DNSenum – Gathering DNS Information

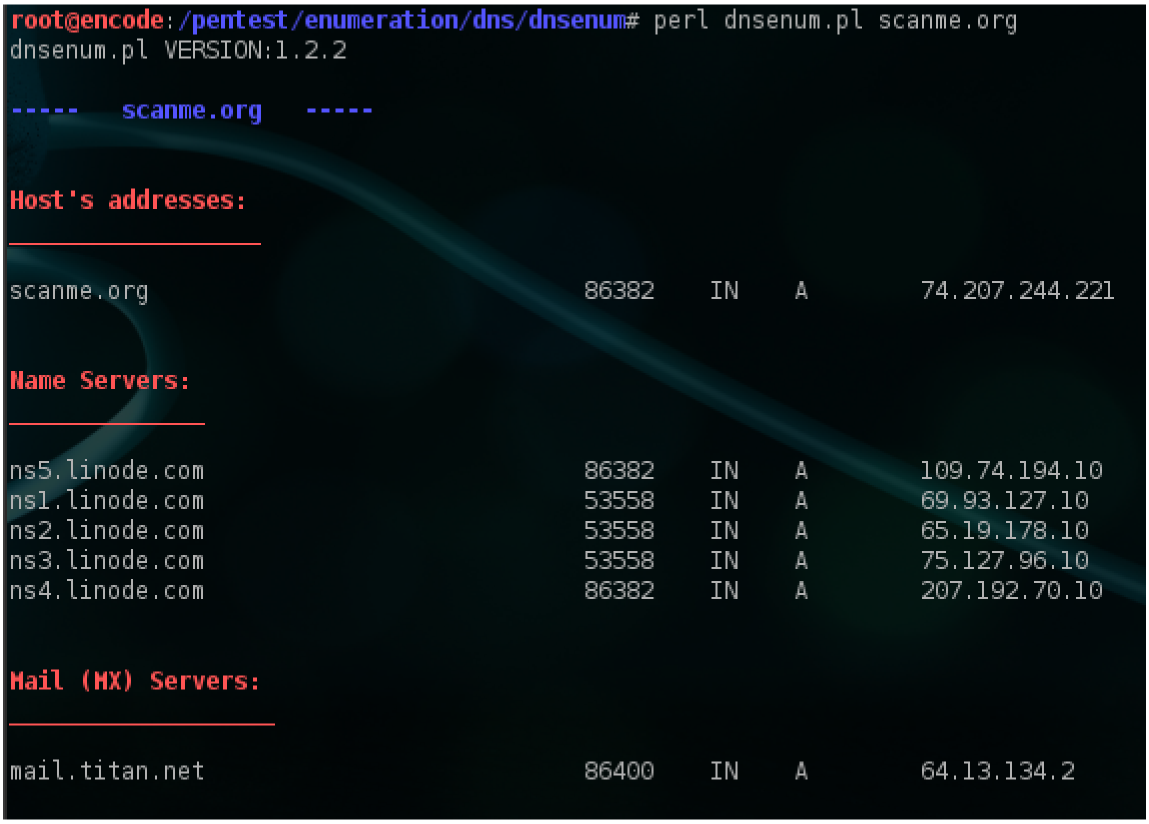
pentestlab.blog/category/information-gathering/page/8

July 13, 2012

DNSenum is a tool that it was designed with the purpose of enumerating DNS information about a domain.Then information that you can obtain from this tool is useful for the phase of information gathering when you are conducting especially a penetration test.

So lets say that you want to obtain information about a specific domain.In this article we will use different domains as an example in order to see the different responses that we can get.First you will need to go to the directory that the DNSenum is located.In backtrack 5 this in the **/pentest/enumeration/dns/dnsenum** and in order to run it you can use the command: **perl dnsenum.pl [host]**

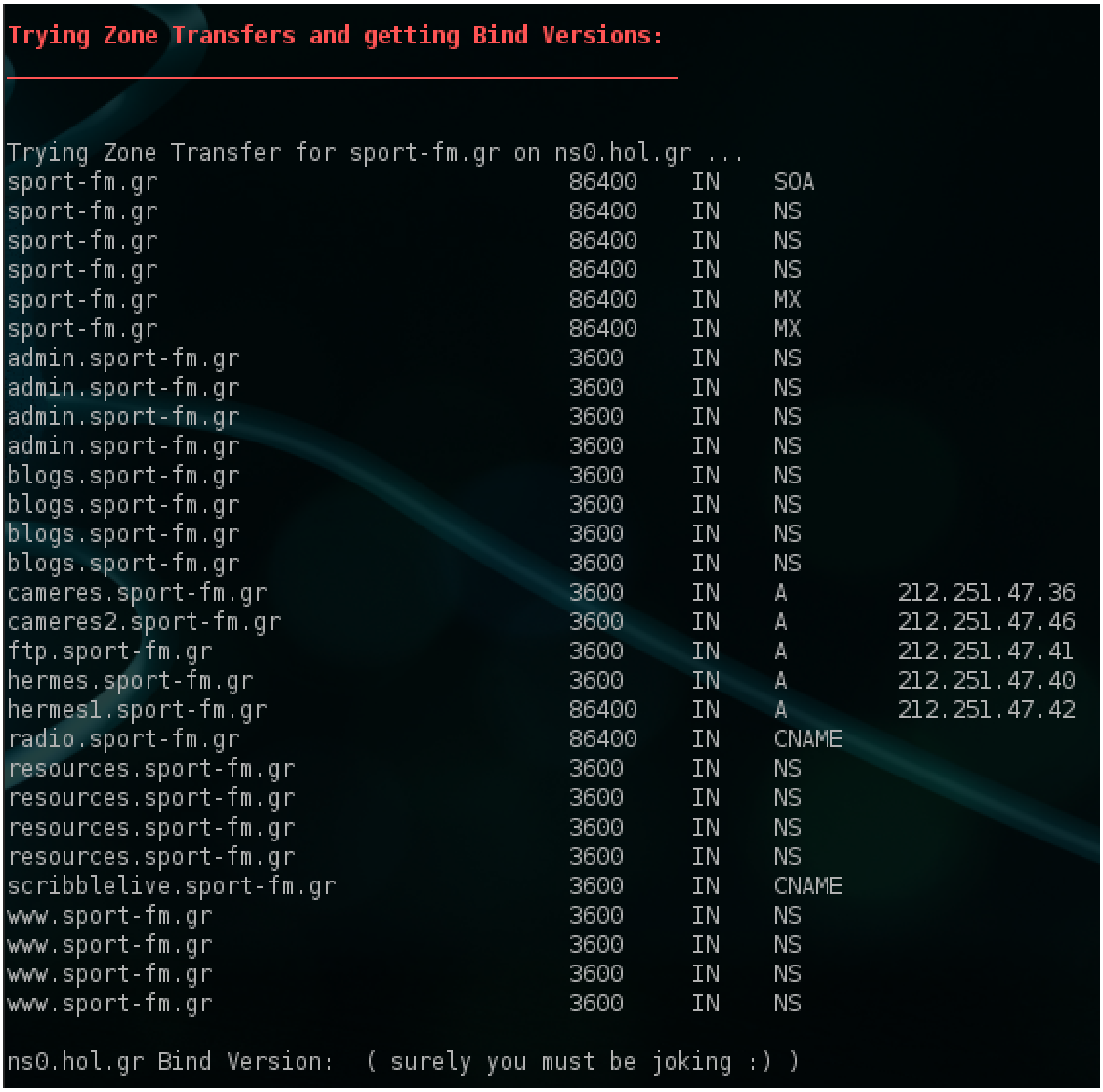
The DNSenum will start querying the DNS servers of scanme.org.The first information that we will get is the host address which for scanme.org is the 74.207.244.221.Next we will see the name servers which will give us an idea of the hosting provider that the scanme.org is using and after that is the MX record where we can see the mail server of our target host.



```
root@encode:/pentest/enumeration/dns/dnsenum# perl dnsenum.pl scanme.org
dnsenum.pl VERSION:1.2.2

-----   scanme.org   -----


Host's addresses:
__________________

scanme.org                               86382    IN    A        74.207.244.221


Name Servers:
______________

ns5.linode.com                           86382    IN    A        109.74.194.10
ns1.linode.com                           53558    IN    A        69.93.127.10
ns2.linode.com                           53558    IN    A        65.19.178.10
ns3.linode.com                           53558    IN    A        75.127.96.10
ns4.linode.com                           86382    IN    A        207.192.70.10


Mail (MX) Servers:
___________________

mail.titan.net                           86400    IN    A        64.13.134.2
```

Gathering the first information

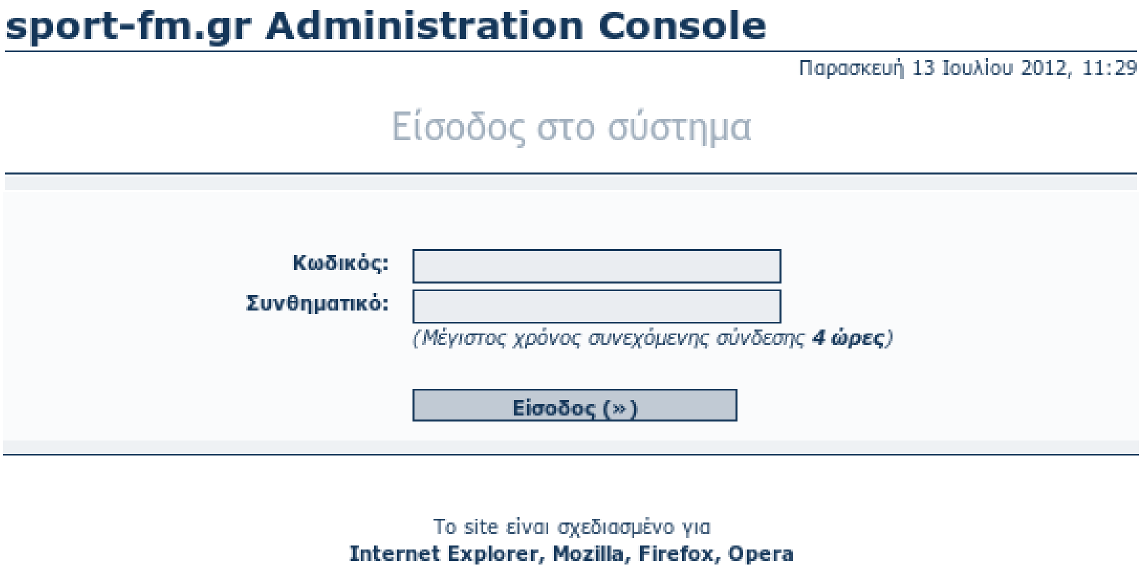
After that the DNSenum will start the DNS Zone Transfer.Performing a Zone Transfer you can discover more information about a domain like any sub-domains that are included in the same zone, SOA records etc.In the screenshot below you can see the results after performing a zone transfer for the domain sport-fm.gr.



```
Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for sport-fm.gr on ns0.hol.gr ...
sport-fm.gr                              86400    IN    SOA
sport-fm.gr                              86400    IN    NS
sport-fm.gr                              86400    IN    NS
sport-fm.gr                              86400    IN    NS
sport-fm.gr                              86400    IN    MX
sport-fm.gr                              86400    IN    MX
admin.sport-fm.gr                        3600     IN    NS
admin.sport-fm.gr                        3600     IN    NS
admin.sport-fm.gr                        3600     IN    NS
admin.sport-fm.gr                        3600     IN    NS
blogs.sport-fm.gr                        3600     IN    NS
blogs.sport-fm.gr                        3600     IN    NS
blogs.sport-fm.gr                        3600     IN    NS
blogs.sport-fm.gr                        3600     IN    NS
cameres.sport-fm.gr                      3600     IN    A        212.251.47.36
cameres2.sport-fm.gr                     3600     IN    A        212.251.47.46
ftp.sport-fm.gr                          3600     IN    A        212.251.47.41
hermes.sport-fm.gr                       3600     IN    A        212.251.47.40
hermes1.sport-fm.gr                      86400    IN    A        212.251.47.42
radio.sport-fm.gr                        86400    IN    CNAME
resources.sport-fm.gr                    3600     IN    NS
resources.sport-fm.gr                    3600     IN    NS
resources.sport-fm.gr                    3600     IN    NS
resources.sport-fm.gr                    3600     IN    NS
scribblelive.sport-fm.gr                 3600     IN    CNAME
www.sport-fm.gr                          3600     IN    NS
www.sport-fm.gr                          3600     IN    NS
www.sport-fm.gr                          3600     IN    NS
www.sport-fm.gr                          3600     IN    NS

ns0.hol.gr Bind Version:  ( surely you must be joking :) )
```

DNS Zone Transfer

By reviewing the results we can see that the SOA record is the http://www.sport-fm.gr.This means that this DNS name server is the best source of information for the data within this domain.Also we have a list with all the sub-domains and the interesting thing is that we have located the administration panel which is on the sub-domain admin.sport-fm.gr.



sport-fm.gr Administration Console

Παρασκευή 13 Ιουλίου 2012, 11:29

Είσοδος στο σύστημα

Κωδικός:

Συνθηματικό:

(Μέγιστος χρόνος συνεχόμενης σύνδεσης **4 ώρες**)

Το site είναι σχεδιασμένο για
Internet Explorer, Mozilla, Firefox, Opera

Administration Panel

Another option that DNSenum offers is the Google Scraping which it queries google search pages to discover various domain names of the target domain.This can be particular helpful when the zone transfer is disabled.Basically what it does is trying to get results from google by using the following command:

allinurl: -www site:target.com

Conclusion

DNSenum is a great tool to be used in the information gathering stage of a penetration testing.As we saw in this article we obtained a lot of information about our targets and we even discovered an administration panel from the early stage of our penetration test which can help us to perform further attacks on the target.