



Capturing DNS

Capturing DNS

- » **What is DNS?**
- » **Capturing DNS with Wireshark**
 - You can filter via IP addresses
 - You can filter by port (53)
 - You can review the UDP stream

Capturing DNS

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dig

; <<>> DiG 9.8.4-rpz2+r1005.12-P1 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39910
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
.                IN      NS

;; ANSWER SECTION:
.                5      IN      NS      d.root-servers.net.
.                5      IN      NS      i.root-servers.net.
.                5      IN      NS      h.root-servers.net.
.                5      IN      NS      f.root-servers.net.
.                5      IN      NS      j.root-servers.net.
.                5      IN      NS      m.root-servers.net.
.                5      IN      NS      b.root-servers.net.
.                5      IN      NS      g.root-servers.net.
.                5      IN      NS      a.root-servers.net.
.                5      IN      NS      k.root-servers.net.
.                5      IN      NS      c.root-servers.net.
.                5      IN      NS      e.root-servers.net.
```

Capturing DNS

» Using tshark

- You can run tshark from the command line. By running a simple dig, accessing a website, or attempting to access a resource by DNS name, you will capture DNS-related data.

» Possible issues

- Poisoned DNS server
- Failed DNS server
- Stale records

Capturing DNS

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# tshark
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to ru
nning Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/Capture
Privileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
  0.000000 192.168.73.128 -> 255.255.255.255 UDP 79 Source port: 35222  Destinat
ion port: hpvmmcontrol
  1  10.300184 192.168.73.128 -> 192.168.73.2 DNS 59 Standard query 0x9be6  NS <Ro
ot>
  10.302628 192.168.73.2 -> 192.168.73.128 DNS 491 Standard query response 0x9be6
  NS d.root-servers.net NS i.root-servers.net NS h.root-servers.net NS f.root-se
rvers.net NS j.root-servers.net NS m.root-servers.net NS b.root-servers.net NS g
.root-servers.net NS a.root-servers.net NS k.root-servers.net NS c.root-servers.
net NS e.root-servers.net NS l.root-servers.net
  3  15.307628 Vmware_ce:8e:45 -> Vmware_fb:a2:ce ARP 42 Who has 192.168.73.2?  Te
ll 192.168.73.128
  15.307820 Vmware_fb:a2:ce -> Vmware_ce:8e:45 ARP 60 192.168.73.2 is at 00:50:56
:fb:a2:ce
5
```

Questions?