and finally DNS brute forcing
10b. I would say law of cyber crimes never been impressive in Pakistan. People of Pakistan 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



As you can see, how easy it is to pull records using associated or authoritive 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

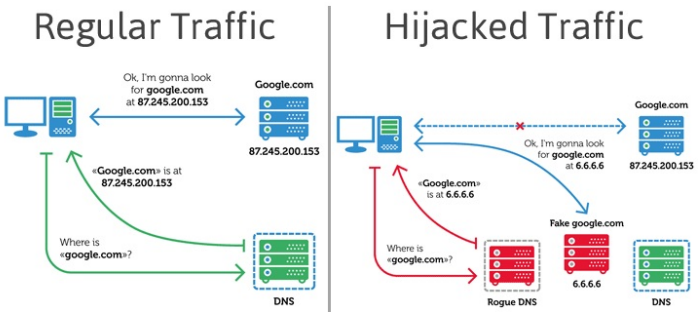
Intercept communication between a user and a DNS server via Host file

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



Spoofing DNS

Type A

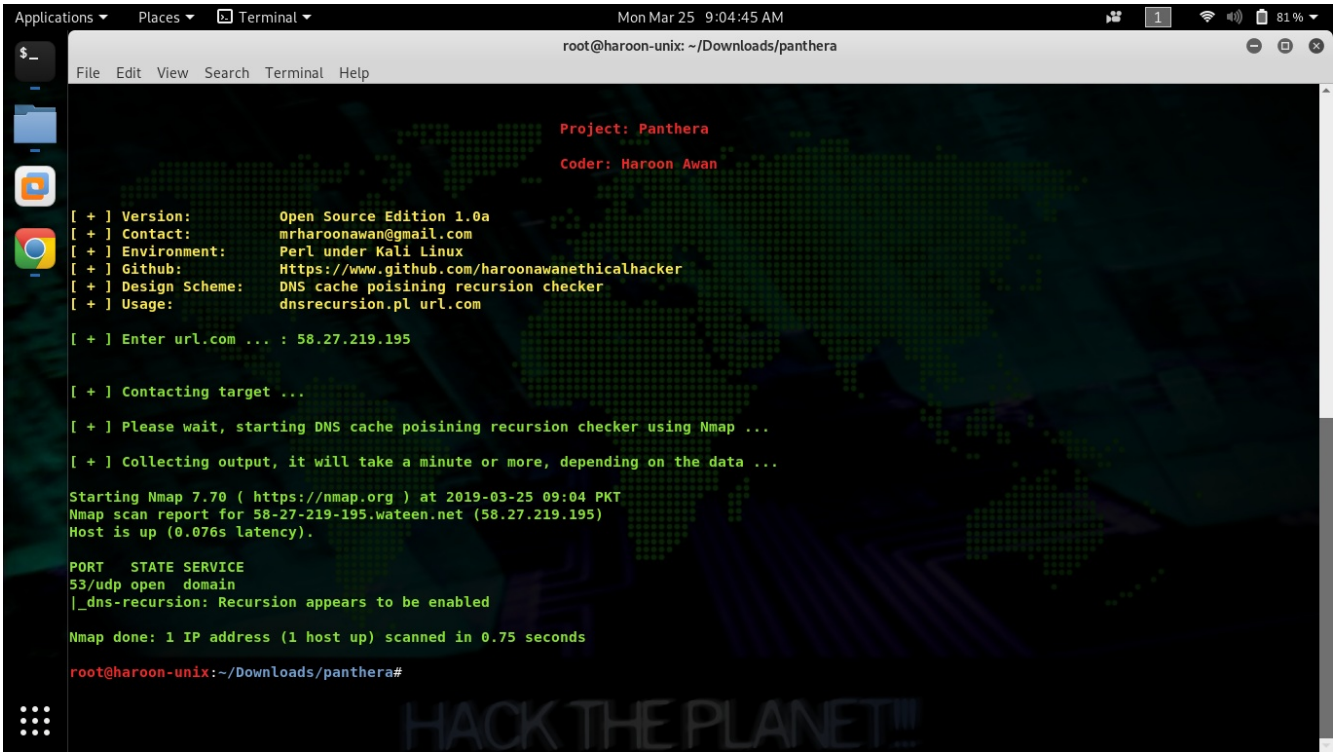
1. What is DNS recursive and resolver?

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

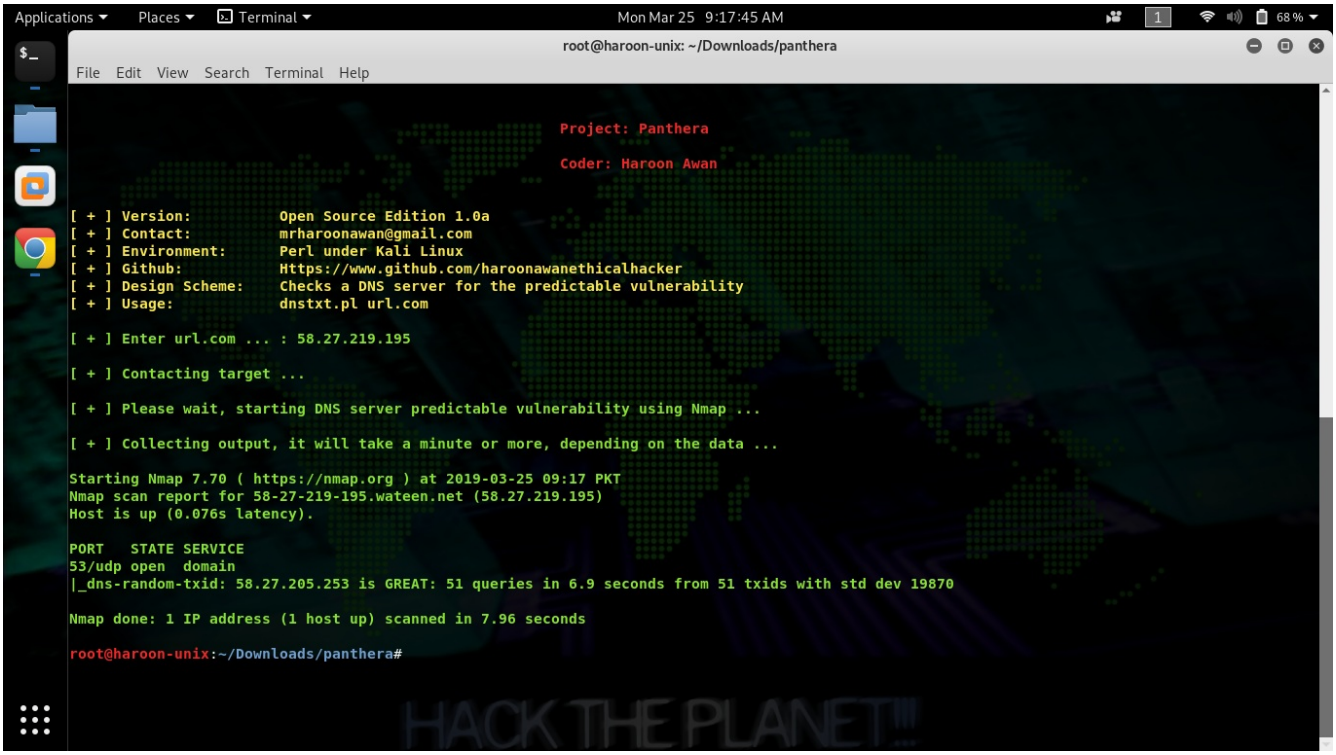


Why we need DNS recursion, once recursion is established, you can hijack DNS traffic sitting anywhere!

Type B
This gets DNS txtid records from Server

Real life example:

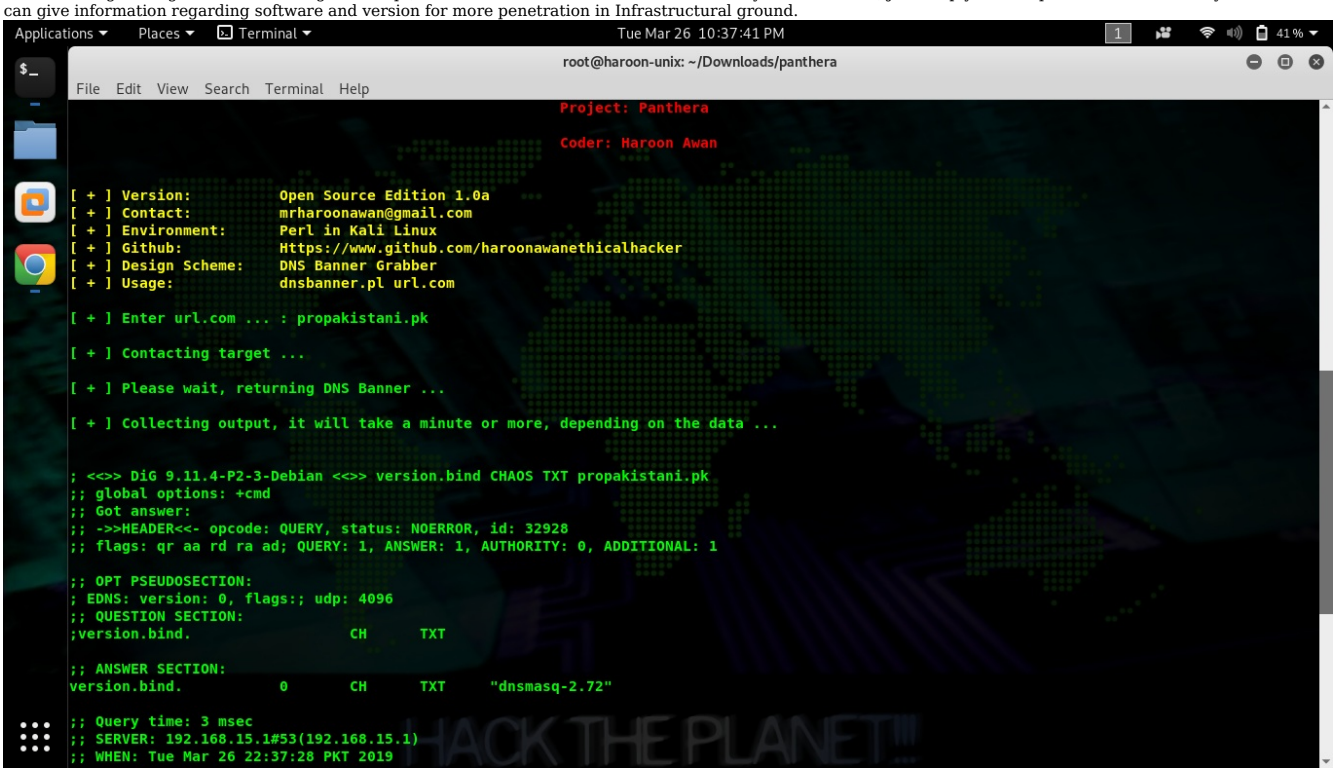
182.xxx.1xx.122
Pakistan Telecommunication Company Limited
Added on 2019-03-23 08:54:28 GMT
Pakistan
Recursion: enabled



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

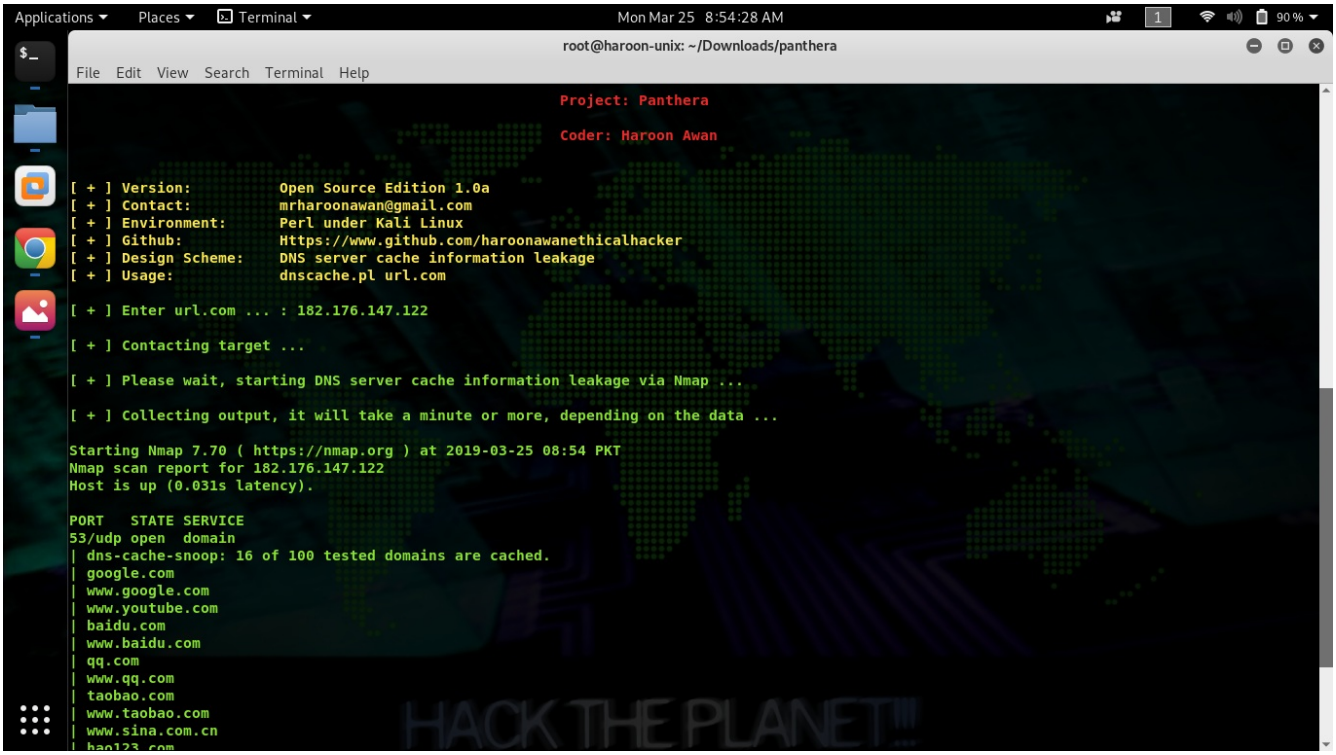
DNS Banner Grabbing

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 grabing? DNS can give information regarding software and version for more penetration in Infrastructural ground.



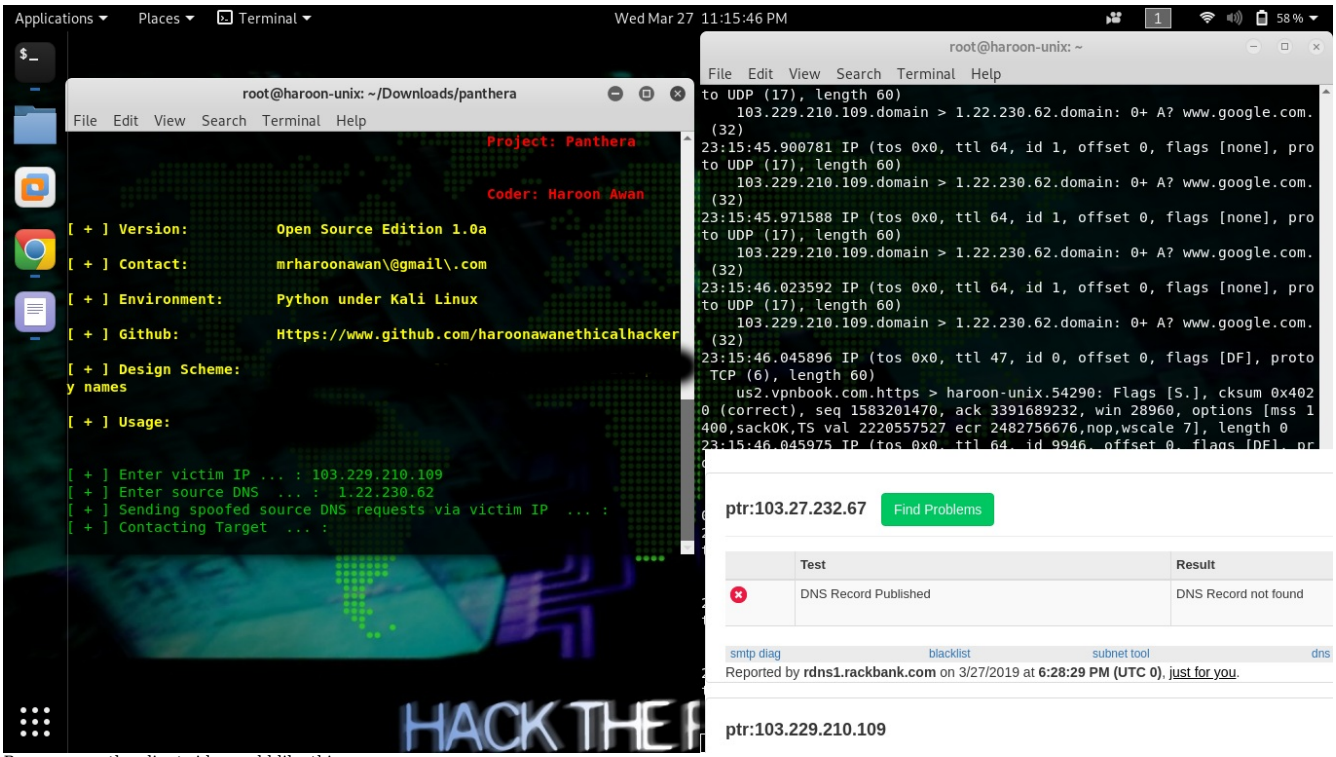
DNS Cache Snooping

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.

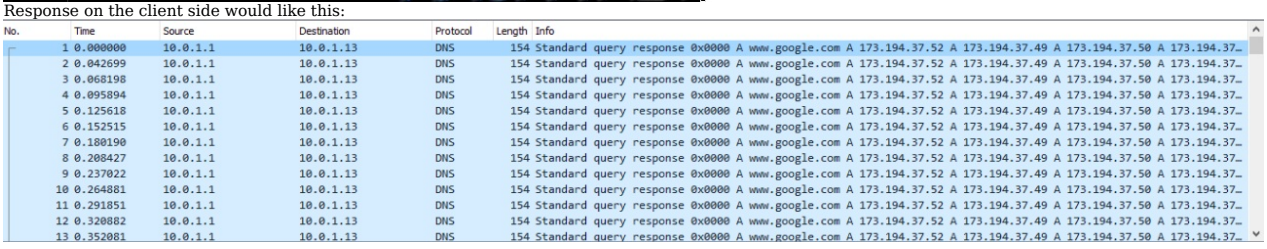


DDOS DNS

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!

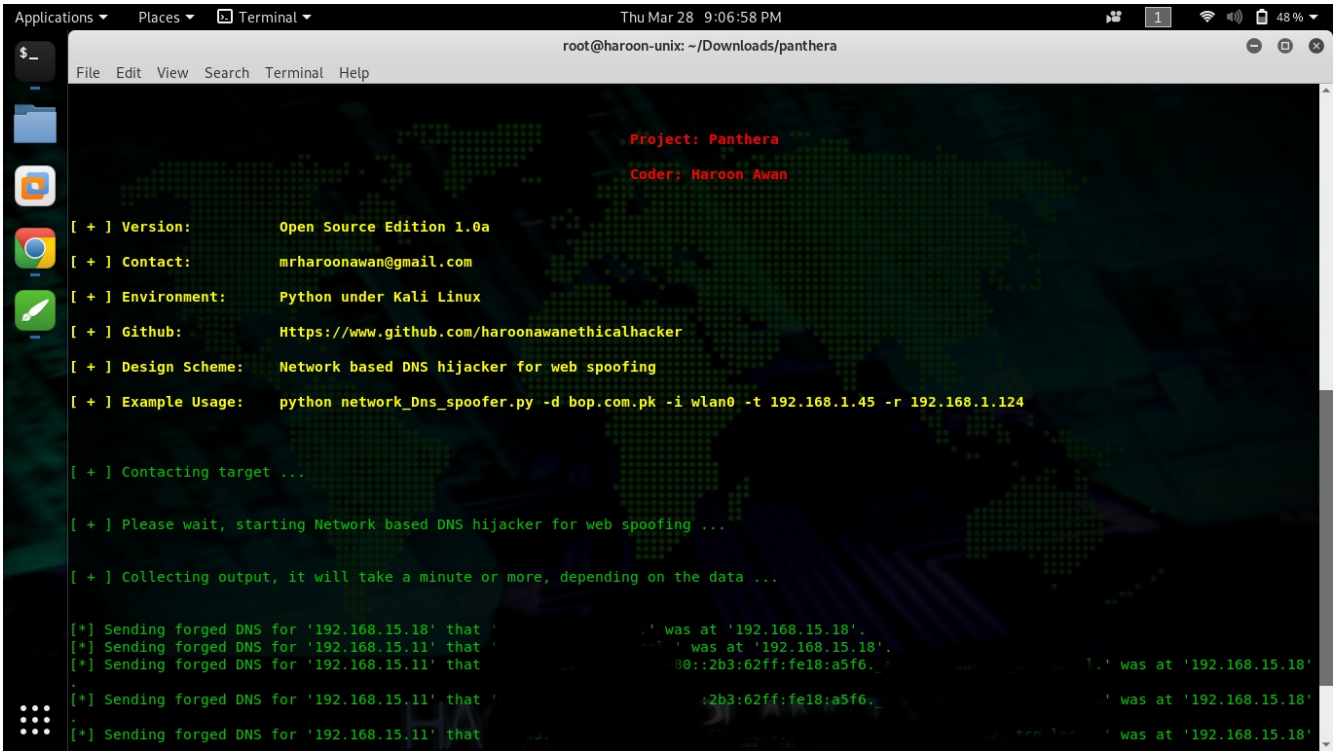


Response on the client side would like this:

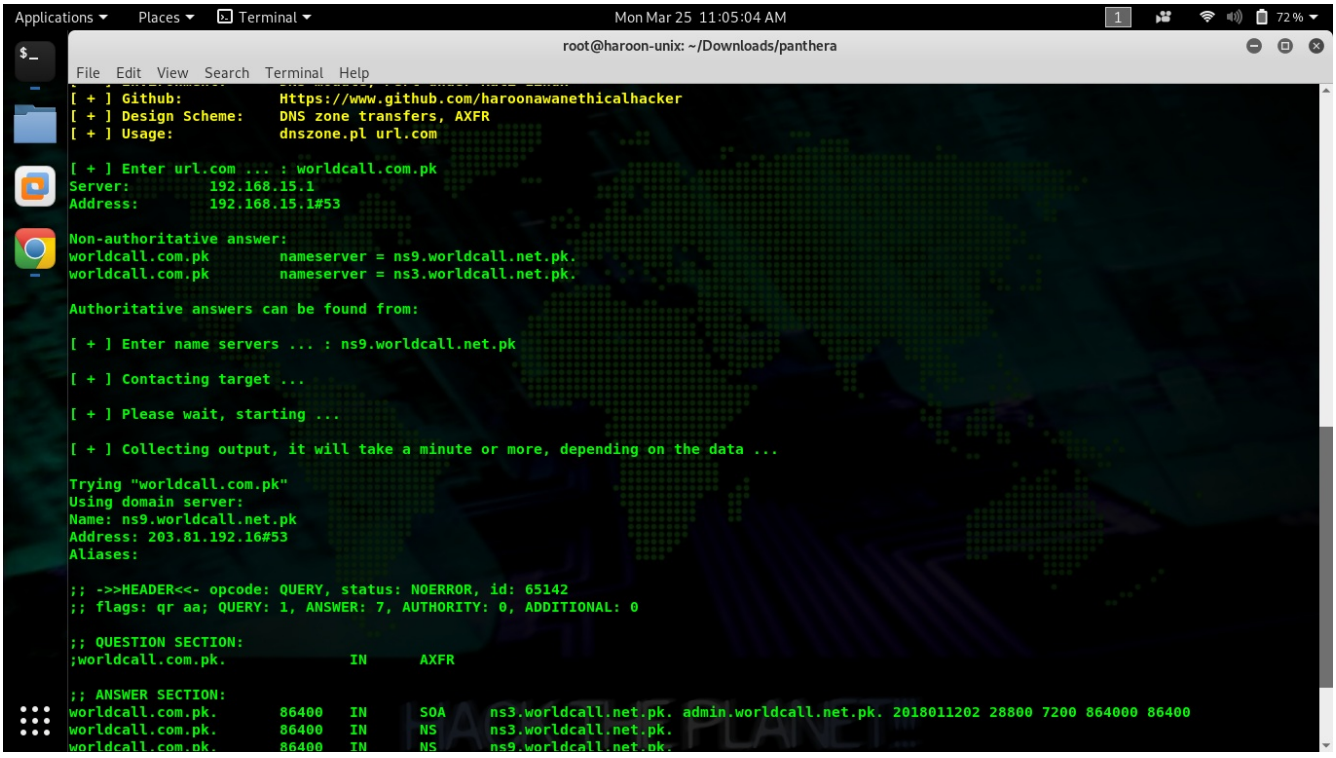


Network DNS hijacking

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.



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



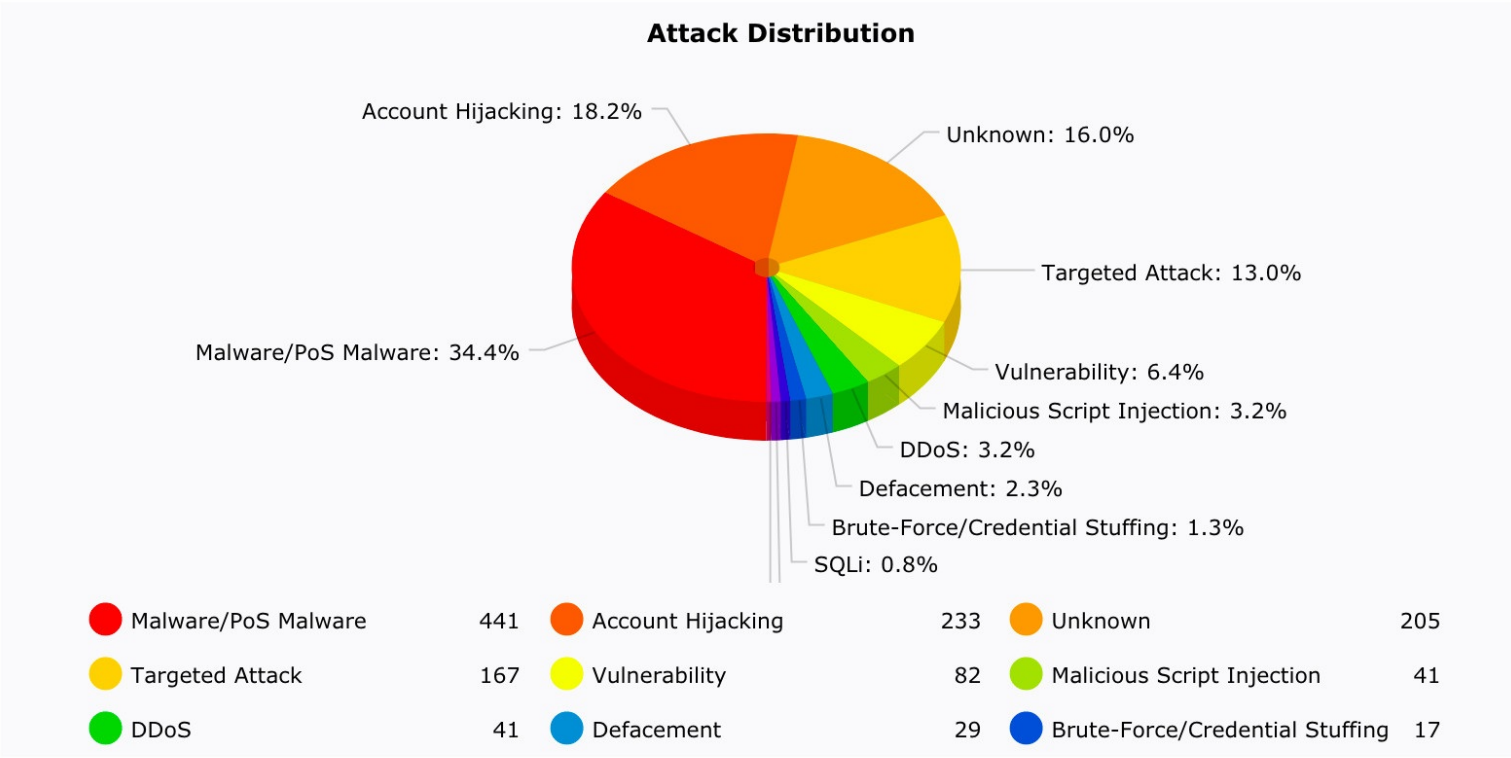
Notice, how DNS is walking and giving us everything like admin.worldcall.net.pk. If server have 100 records, it will just throw that to us in seconds.

Policies, Guidelines and Firewalls

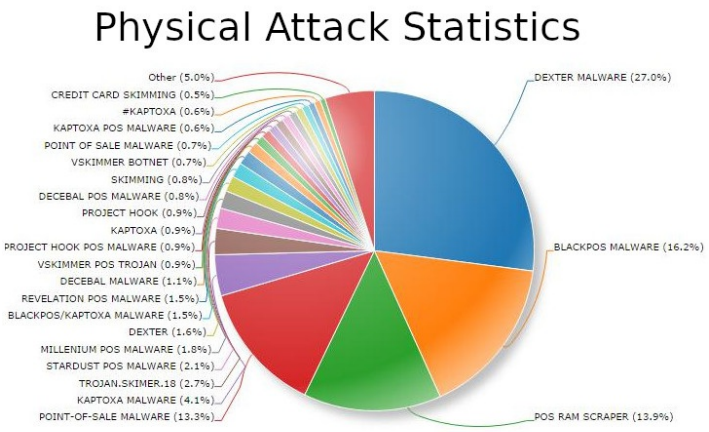
19.Script-kiddies
19a.Pakistan definitely needs an effective “National Cyber Security Act “ to protect its people from cyber crime. Unfortunately more immature and dangerous

> 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.



3. Check out the POS related frauds over the year



20. Setting up Traps for DNS

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

21. Firewall DNS Policies Guidline

a.Install Firewall policy
b.Set access control policy in DNS file
c.Restrict DNS registry
d.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/