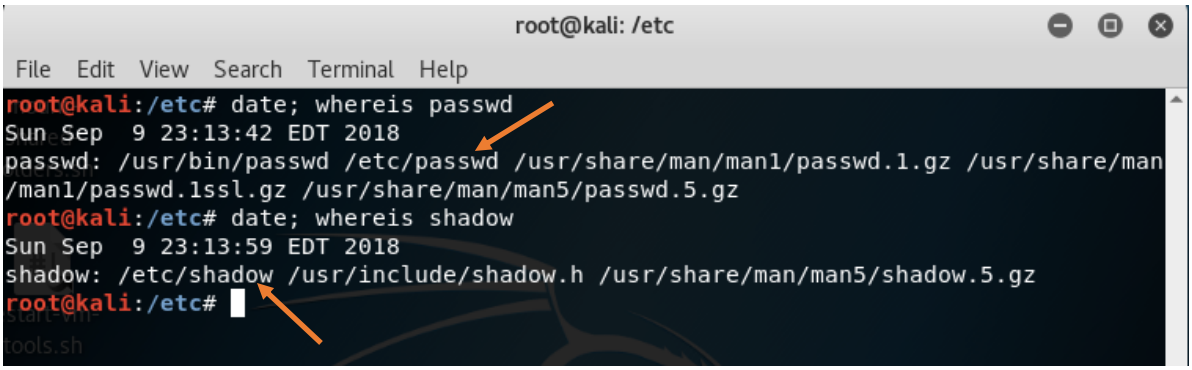
Name : Prashanth Rajasekar
SJSUID : 011822460

1.



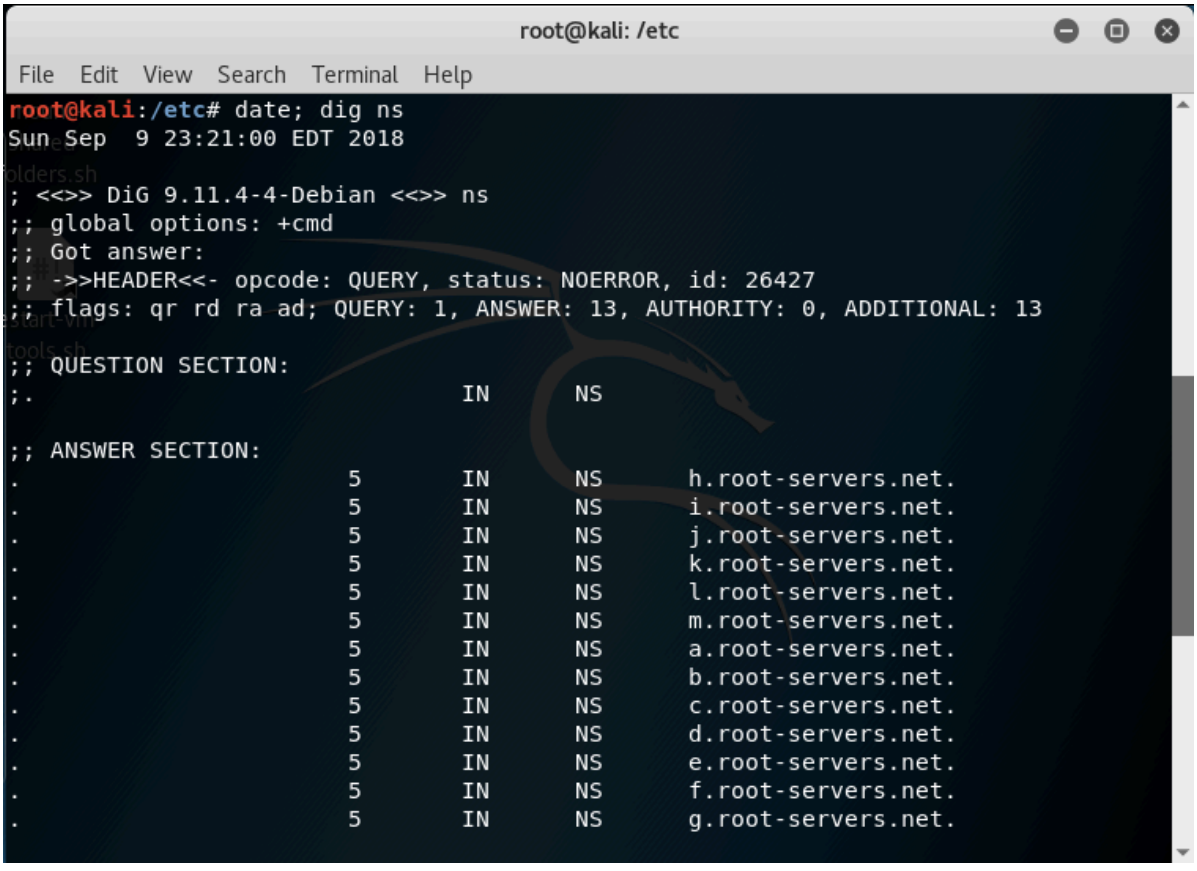
Directory of shadow: /etc/shadow
Directory of passwd: /etc/passwd

Description:

Passwd file contains essential information required login like useraccount information. It's a text file containing system's accounts giving each account some information like user ID, group ID. We can read it, but should have necessary permissions to write it.

Shadow file contains the actual password which is encrypted.

2.



```
;; ADDITIONAL SECTION:
a.root-servers.net.     5       IN      A       198.41.0.4
a.root-servers.net.     5       IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     5       IN      A       199.9.14.201
b.root-servers.net.     5       IN      AAAA    2001:500:200::b
c.root-servers.net.     5       IN      A       192.33.4.12
c.root-servers.net.     5       IN      AAAA    2001:500:2::c
d.root-servers.net.     5       IN      A       199.7.91.13
d.root-servers.net.     5       IN      AAAA    2001:500:2d::d
e.root-servers.net.     5       IN      A       192.203.230.10
e.root-servers.net.     5       IN      AAAA    2001:500:a8::e
f.root-servers.net.     5       IN      A       192.5.5.241
g.root-servers.net.     5       IN      A       192.112.36.4
g.root-servers.net.     5       IN      AAAA    2001:500:12::d0d

;; Query time: 18 msec
;; SERVER: 192.168.203.2#53(192.168.203.2)
;; WHEN: Sun Sep 09 23:21:00 EDT 2018
;; MSG SIZE  rcvd: 508

root@kali:/etc#
```

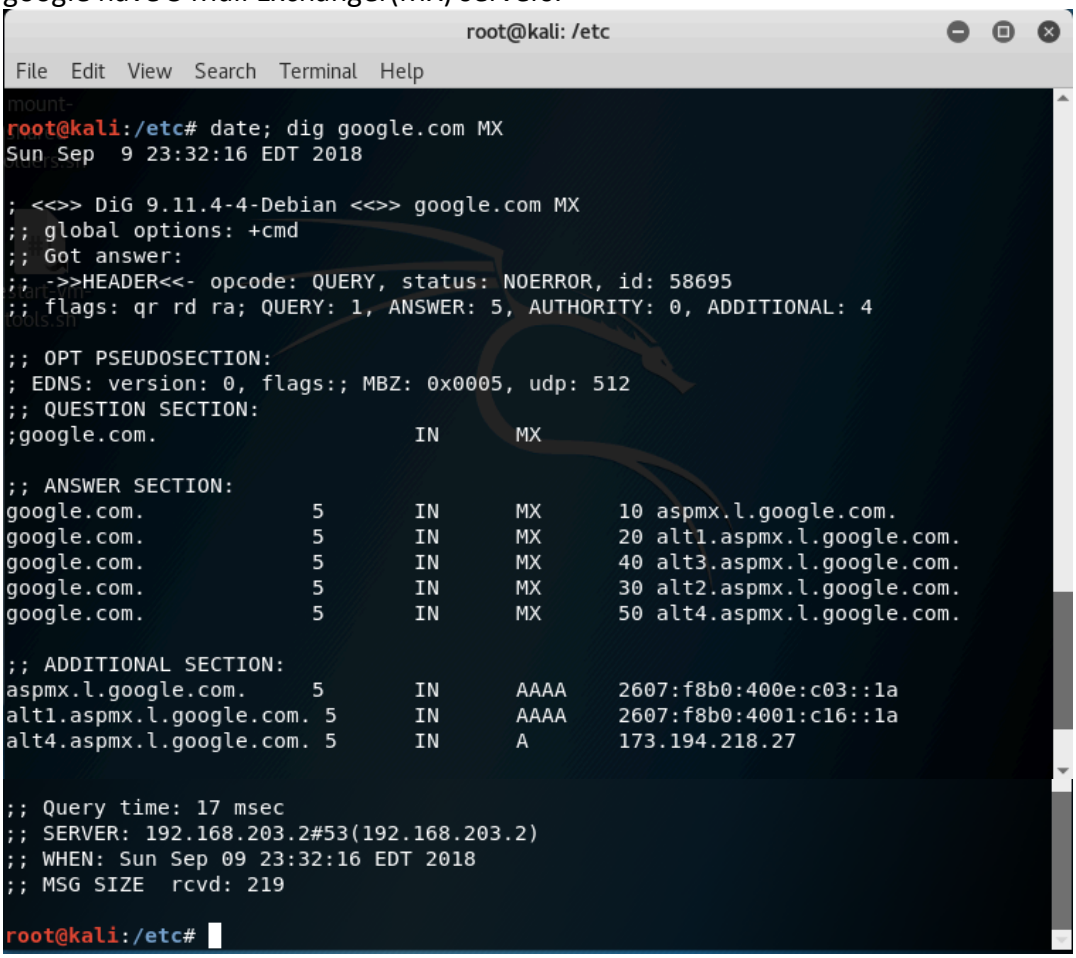
There are 13 root name servers.

8 in USA, 3 in Europe, 2 in ASIA

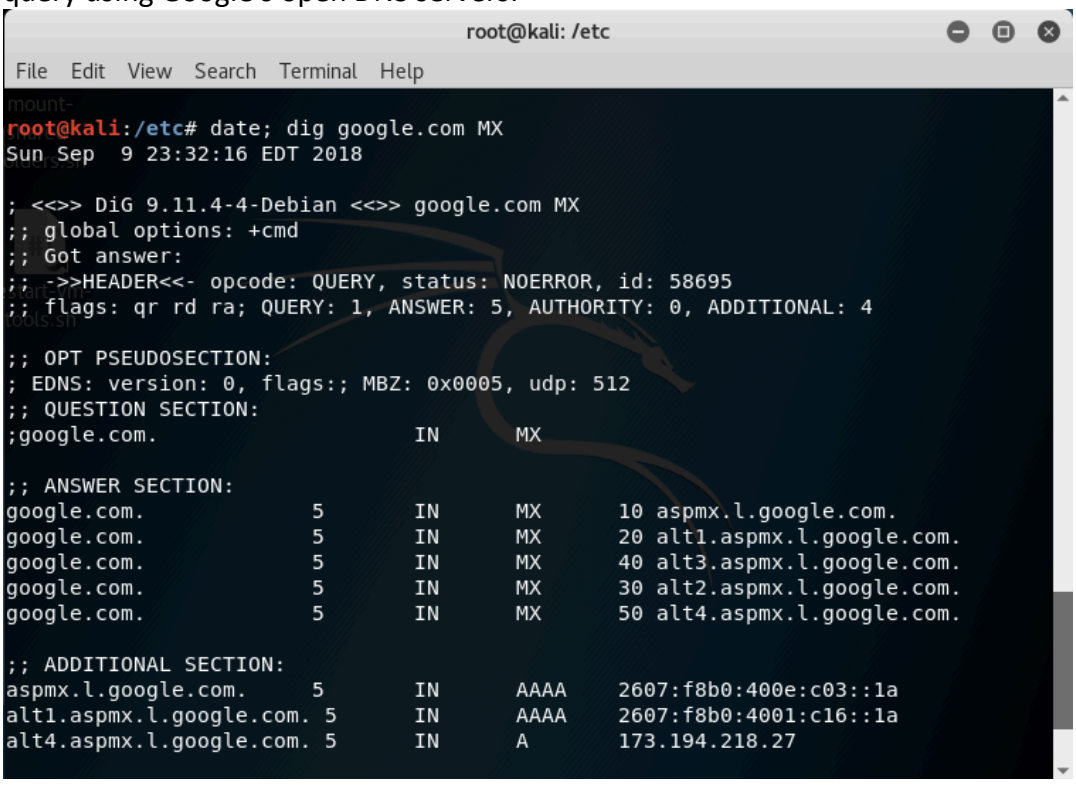
PLACES	COUNTS
USA	8
Europe	3
ASIA	2

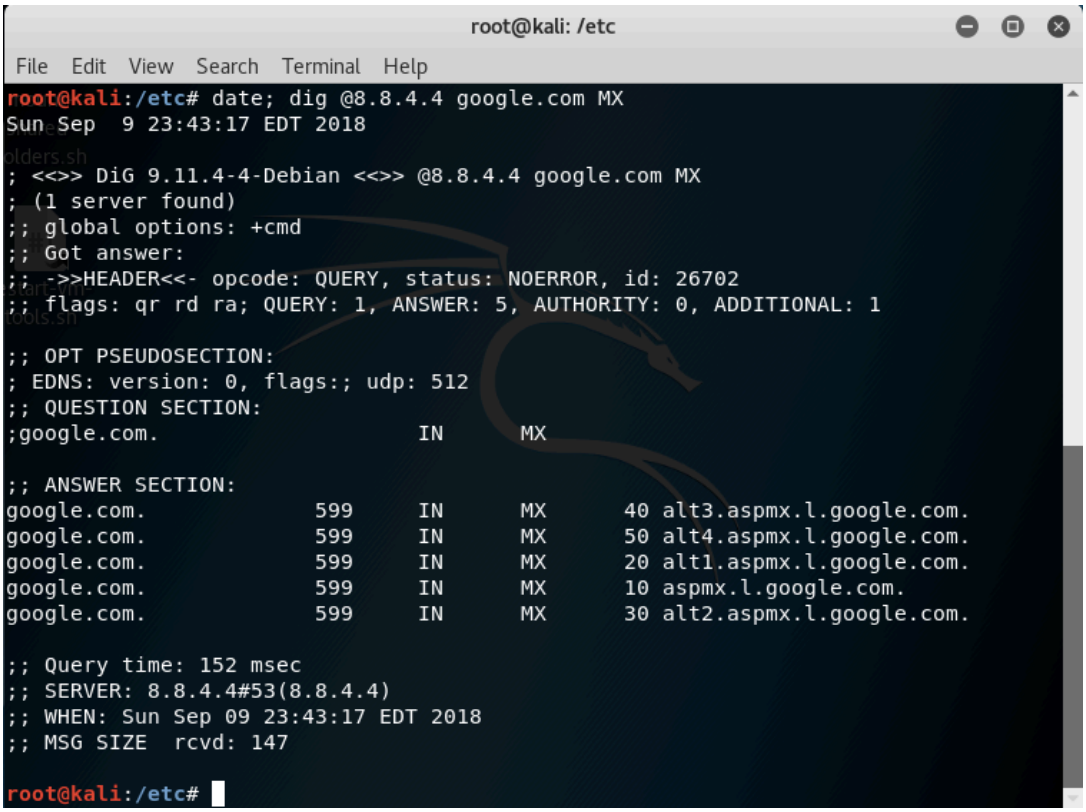
Ref :https://archive.icann.org/en/tlds/org/applications/uia/C17_5.html

3. google have 5 Mail Exchanger(MX) servers.



query using Google's open DNS servers:





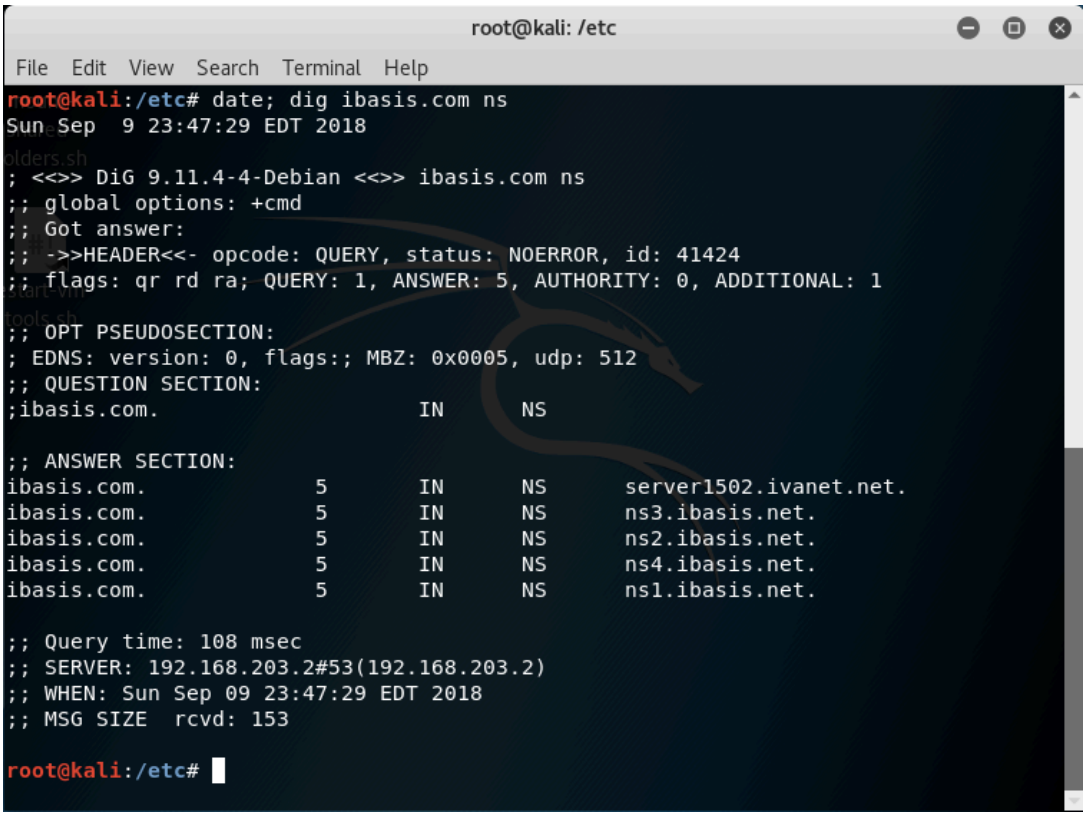
4. Ways to find the authoritative name server:

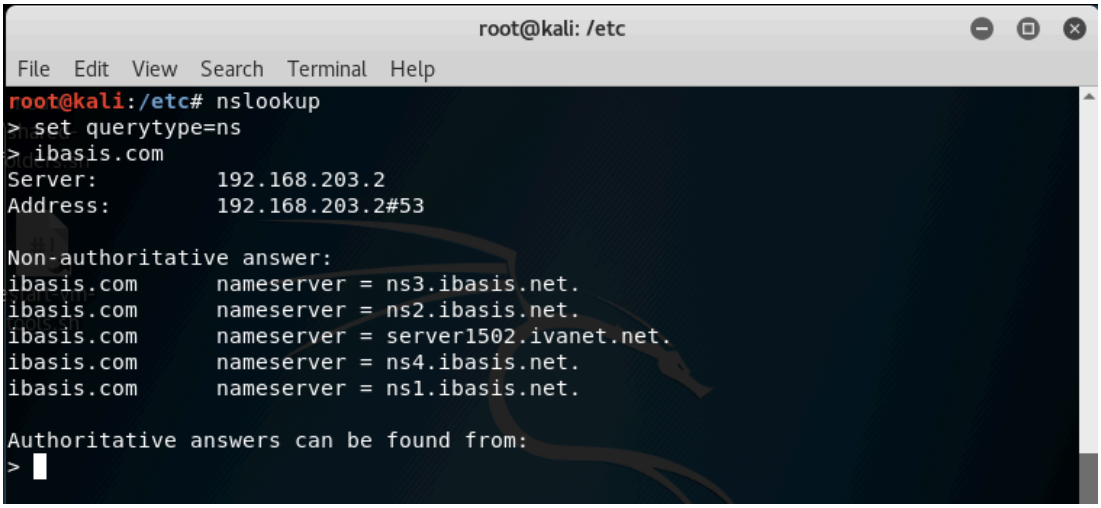
a. nslookup

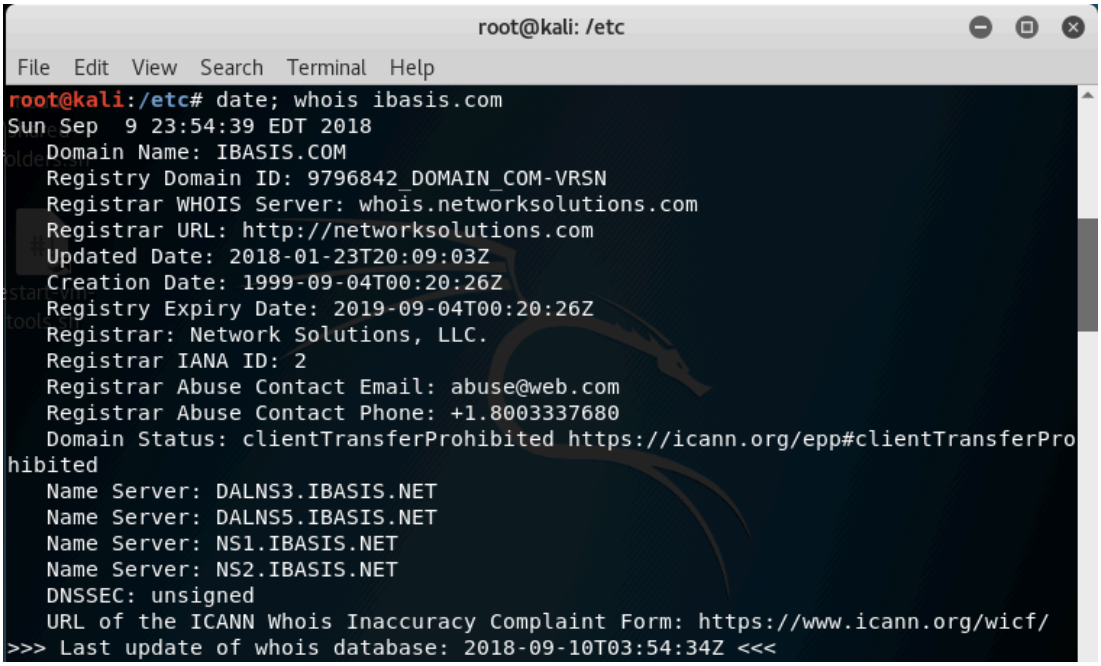
b. dig

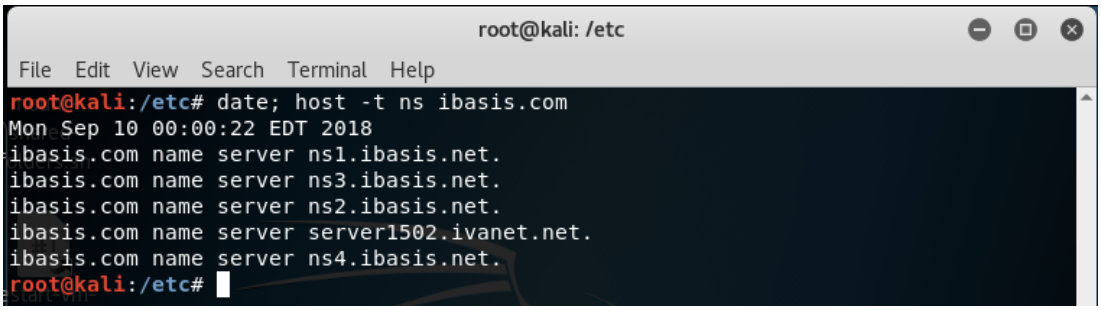
c. host

d. whois

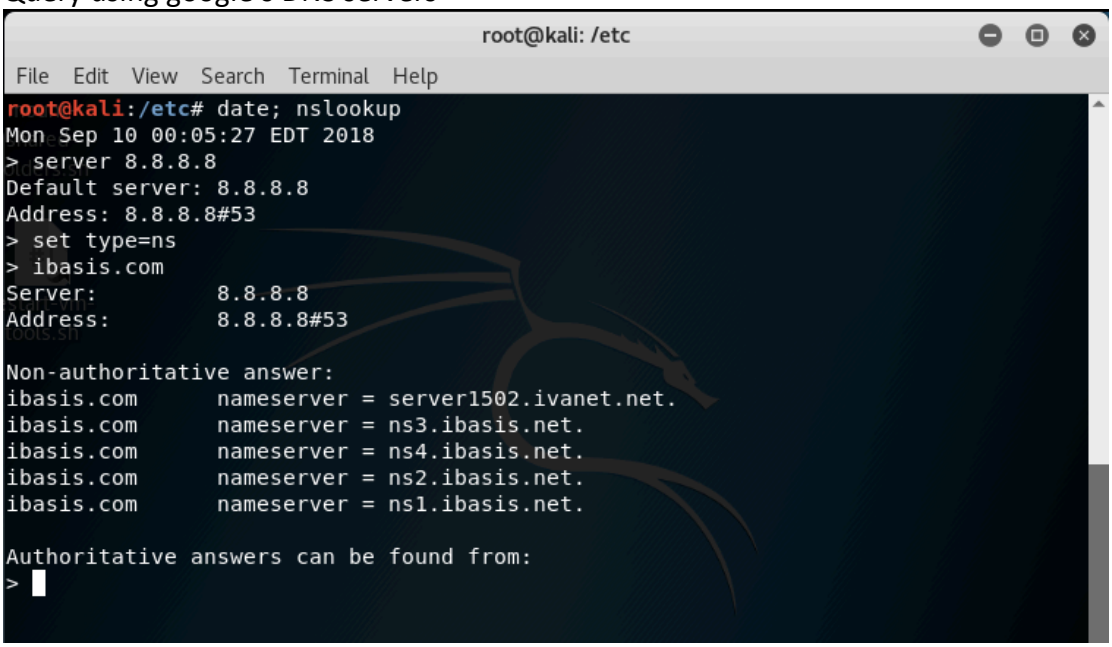



root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# nslookup
> set querytype=ns
> ibasis.com
Server: 192.168.203.2
Address: 192.168.203.2#53
Non-authoritative answer:
ibasis.com nameserver = ns3.ibasis.net.
ibasis.com nameserver = ns2.ibasis.net.
ibasis.com nameserver = server1502.ivanet.net.
ibasis.com nameserver = ns4.ibasis.net.
ibasis.com nameserver = ns1.ibasis.net.
Authoritative answers can be found from:
>

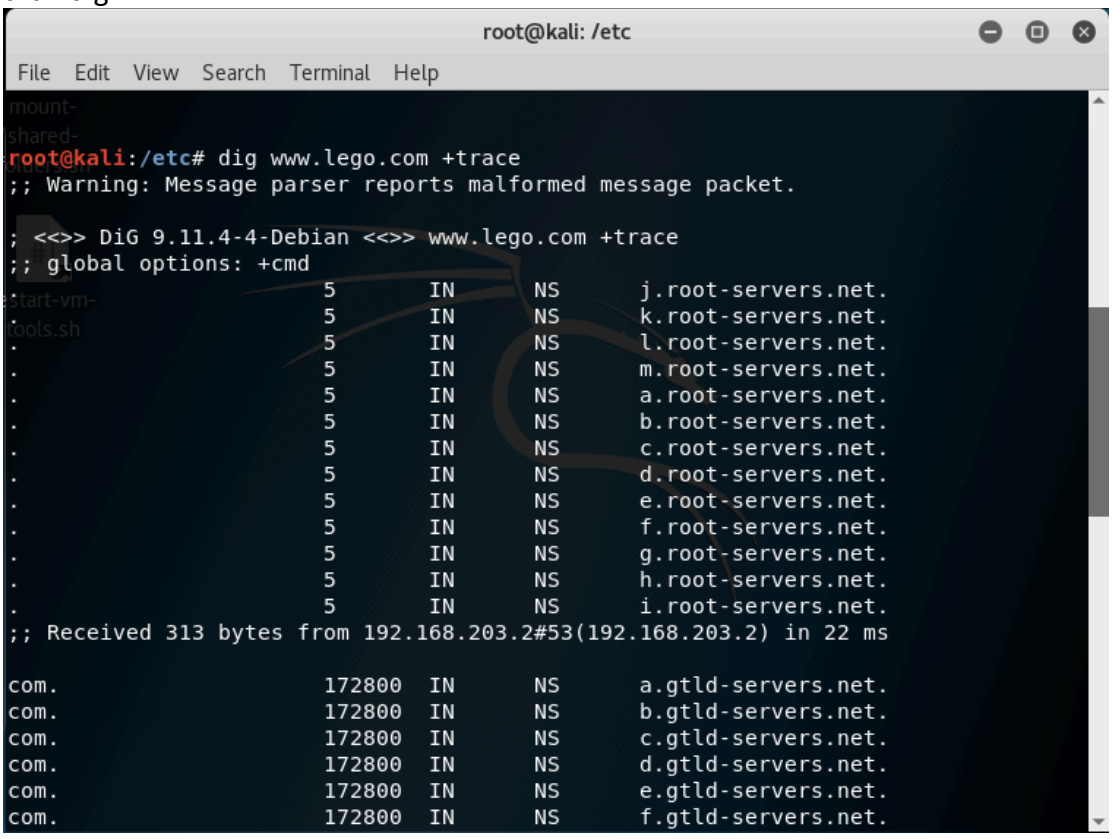

root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; whois ibasis.com
Sun Sep 9 23:54:39 EDT 2018
Domain Name: IBASIS.COM
Registry Domain ID: 9796842_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-01-23T20:09:03Z
Creation Date: 1999-09-04T00:20:26Z
Registry Expiry Date: 2019-09-04T00:20:26Z
Registrar: Network Solutions, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPro
hibited
Name Server: DALNS3.IBASIS.NET
Name Server: DALNS5.IBASIS.NET
Name Server: NS1.IBASIS.NET
Name Server: NS2.IBASIS.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-09-10T03:54:34Z <<<

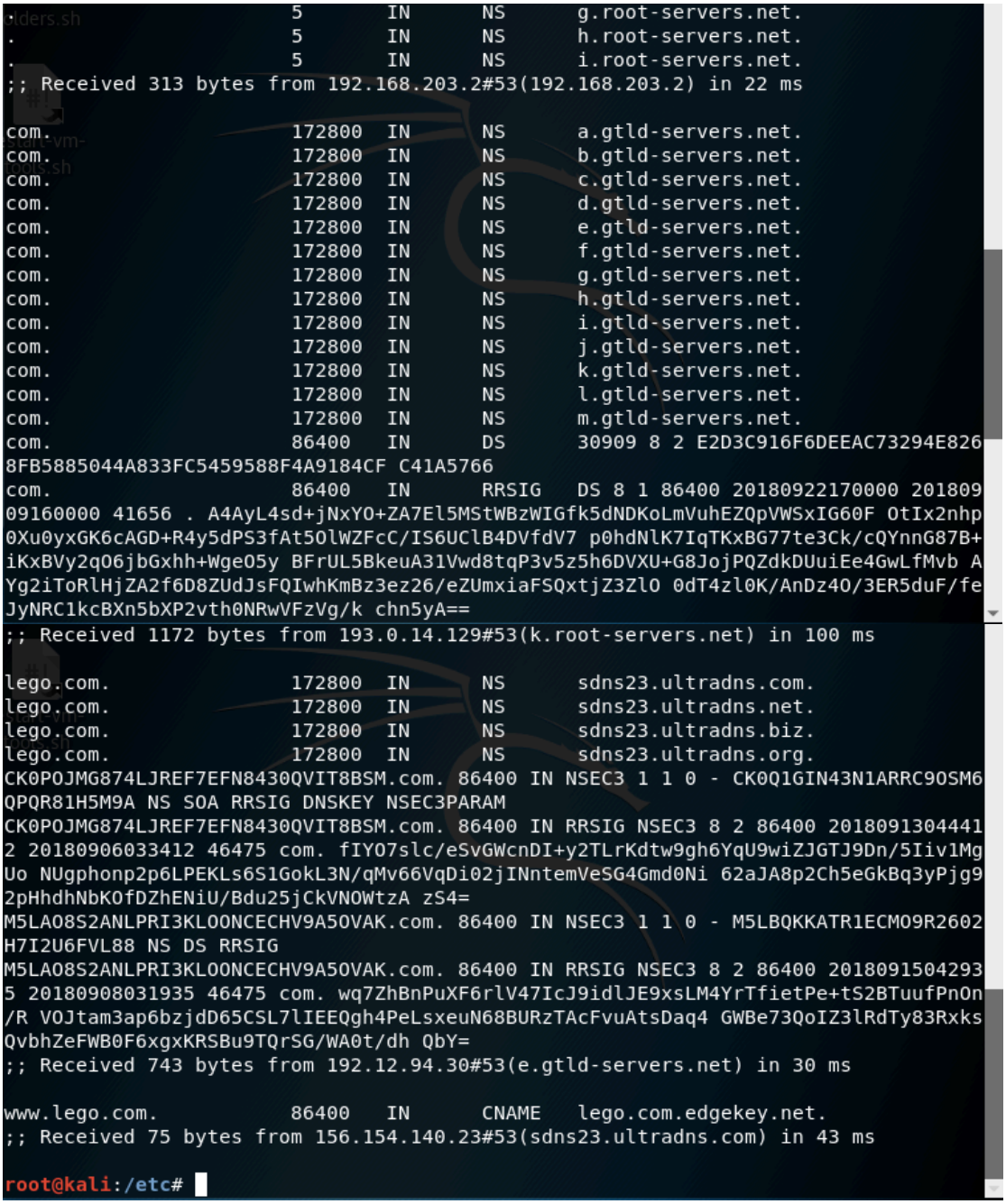

root@kali: /etc
File Edit View Search Terminal Help
root@kali:/etc# date; host -t ns ibasis.com
Mon Sep 10 00:00:22 EDT 2018
ibasis.com name server ns1.ibasis.net.
ibasis.com name server ns3.ibasis.net.
ibasis.com name server ns2.ibasis.net.
ibasis.com name server server1502.ivanet.net.
ibasis.com name server ns4.ibasis.net.
root@kali:/etc#

Query using google's DNS servers

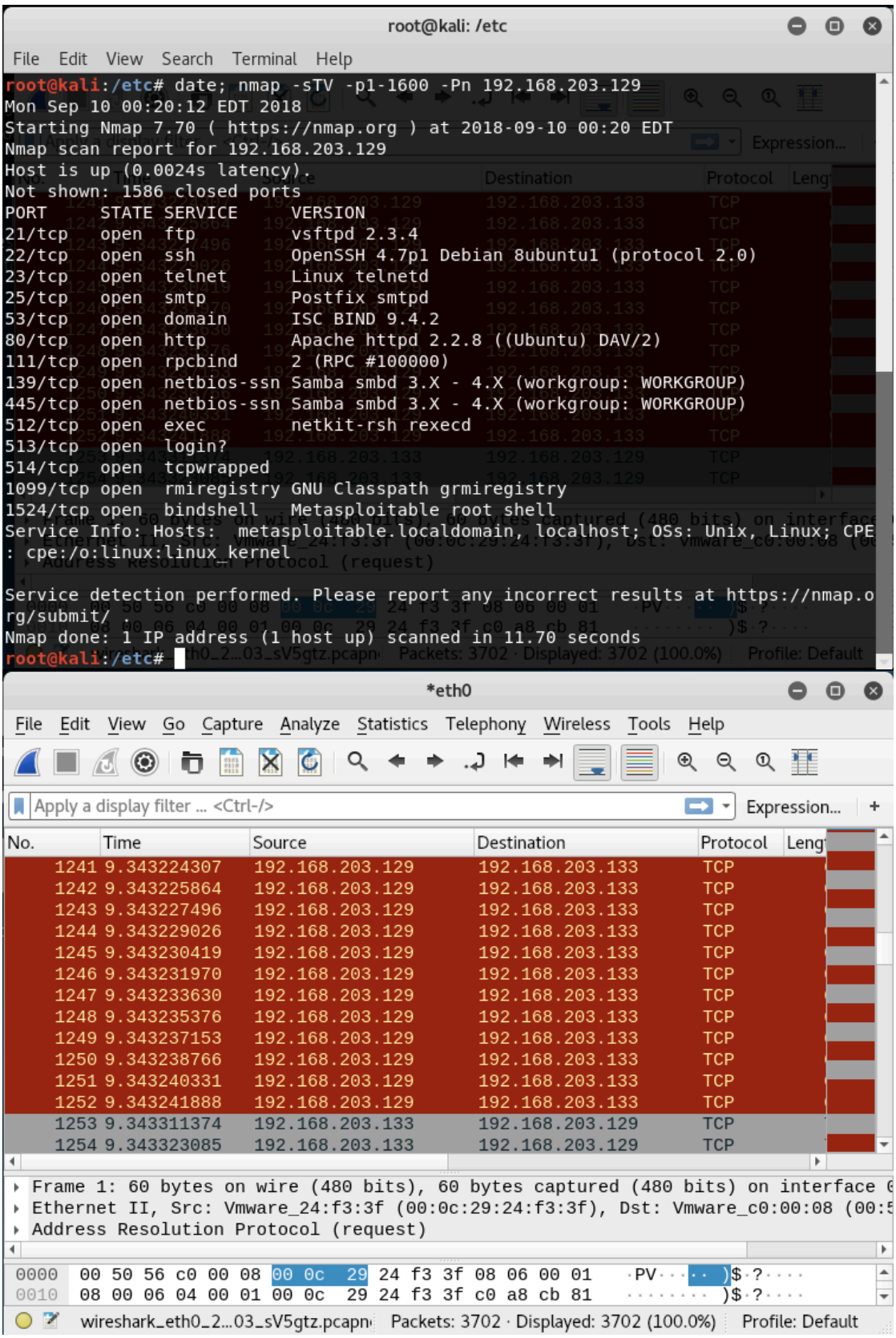


5. dig stands for "Domain Information Groper" flexible tool for interrogating DNS name servers. Most DNS administrators use dig to troubleshoot DNS problems.other lookup tools tend to have less functionality than dig.

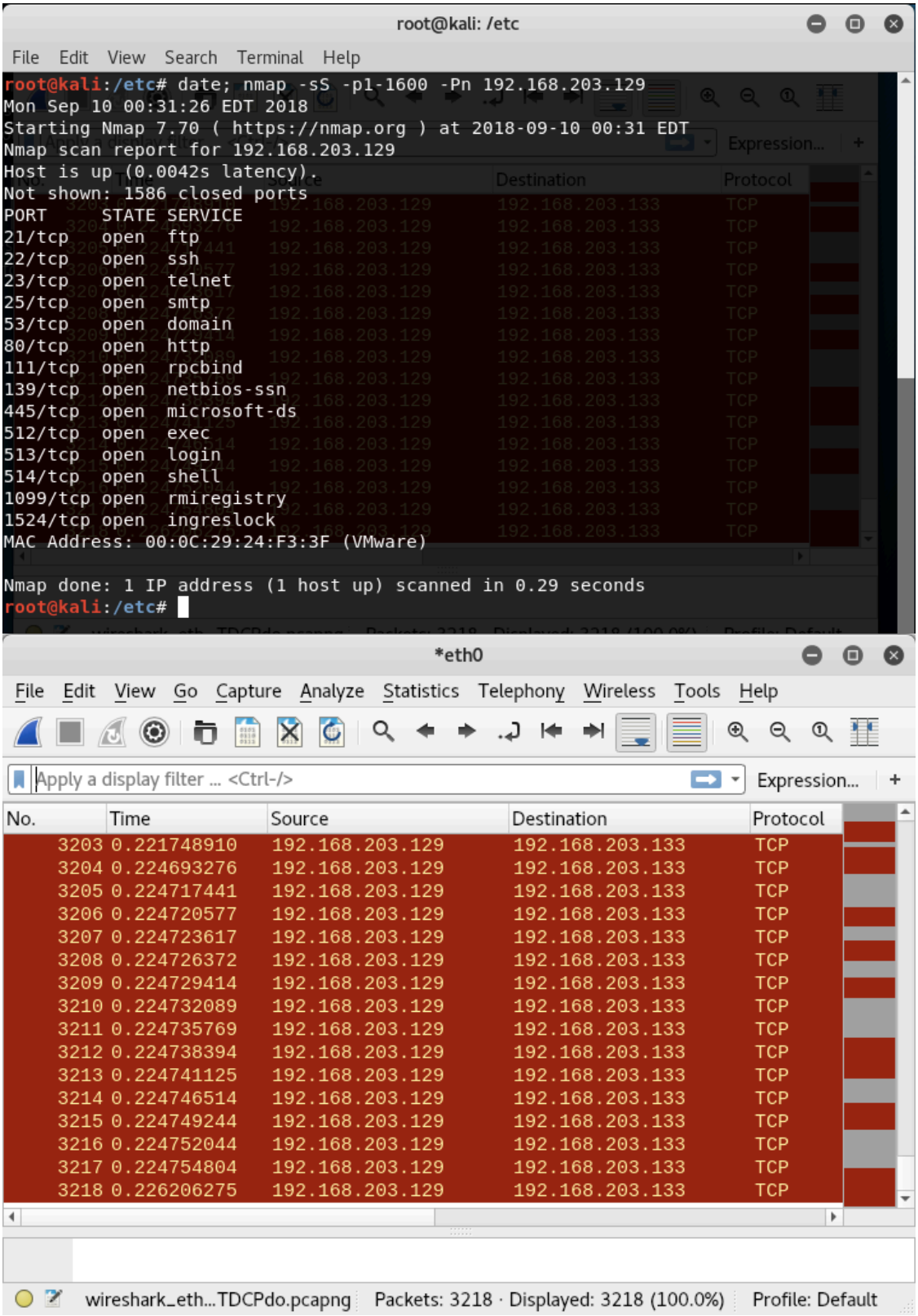



. 5 IN NS g.root-servers.net.
. 5 IN NS h.root-servers.net.
. 5 IN NS i.root-servers.net.
;; Received 313 bytes from 192.168.203.2#53(192.168.203.2) in 22 ms
com. 172800 IN NS a.gtld-servers.net.
com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS c.gtld-servers.net.
com. 172800 IN NS d.gtld-servers.net.
com. 172800 IN NS e.gtld-servers.net.
com. 172800 IN NS f.gtld-servers.net.
com. 172800 IN NS g.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS i.gtld-servers.net.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS k.gtld-servers.net.
com. 172800 IN NS l.gtld-servers.net.
com. 172800 IN NS m.gtld-servers.net.
com. 86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E826
8FB5885044A833FC5459588F4A9184CF C41A5766
com. 86400 IN RRSIG DS 8 1 86400 20180922170000 201809
09160000 41656 . A4AyL4sd+jNxYO+ZA7El5MStWBzWIGfk5dNDKoLmVuhEZQpVWSxIG60F OtIx2nhp
0Xu0yxGK6cAGD+R4y5dPS3fAt5OlWZFcC/IS6UClB4DVfdV7 p0hdNlK7IqTKxBG77te3Ck/cQYnnG87B+
iKxBVy2qO6jbGxhh+WgeO5y BFrUL5BkeuA31Vwd8tqP3v5z5h6DVXU+G8JojPQZdkDUuiEe4GwLfMvb A
Yg2iToRlHjZA2f6D8ZUdJsFQIwhKmBz3ez26/eZUmxiaFSQxtjZ3ZlO 0dT4zl0K/AnDz4O/3ER5duF/fe
JyNRC1kcBXn5bXP2vth0NRwVFzVg/k chn5yA==
;; Received 1172 bytes from 193.0.14.129#53(k.root-servers.net) in 100 ms
lego.com. 172800 IN NS sdns23.ultradns.com.
lego.com. 172800 IN NS sdns23.ultradns.net.
lego.com. 172800 IN NS sdns23.ultradns.biz.
lego.com. 172800 IN NS sdns23.ultradns.org.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6
QPQR81H5M9A NS SOA RRSIG DNSKEY NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 2018091304441
2 20180906033412 46475 com. fIYO7slc/eSvGWcnDI+y2TLrKdtw9gh6YqU9wiZJGTJ9Dn/5Iiv1Mg
Uo NUgphonp2p6LPEKLs6S1GokL3N/qMv66VqDi02jINntemVeSG4Gmd0Ni 62aJA8p2Ch5eGkBq3yPjg9
2pHhdhNbKOfDZhENiU/Bdu25jCkVNOWtzA zS4=
M5LAO8S2ANLPRI3KLOONCECHV9A5OVAK.com. 86400 IN NSEC3 1 1 0 - M5LBQKKATR1ECMO9R2602
H7I2U6FVL88 NS DS RRSIG
M5LAO8S2ANLPRI3KLOONCECHV9A5OVAK.com. 86400 IN RRSIG NSEC3 8 2 86400 2018091504293
5 20180908031935 46475 com. wq7ZhBnPuXF6rlV47IcJ9idlJE9xsLM4YrTfietPe+tS2BTuufPnOn
/R VOJtam3ap6bzjdD65CSL7lIEEQgh4PeLsxeuN68BURzTAcFvuAtsDaq4 GWBe73QoIZ3lRdTy83Rxks
QvbhZeFWB0F6xgxKRSBu9TQrSG/WA0t/dh QbY=
;; Received 743 bytes from 192.12.94.30#53(e.gtld-servers.net) in 30 ms
www.lego.com. 86400 IN CNAME lego.com.edgekey.net.
;; Received 75 bytes from 156.154.140.23#53(sdns23.ultradns.com) in 43 ms
root@kali:/etc#

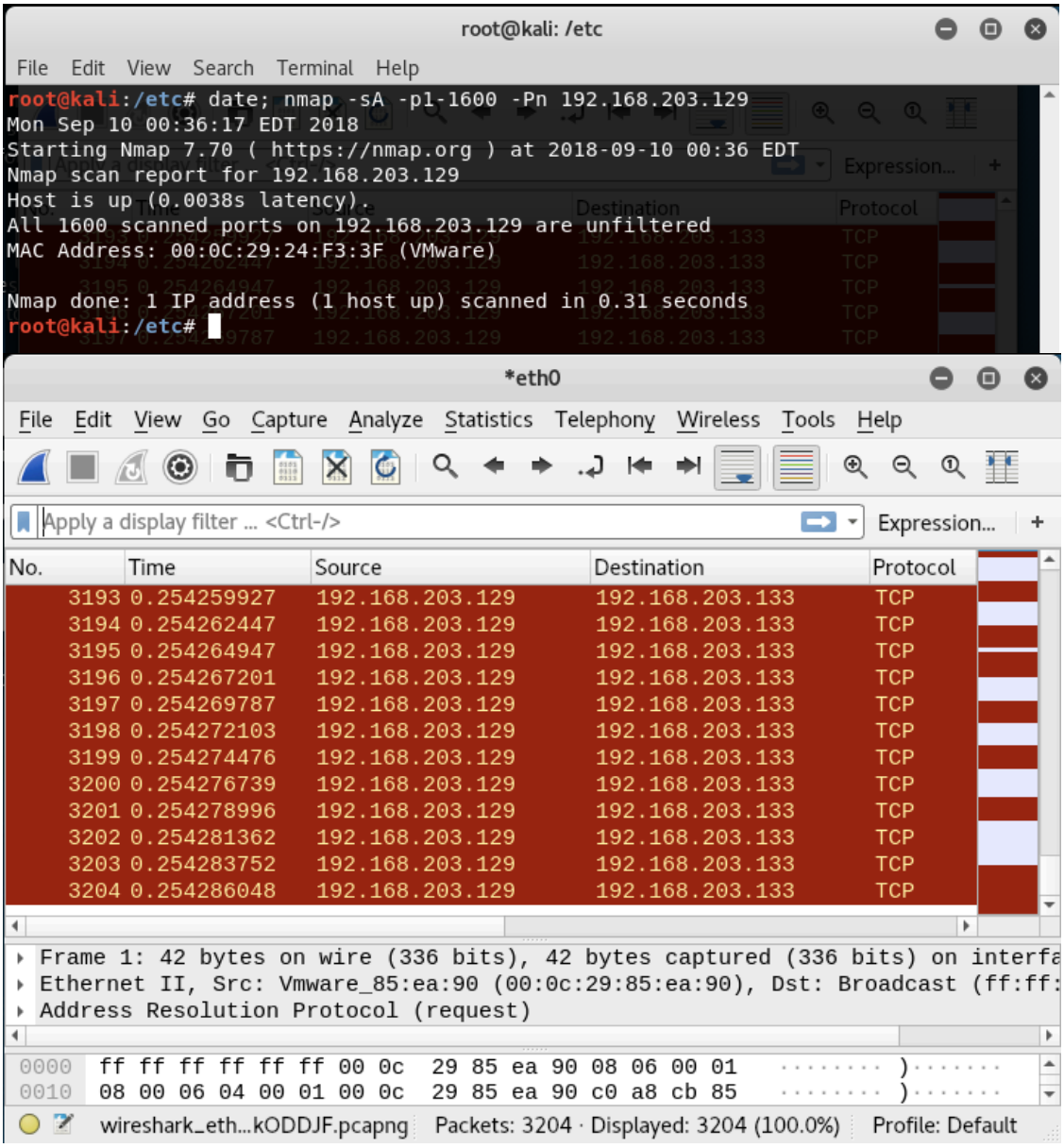
6. Using connect scan



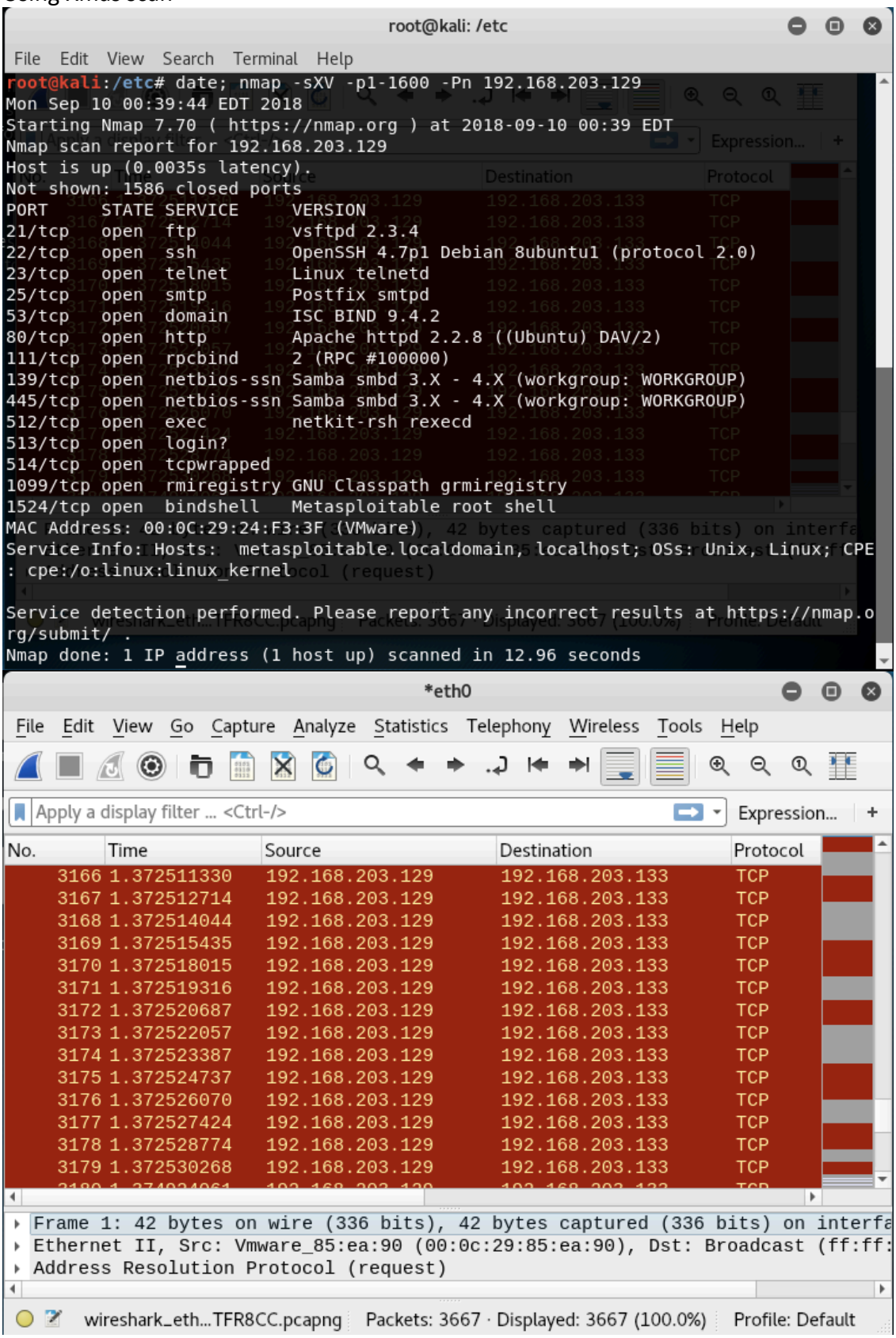
Using stealth scan



Using ACK Scan

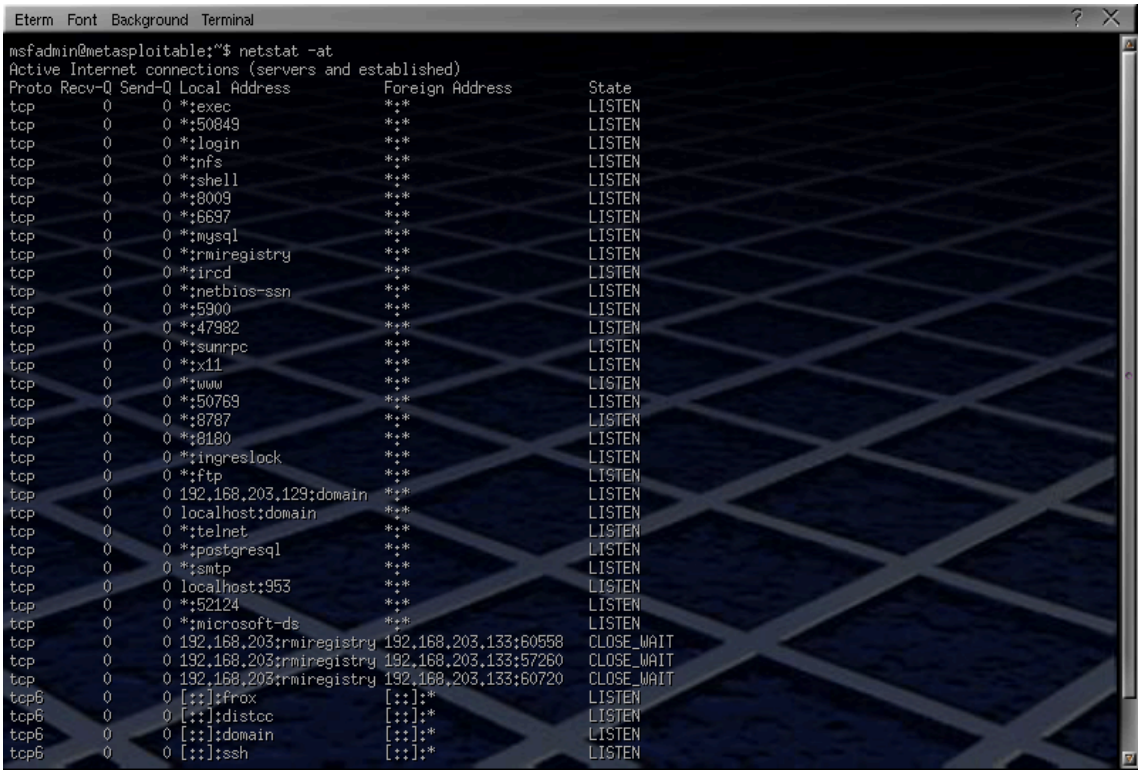


Using Xmas scan

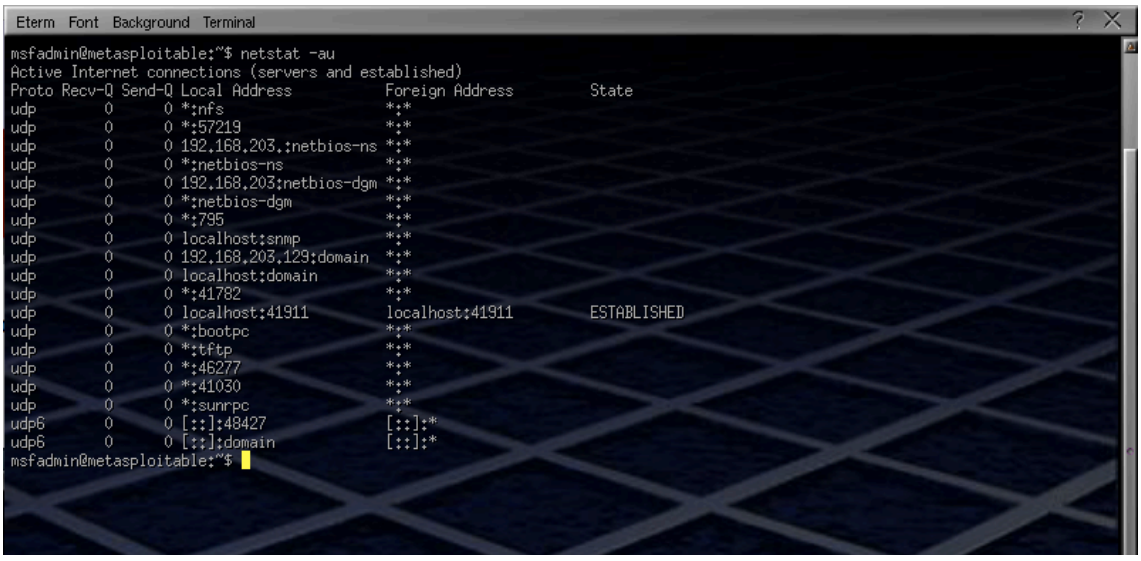


7.

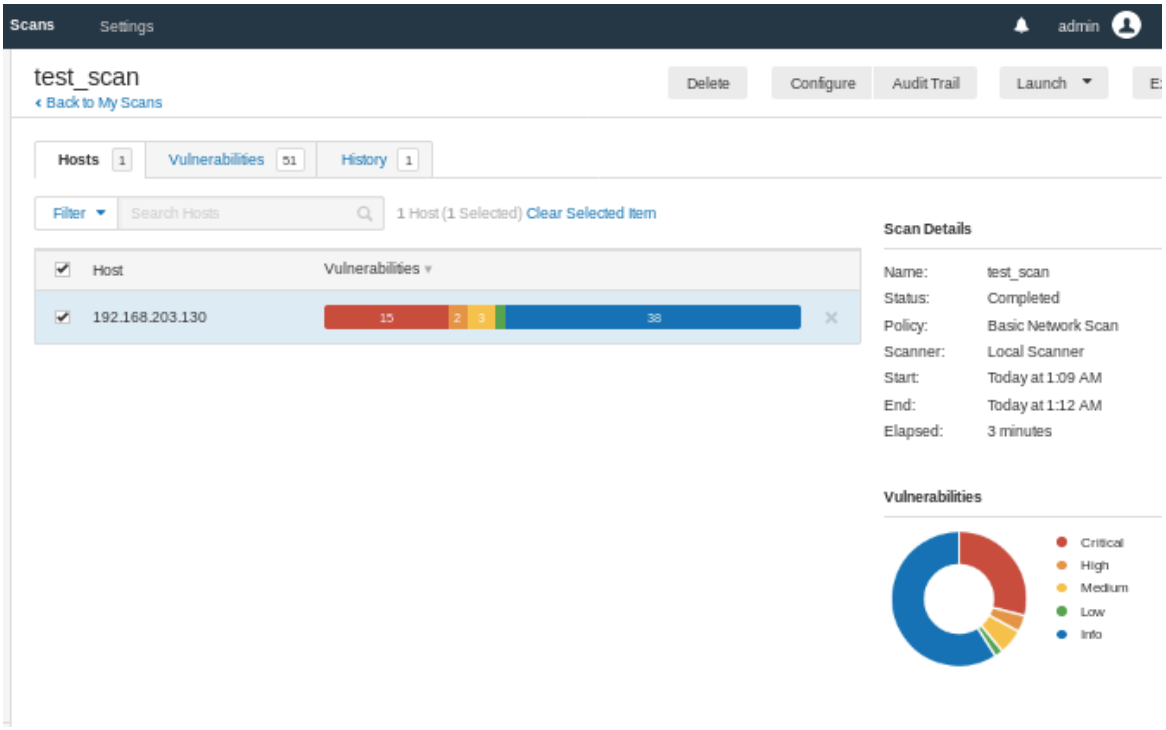
netstat -at : TCP

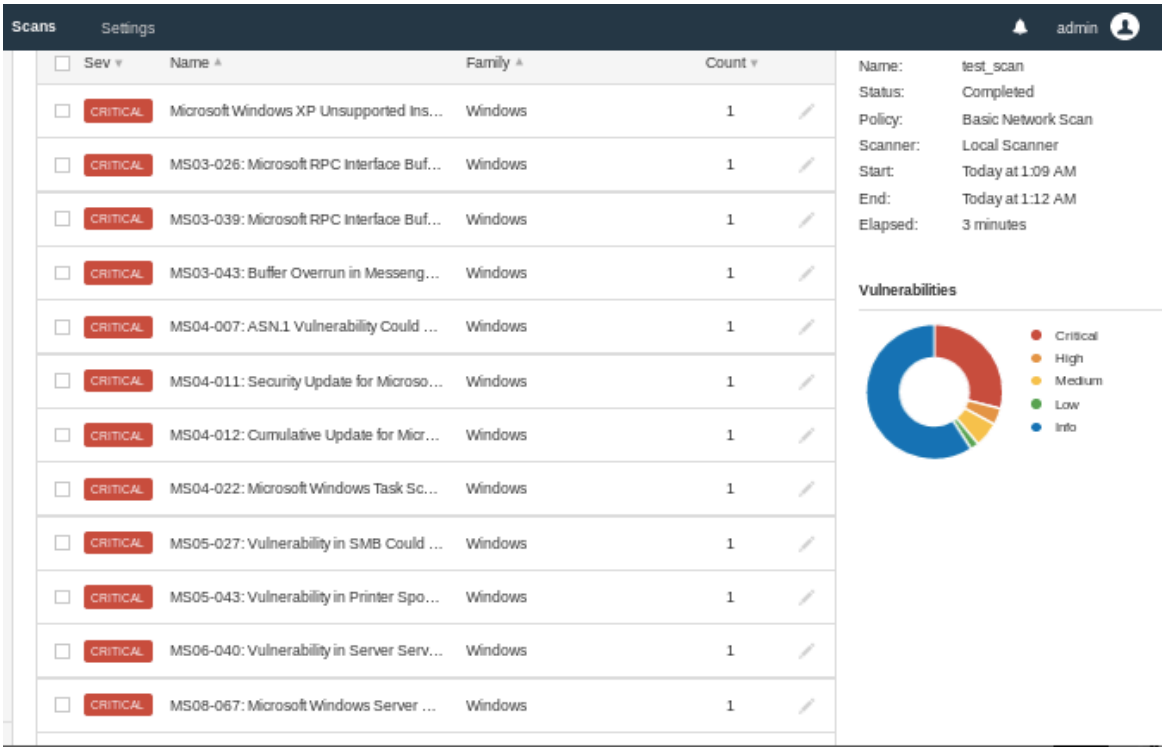


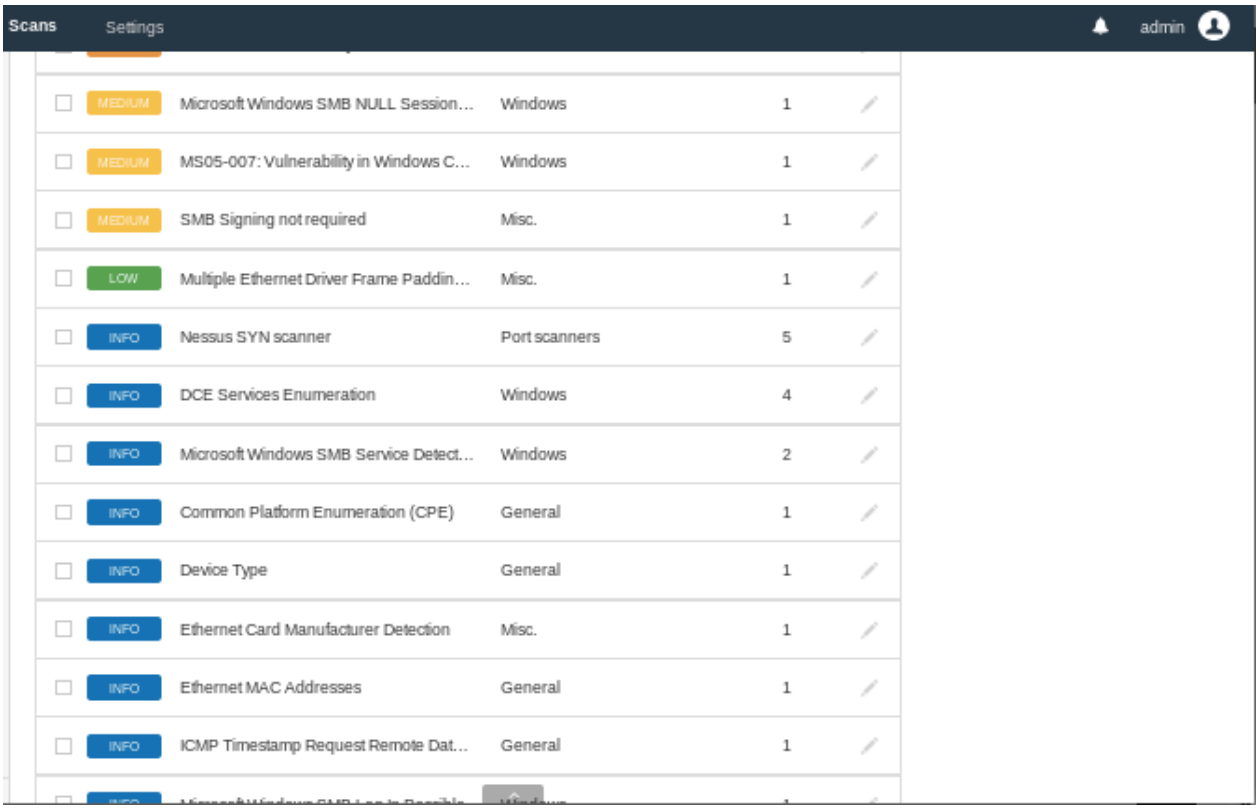
netstat -au : UDP

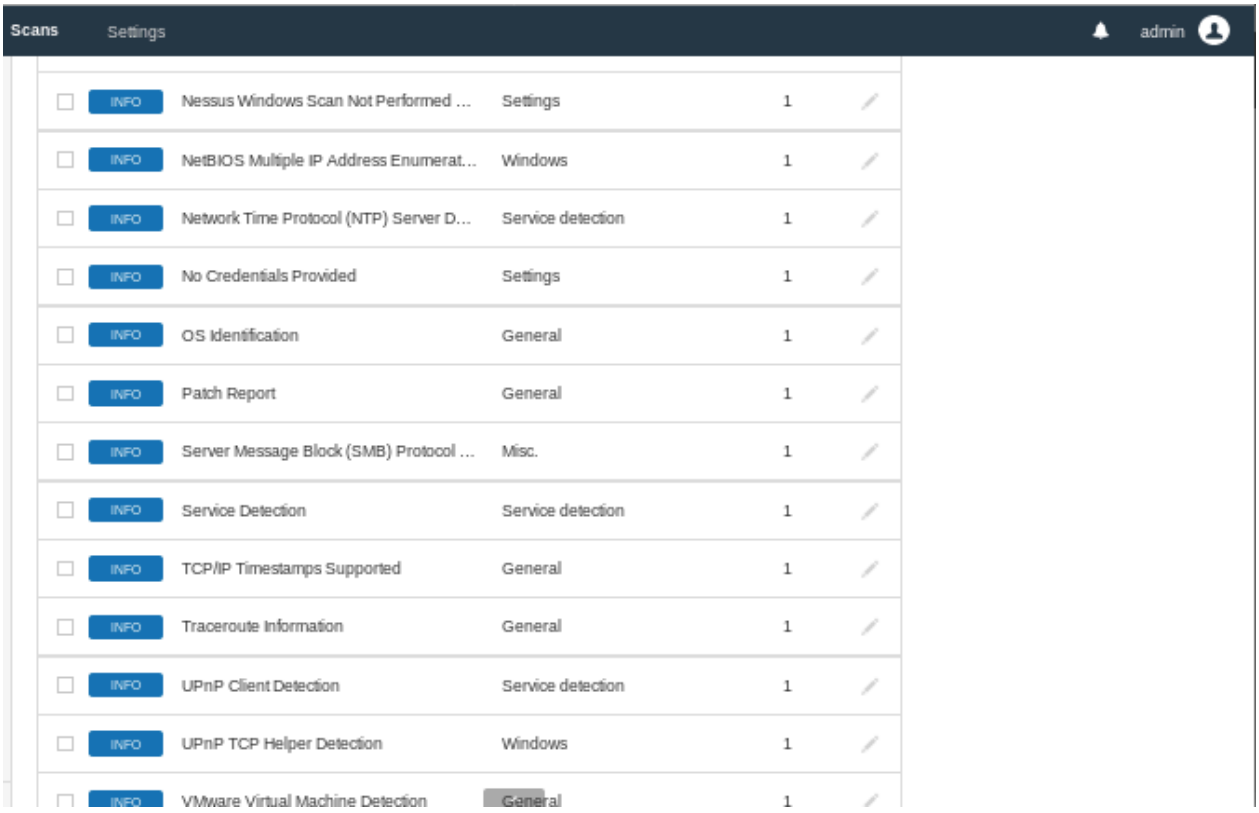


8.


Scans
Settings
admin
test_scan
Back to My Scans
Delete
Configure
Audit Trail
Launch
Hosts 1
Vulnerabilities 51
History 1
Filter
Search Hosts
1 Host (1 Selected) Clear Selected Item
Host
Vulnerabilities
192.168.203.130
15
2
3
38
Scan Details
Name: test_scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 1:09 AM
End: Today at 1:12 AM
Elapsed: 3 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Scans
Settings
admin
Sev
Name
Family
Count
CRITICAL Microsoft Windows XP Unsupported Ins... Windows 1
CRITICAL MS03-026: Microsoft RPC Interface Buf... Windows 1
CRITICAL MS03-039: Microsoft RPC Interface Buf... Windows 1
CRITICAL MS03-043: Buffer Overrun in Messeng... Windows 1
CRITICAL MS04-007: ASN.1 Vulnerability Could ... Windows 1
CRITICAL MS04-011: Security Update for Microso... Windows 1
CRITICAL MS04-012: Cumulative Update for Micr... Windows 1
CRITICAL MS04-022: Microsoft Windows Task Sc... Windows 1
CRITICAL MS05-027: Vulnerability in SMB Could ... Windows 1
CRITICAL MS05-043: Vulnerability in Printer Spo... Windows 1
CRITICAL MS06-040: Vulnerability in Server Serv... Windows 1
CRITICAL MS08-067: Microsoft Windows Server ... Windows 1
Name: test_scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 1:09 AM
End: Today at 1:12 AM
Elapsed: 3 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Scans
Settings
admin
MEDIUM Microsoft Windows SMB NULL Session… Windows 1
MEDIUM MS05-007: Vulnerability in Windows C… Windows 1
MEDIUM SMB Signing not required Misc. 1
LOW Multiple Ethernet Driver Frame Paddin… Misc. 1
INFO Nessus SYN scanner Port scanners 5
INFO DCE Services Enumeration Windows 4
INFO Microsoft Windows SMB Service Detect… Windows 2
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO Ethernet MAC Addresses General 1
INFO ICMP Timestamp Request Remote Dat… General 1


Scans
Settings
admin
INFO Nessus Windows Scan Not Performed … Settings 1
INFO NetBIOS Multiple IP Address Enumerat… Windows 1
INFO Network Time Protocol (NTP) Server D… Service detection 1
INFO No Credentials Provided Settings 1
INFO OS Identification General 1
INFO Patch Report General 1
INFO Server Message Block (SMB) Protocol … Misc. 1
INFO Service Detection Service detection 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
INFO UPnP Client Detection Service detection 1
INFO UPnP TCP Helper Detection Windows 1
INFO VMware Virtual Machine Detection General 1