DNS Reconnaissance – DNSRecon

November 13, 2012

DNS reconnaissance is part of the information gathering stage on a penetration test engagement.When a penetration tester is performing a DNS reconnaissance is trying to obtain as much as information as he can regarding the DNS servers and their records.The information that can be gathered it can disclose the network infrastructure of the company without alerting the IDS/IPS.This is due that most of the organizations are not monitoring their DNS server traffic and those that do they only monitor the zone transfers attempts.

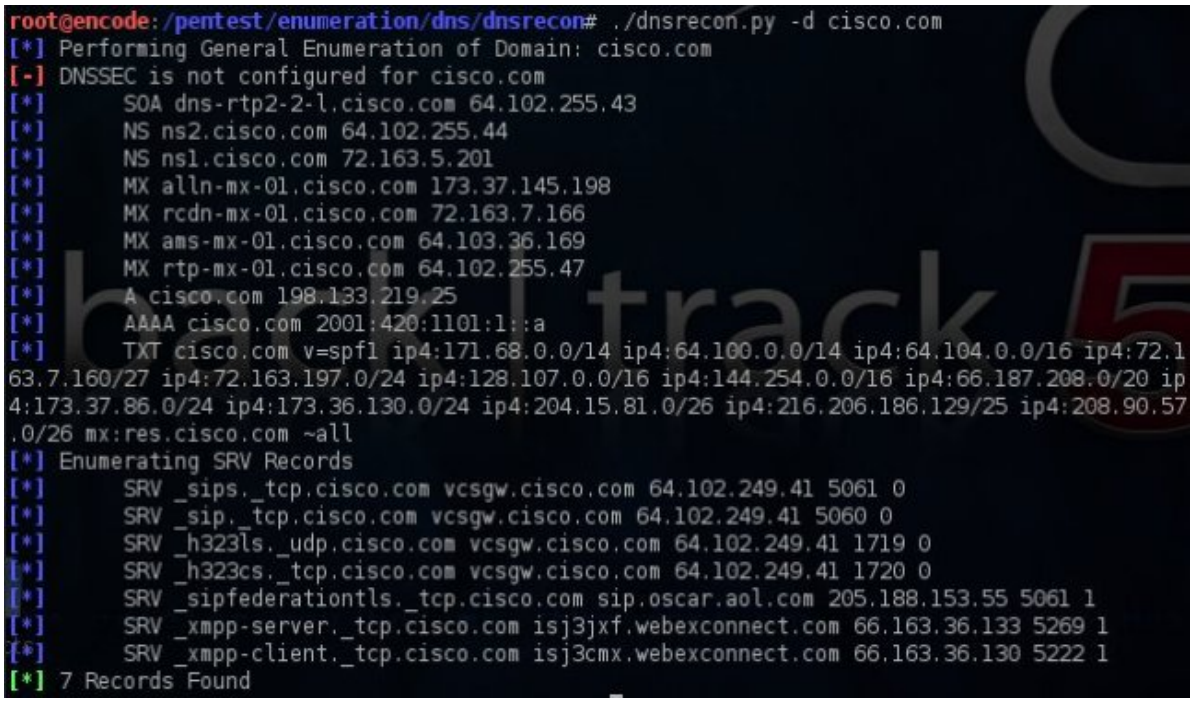
On the web there are a variety of tools available that can gather DNS information effectively but in this article we will focus on the DNSRecon which is a tool that was developed by Carlos Perez and it is designed to perform DNS reconnaissance.This tool is included on backtrack and it is written in python.

The types of enumeration that performs include the following:

- Zone Transfer
- Reverse Lookup
- Domain and Host Brute-Force
- Standard Record Enumeration (wildcard,SOA,MX,A,TXT etc.)
- Cache Snooping
- Zone Walking
- Google Lookup

Standard Record Enumeration

In order to perform standard DNS enumeration with the DNSRecon the command that we have to use is the **./dnsrecon.py -d <domain>**.So let's try that command against the domain cisco.com to see what kind of information can we retrieve.



DNSRecon – Standard Enumeration

From the image above we can see that Cisco is not using DNSSec,we discover the SOA record,the mail servers,the IP ranges that the company is using and what servers can send emails (SPF) and of course we enumerated the SRV (Service) records.But what the SRV records tell us?First of all they tell us that Cisco is using VoIP.We understand that because we can see the SIP protocol in use.Also we know that they are using a jabber (XMPP) and videoconferencing in their infrastructure.We also obtained the IP and the ports that these services are running.

Zone Transfer

The security problem with DNS zone transfer is that it can be used to decipher the topology of a company's network.Specifically when a user is trying to perform a zone transfer it sends a DNS query to list all DNS information like name servers,host names,MX and CNAME records,zone serial number,Time to Live records etc.Due to the amount of information that can be obtained DNS zone transfer cannot be easily found in nowadays.However DNSRecon provides the ability to perform Zone Transfers with the commands

./dnsrecon.py -d <domain> -a or

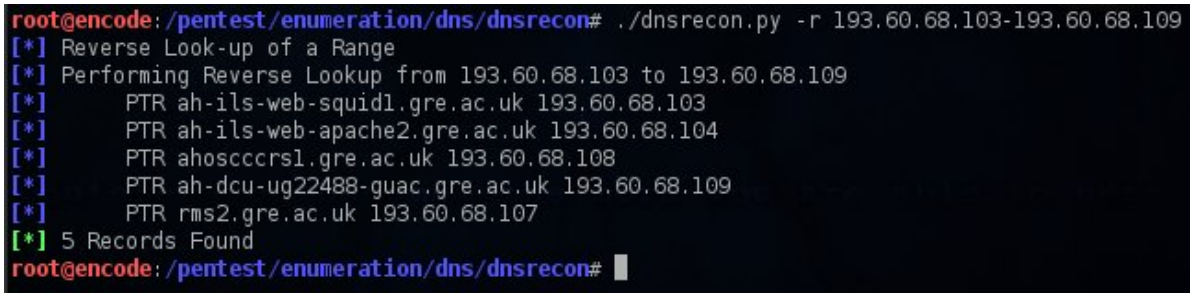
./dnsrecon.py -d <domain> -t axfr

Reverse Lookup

According to Wikipedia reverse DNS lookup is the determination of a domain name with the associated IP address.DNSRecon can perform a reverse lookup for PTR (Pointer) records against IPv4 and IPv6 address ranges.To run reverse lookup enumeration the command

./dnsrecon.py -r <startIP-endIP>

must be used.Also reverse lookup can be performed against all ranges in SPF records with the command **./dnsrecon.py -d <domain> -s**.In the next image you can see the output that produces a reverse lookup in a range of IP addresses.

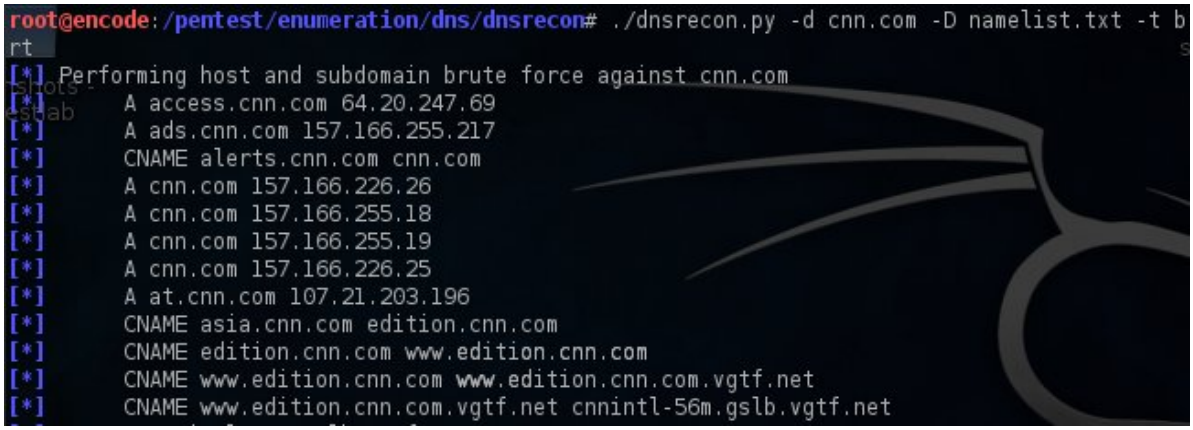


Reverse Lookup

Domain Brute-Force

For performing this technique all we have to do is to give a name list and it will try to resolve the A,AAA and CNAME records against the domain by trying each entry one by one.In order to run the Domain Name Brute-Force we need to type:

./dnsrecon.py -d <domain> -D <namelist> -t brt



Domain Brute-Force

As we can see we obtained A and CNAME records of the domain cnn.com and their IP addresses.

Cache Snooping

DNS cache snooping is occurred when the DNS server has a specific DNS record cached.This DNS record will often reveal plenty of information.However DNS cache snooping is not happening very often.The command that can be used in order to perform cache snooping is the following:

./dnsrecon.py -t snoop -n Sever -D <Dict>

Zone Walking

This technique may unveils internal records if zone is not configured properly.The information that can be obtained can help us to map network hosts by enumerating the contents of a zone.In order to perform the zone walking we need to type the command:

./dnsrecon.py -d <host> -t zonewalk

Conclusion

As we saw in this article the amount of information that can be discovered during DNS reconnaissance is huge.Often misconfigurations on the DNS servers of our client can help us to map the entire network.DNS reconnaissance is an important step that cannot be missed during network infrastructure penetration tests and DNSRecon can help us to enumerate DNS information.