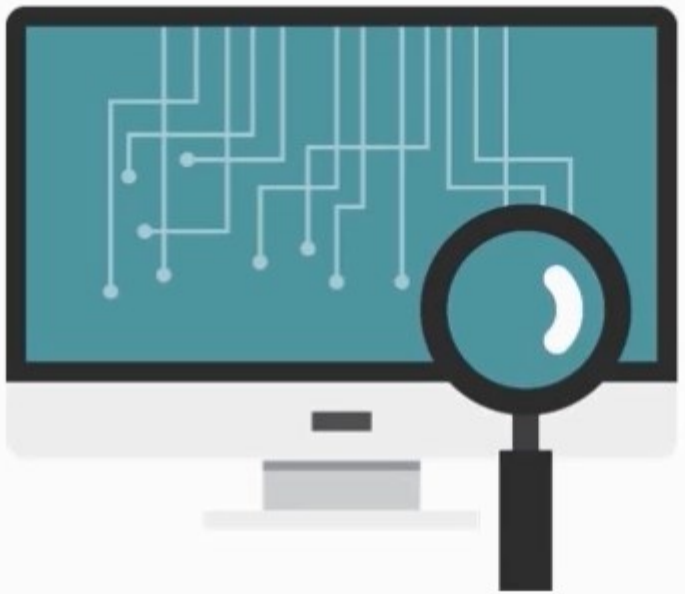
Enumerate This!



What is enumeration?

How does enumeration work?

What can we learn from enumeration?

Technologies that we can enumerate

What Do You Mean By "Enumeration"?

- This technique is usually conducted internally
- Requires an active connection
- Attacker then directly queries the target
  - Looks for remote IPC$ shares
  - Looks for services that offer up data
  - Create a Null session

What Do You Mean By "Enumeration"?

Looking at a target expose:

- ✓ Usernames
- ✓ Groups
- ✓ Machine names
- ✓ Network resources
- ✓ Services running

What Do You Mean By "Enumeration"?

Looking at a target expose:

- ✓ Routing tables
- ✓ Auditing services
- ✓ Applications
- ✓ DNS & SNMP info

The Techniques of Enumeration

What Are Possible Weaknesses?

Email/business cards

Brute force Active Directory

DNS zone transfers

SNMP

Windows groups

Default passwords

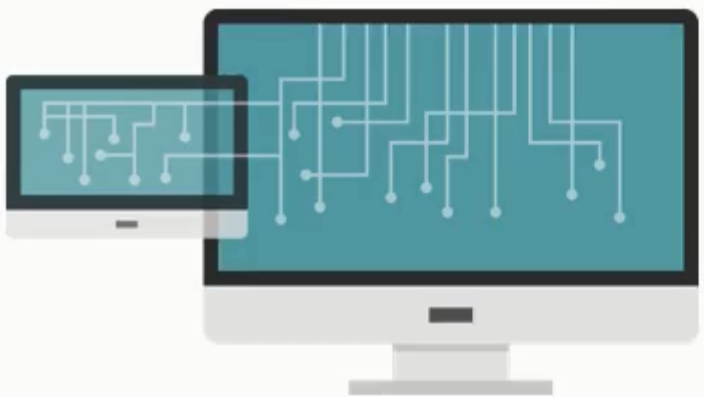
Know Your Ports and Services

Know Your Ports and Services!

DNS zone transfers	SMTP	MS RPC Endpoint	Global Catalog Service	NetBIOS Naming Service
• TCP 53	• TCP 25	• TCP 135	• TCP/UDP 3368	• TCP 137

LDAP	SMB over NetBIOS	SNMP	SMB over TCP
• TCP/UDP 389	• TCP 139	• UDP 161	• TCP 445

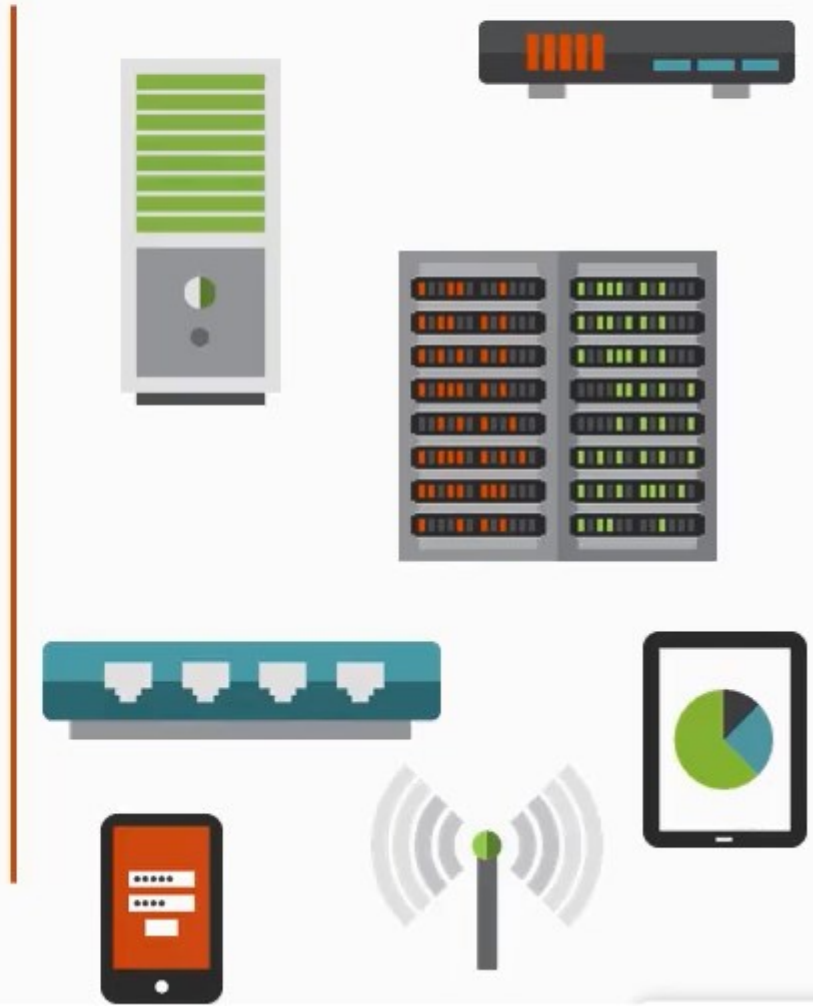
You'll Never Guess My…



- Defaults: Your Biggest Security Issue
- The "Art of Misdirection"
- What Is NetBIOS – a Review
- DEMO: Using Built-in commands
- DEMO: Pulling SID's and User Accounts
- DEMO: NetBIOS Enumeration Tool
- DEMO: SuperScan Tool

Complacency Will Be Your Downfall

- How many devices/software?
- Every device has a default
- NEVER leave default user accounts or passwords



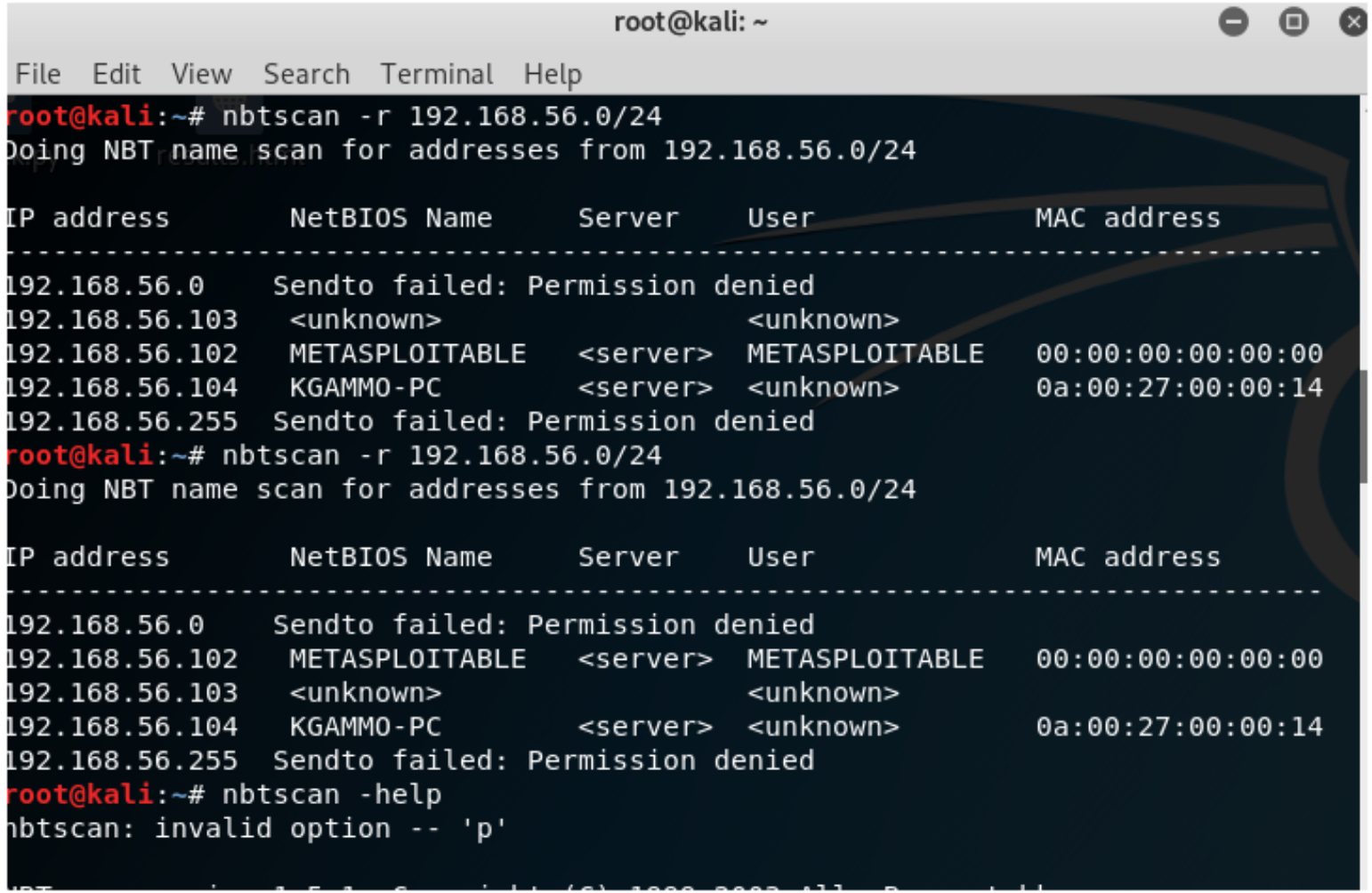
The “Art of Misdirection”

- What’s the default SSID for a Linksys wireless router?
- What would someone “assume” if I used the username of “root”?
- What if I named my Samsung Tablet “iPad”?

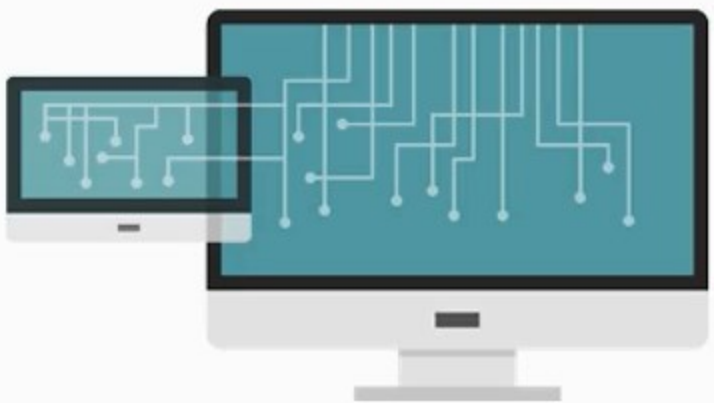
What Is NetBIOS – a Review

Now…what Is NetBIOS?

- Network Basic Input/Output System
  - IBM – Microsoft - Novell
  - Used by “client for Microsoft networks”
    - File and print services
  - Included in a most operating systems

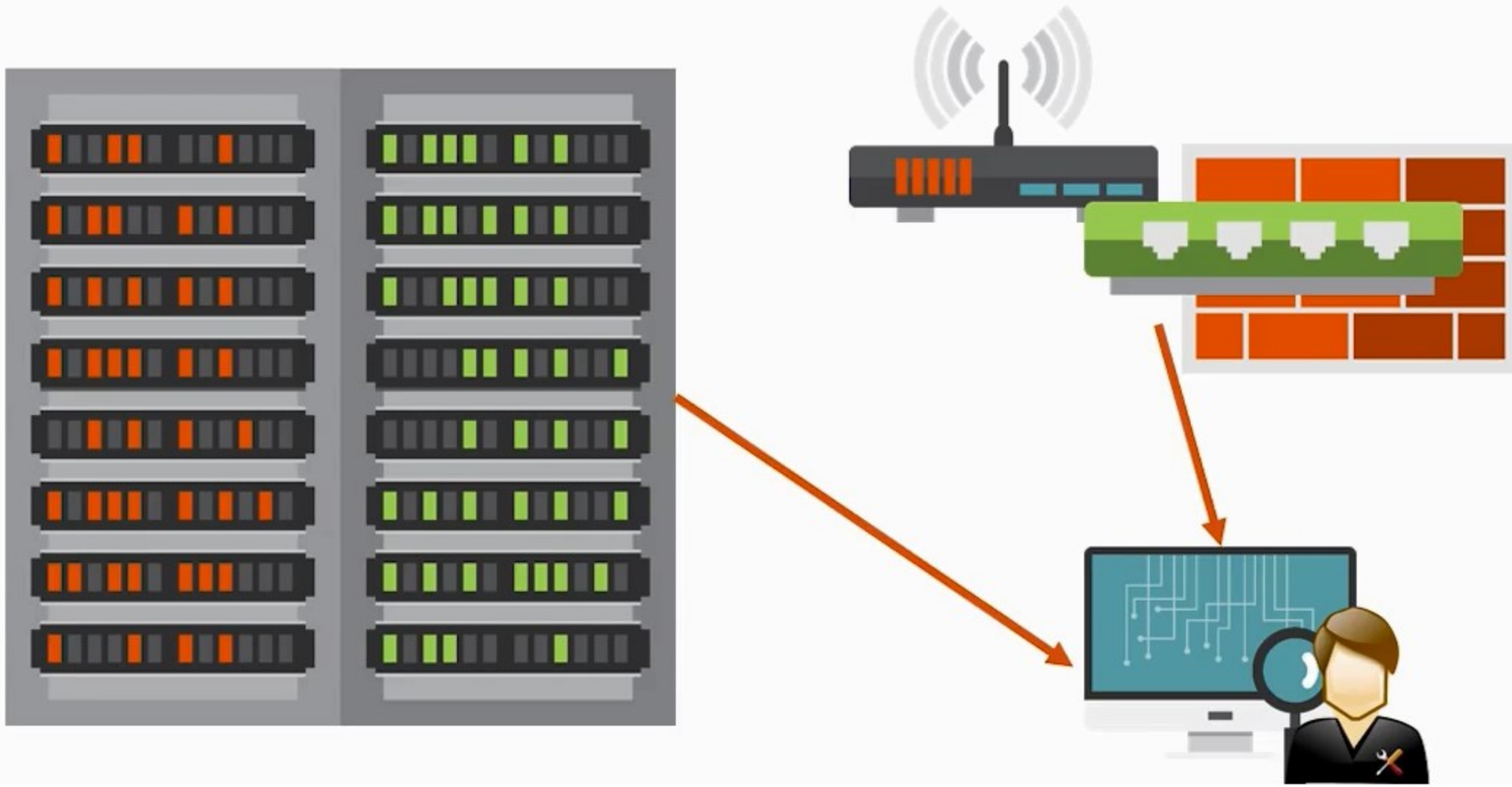

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nbtscan -r 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.0 Sendto failed: Permission denied
192.168.56.103 <unknown> <unknown>
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.104 KGAMMO-PC <server> <unknown> 0a:00:27:00:00:14
192.168.56.255 Sendto failed: Permission denied
root@kali:~# nbtscan -r 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24
IP address NetBIOS Name Server User MAC address
192.168.56.0 Sendto failed: Permission denied
192.168.56.102 METASPLOITABLE <server> METASPLOITABLE 00:00:00:00:00:00
192.168.56.103 <unknown> <unknown>
192.168.56.104 KGAMMO-PC <server> <unknown> 0a:00:27:00:00:14
192.168.56.255 Sendto failed: Permission denied
root@kali:~# nbtscan -help
nbtscan: invalid option -- 'p'

What's the Deal With SNMP?



- What Is SNMP?
- MIB's?
- DEMO: SNMP Enumeration

Simple Network Management Protocol



Security of SNMP (or Lack Thereof)

Depends on the version:

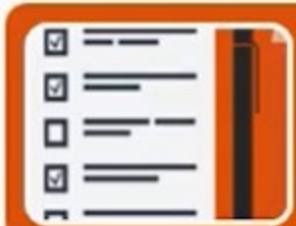
- Version1
  - Simple / basic
- Version2
  - Same as v1 but enhancements
- Both use community strings
  - Public – public
  - Private - private
- Version3
  - Restricted user access
  - Data encryption in transit
  - More complex to configure
  - Common issue –disable v1/v2

MIB’s?

I Make This Look Good

Uses a virtual database that contains official explanation of all the network objects

MIB Hierarchical – Each managed object in a MIB is addressed via OIDs



OIDs include the type of object, counter, string or address, and access levels

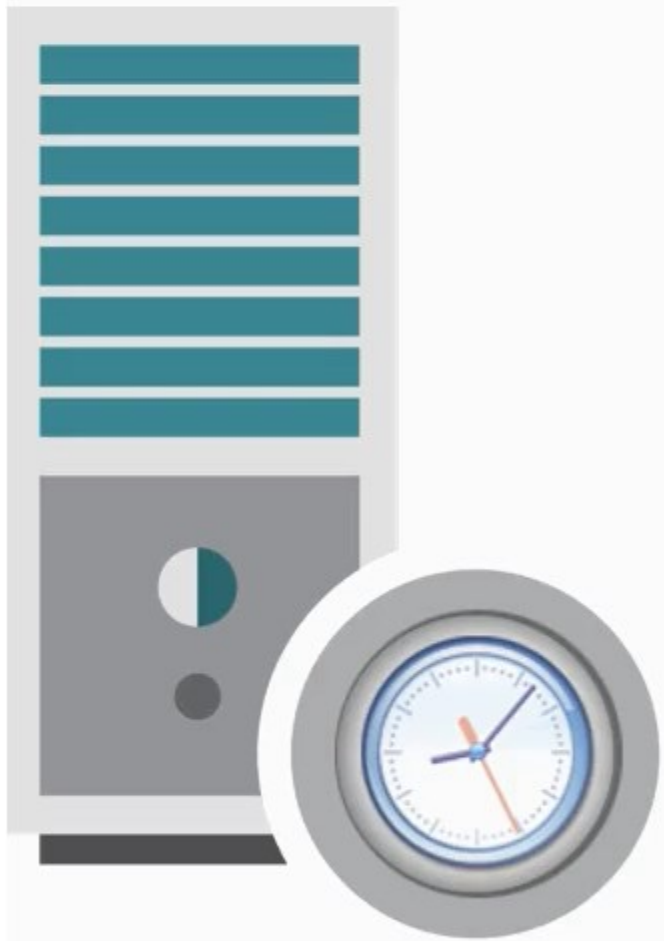
Used by SNMP to convert OID numbers into plain human language

Time Warp!

- What Is NTP?
- What can we learn from NTP?
- DEMO: Enumerating NTP

What Is NTP?

Network Time Protocol (NTP)



- Protocol that synchronizes time on all networked systems
- Extremely important to directory services
- Default NTP server in Windows will be the DC flagged as the PDC Emulator

Behind NTP

Ports

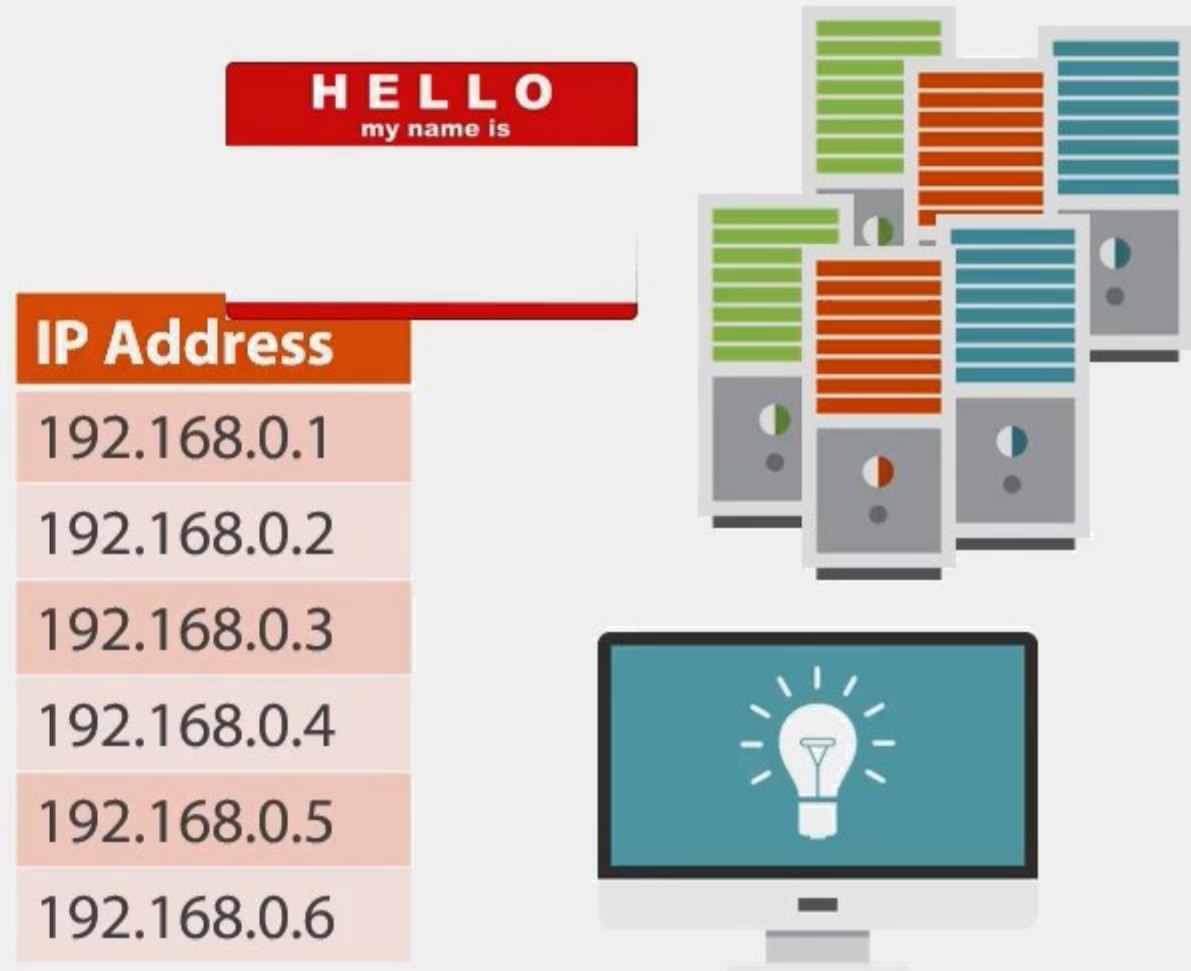
- UDP 123

Extremely accurate

- Private Networks / 200µs
- Public Networks / 10ms

What Can We Learn from NTP?

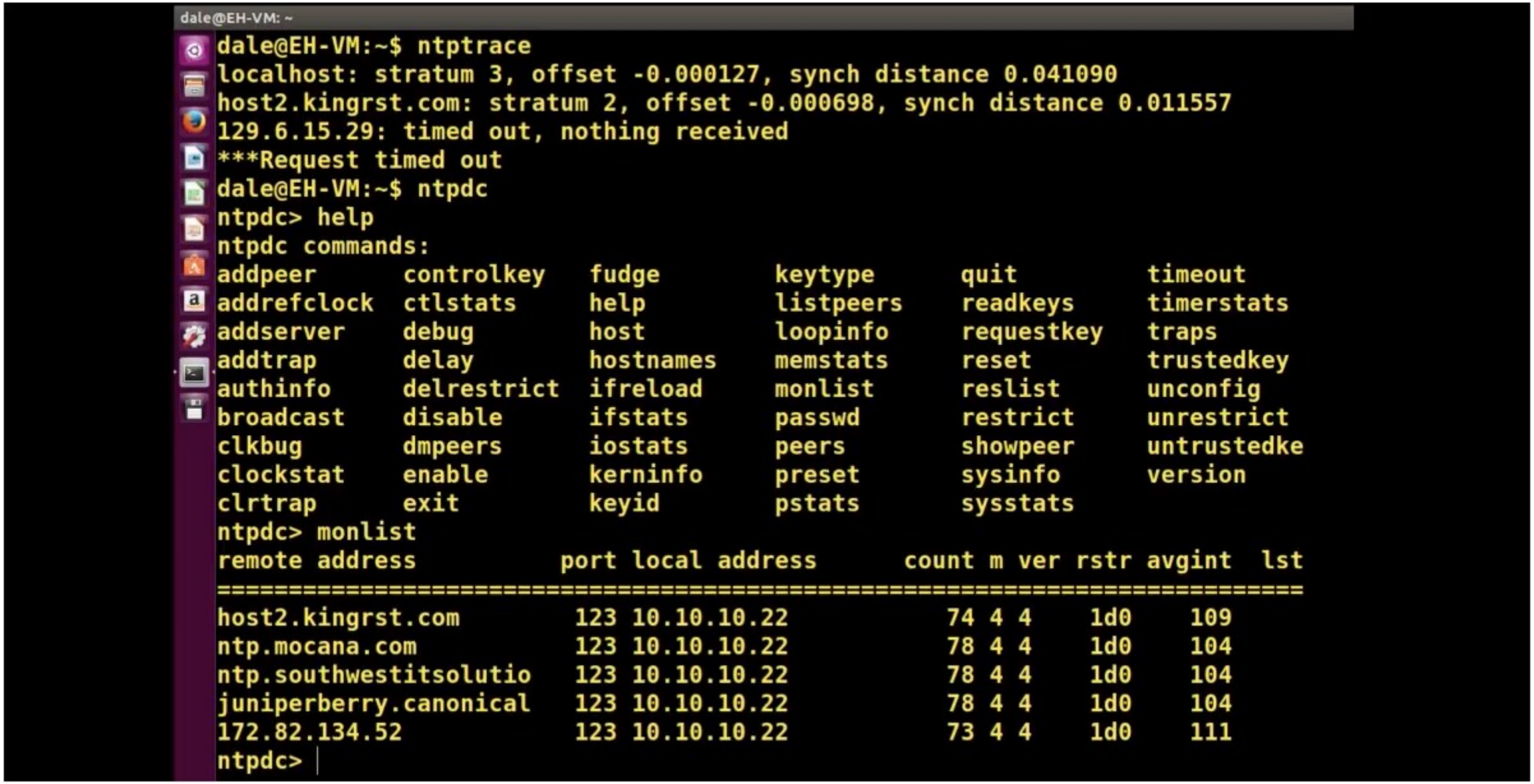
- List of hosts
- IP addresses
- System names
- Operating systems



DEMO: Enumerating NTP

Using NTP command we'll:

- Trace the chain of NTP servers
- Query the NTP Daemon and it's state
- Monitor the NTP Daemon


dale@EH-VM: ~
dale@EH-VM:~$ ntptrace
localhost: stratum 3, offset -0.000127, synch distance 0.041090
host2.kingrst.com: stratum 2, offset -0.000698, synch distance 0.011557
129.6.15.29: timed out, nothing received
***Request timed out
dale@EH-VM:~$ ntpdc
ntpdc> help
ntpdc commands:
addpeer controlkey fudge keytype quit timeout
addrefclock ctlstats help listpeers readkeys timerstats
addserver debug host loopinfo requestkey traps
addtrap delay hostnames memstats reset trustedkey
authinfo delrestrict ifreload monlist reslist unconfig
broadcast disable ifstats passwd restrict unrestrict
clkbug dmpeers iostats peers showpeer untrustedke
clockstat enable kerninfo preset sysinfo version
clrtrap exit keyid pstats sysstats
ntpdc> monlist
remote address port local address count m ver rstr avgint lst
host2.kingrst.com 123 10.10.10.22 74 4 4 1d0 109
ntp.mocana.com 123 10.10.10.22 78 4 4 1d0 104
ntp.southwestitsolutio 123 10.10.10.22 78 4 4 1d0 104
juniperberry.canonical 123 10.10.10.22 78 4 4 1d0 104
172.82.134.52 123 10.10.10.22 73 4 4 1d0 111
ntpdc>

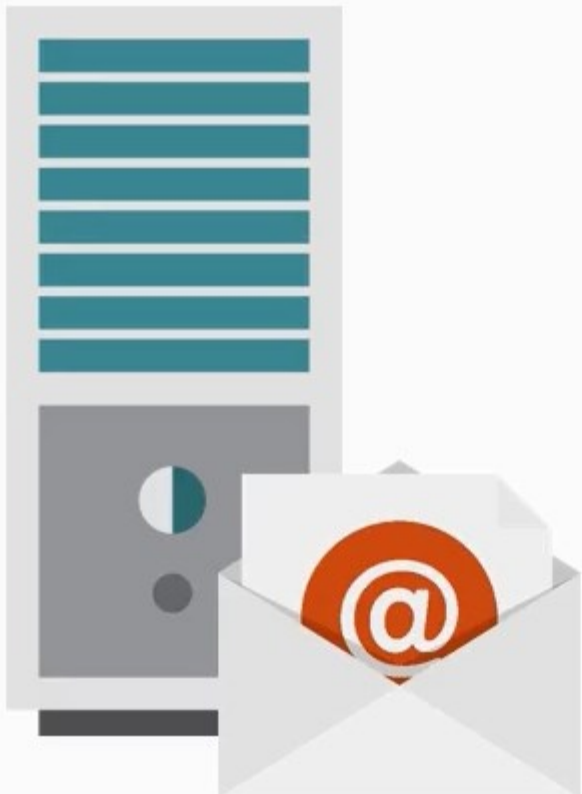
```
dale@EH-VM:~$ ntpq
ntpq> help
ntpq commands:
:config           delay             mreadvar          readlist
addvars           exit              mrl               readvar
associations      help              mrv               rl
authenticate      host              ntpversion        rmvars
cl                hostnames         opeers            rv
clearvars         keyid             passociations     saveconfig
clocklist         keytype           passwd            showvars
clockvar          lassociations     peers             timeout
config-from-file  lopeers           poll              version
cooked            lpassociations    pstatus           writelist
cv                lpeers            quit              writevar
debug             mreadlist         raw
ntpq> host
current host is localhost
ntpq> version
ntpq 4.2.6p5@1.2349-o Mon Apr 13 17:00:21 UTC 2015 (1)
ntpq> readlist
associd=0 status=0618 leap_none, sync_ntp, 1 event, no_sys_peer,
version="ntpd 4.2.6p5@1.2349-o Mon Apr 13 17:00:14 UTC 2015 (1)",
processor="x86_64", system="Linux/3.19.0-15-generic", leap=00, stratum=3,
precision=-21, rootdelay=81.406, rootdisp=94.197, refid=69.167.160.102,
reftime=d973b2f8.6e8d41b6  Mon, Aug 10 2015 17:32:08.431,
clock=d973b3f3.f4bd2eb2  Mon, Aug 10 2015 17:36:19.956, peer=61452, tc=9,
mintc=3, offset=-0.563, frequency=4.375, sys_jitter=2.045,
clk_jitter=3.302, clk_wander=1.014
ntpq> peers
     remote           refid      st t when poll reach   delay   offset  jitt
==============================================================================
+172.82.134.52   152.2.133.54     2 u  593  256  374   94.528    2.115   4.1
-ntp.mocana.com  209.151.225.100  3 u   21  512  377   42.166   -6.272  12.3
-ntp.southwestit 67.18.187.111    3 u   28  512  377   51.706   -3.488   0.8
*host2.kingrst.c 129.6.15.29      2 u  224  512  377   58.305   -0.558   0.9
+juniperberry.ca 131.188.3.220    2 u   47  512  377  139.882   -3.180   0.8
ntpq>
```

Simple Mail Transfer Protocol

- What Is SMTP?
- What could you discover?
- DEMO: Enumerating SMTP with NetScanTools Pro
- DEMO: Enumerating SMTP with SMTP_User_Enum

What Is SMTP?

What Is SMTP?



- The protocol used for email
- Uses “MX” records via DNS
- Uses “MTA” for routing
- Some proprietary systems use other protocols internally

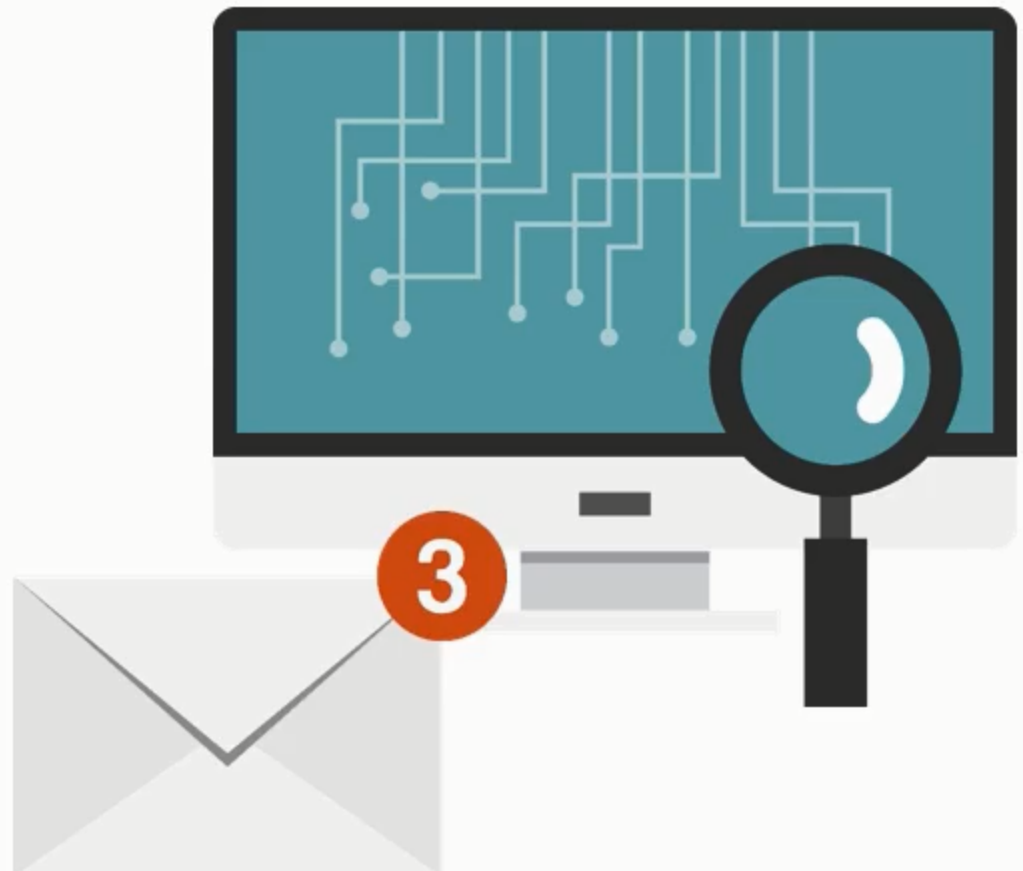
Behind SMTP

Ports

- 25
- 587 (submission)

Commands

- MAIL FROM
- RCPT TO
- DATA
- VRFY
- EXPN



What Can We Learn from SMTP?

- Download a name list
- Valid users

DEMO: Enumeration via SMTP

Using NetScanTools Pro and smtp_user_enum we'll:

- Download a name list
- Enumerate usernames

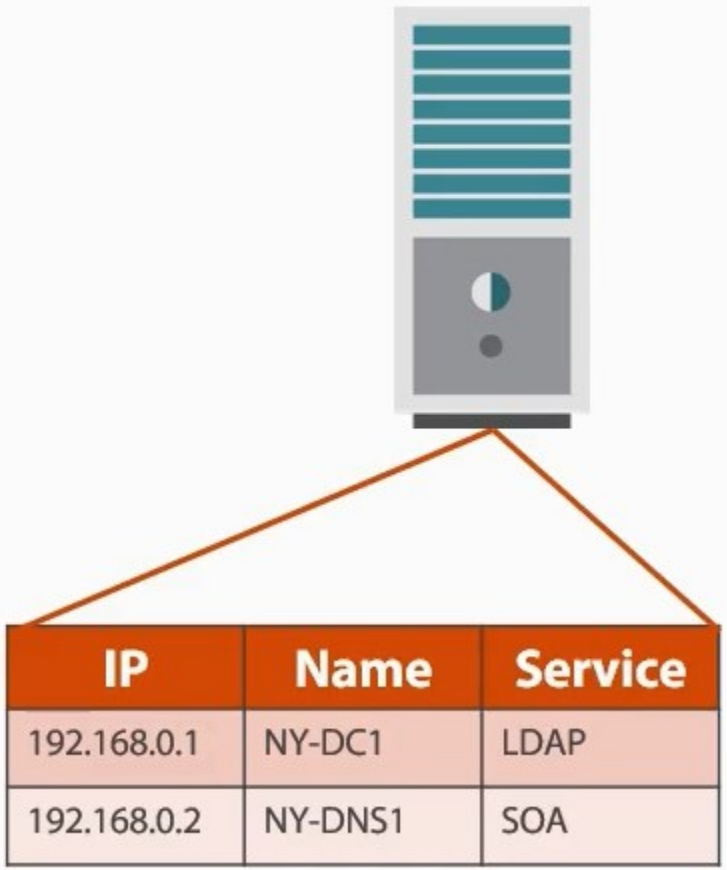
```
root@kali:~# nslookup smtp.gmail.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
smtp.gmail.com  canonical name = gmail-smtp-msa.l.google.com.
Name:   gmail-smtp-msa.l.google.com
Address: 64.233.190.108
Name:   gmail-smtp-msa.l.google.com
Address: 2800:3f0:4003:c01::6d

root@kali:~# sm
smali           smbclient       smbget          smbstatus
smartctl        smbcontrol      smbmap          smbtar
smartd          smbcquotas      smbpasswd       smbtree
smbcacls        smbd            smbspool        smtp-user-enum
root@kali:~# smtp-user-enum -M -VRFY -u baragammo@gmail.com -t 64.233.190.108:587
ERROR: Invalid mode specified with -M.  Should be VRFY, EXPN or RCPT.  -h for help
root@kali:~# smtp-user-enum -M VRFY -u baragammo@gmail.com -t 64.233.190.108:587Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Thu Jun 13 13:06:24 2019 #########
64.233.190.108:587: baragammo@gmail.com exists
######## Scan completed at Thu Jun 13 13:06:26 2019 #########
1 results.

1 queries in 2 seconds (0.5 queries / sec)
```

Domain Naming Service

- What Is DNS?
- Types of DNS enumeration
- DEMO: Enumerating DNS with NSLookup
- DEMO: Enumerating DNS with DNSRecon

What Is DNS?

A Name Is a Name, Is a Name



IP	Name	Service
192.168.0.1	NY-DC1	LDAP
192.168.0.2	NY-DNS1	SOA

- Record lookup
- Cache snooping
- Google lookup
- Reverse lookup
- Zone walking
- Zone transfers

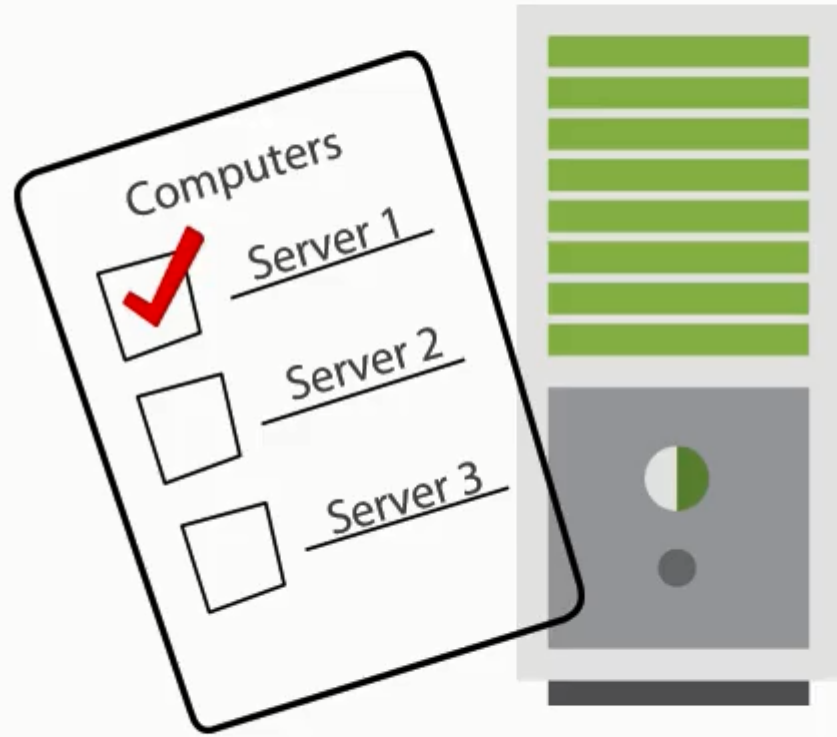
Behind DNS

Ports

- UDP 53
- TCP 53*

Records

- A
- AAAA
- CName
- MX
- NS
- SOA
- PTR
- SRV



What Can We Learn from DNS

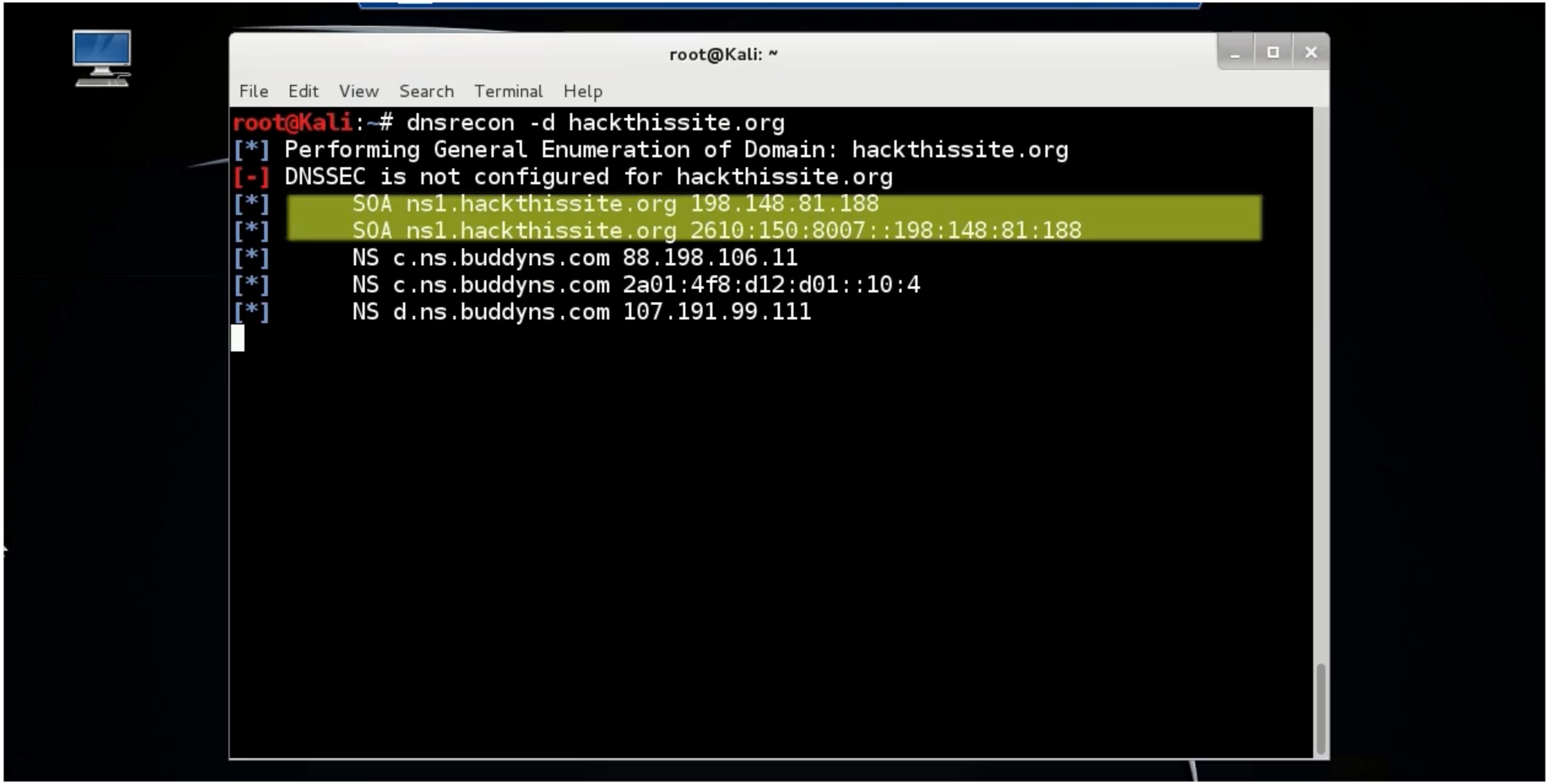
- The “Mother-load”
- Servers
- Workstations
- Services => servers

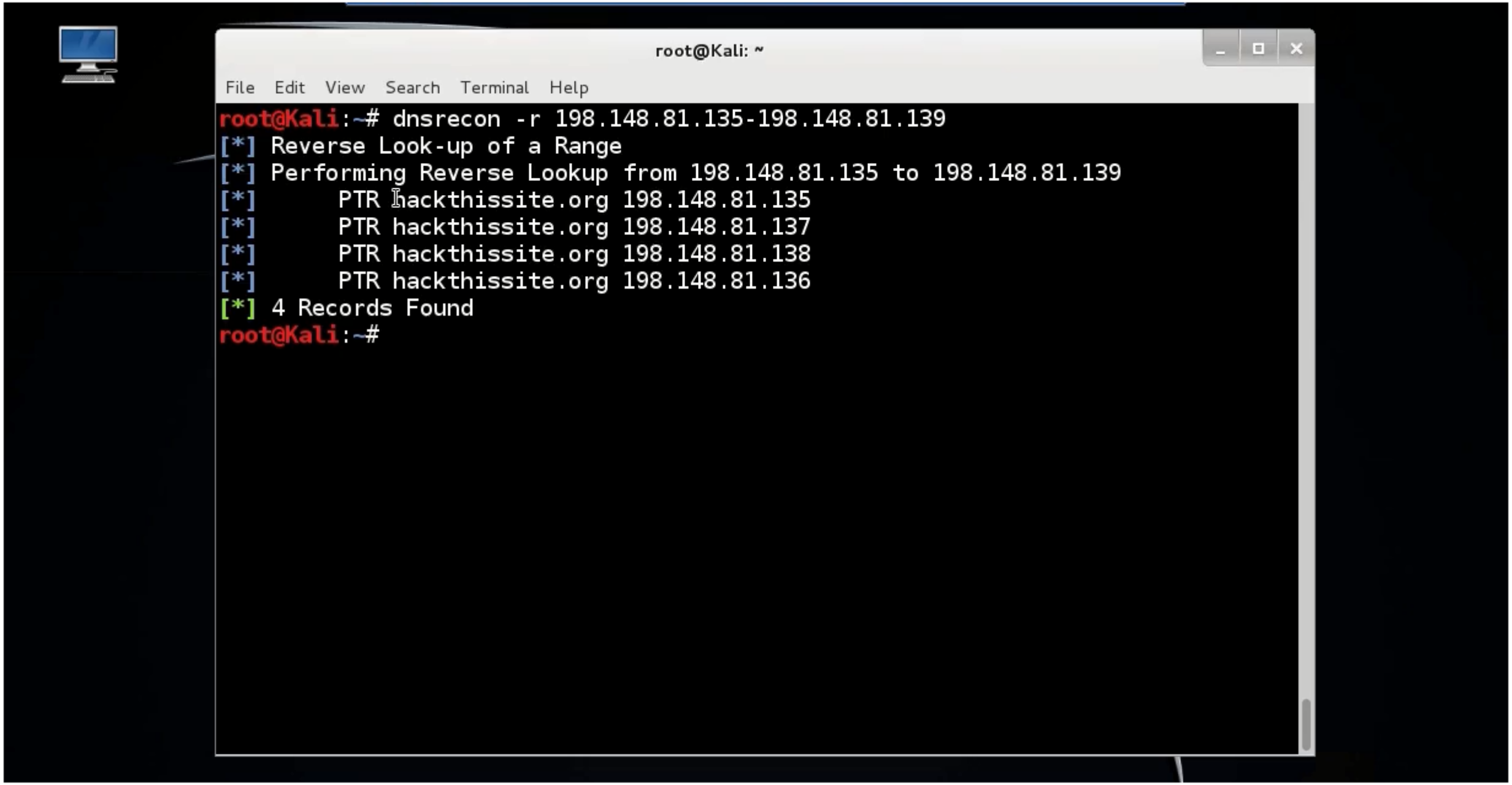
DEMO: Enumeration via DNS

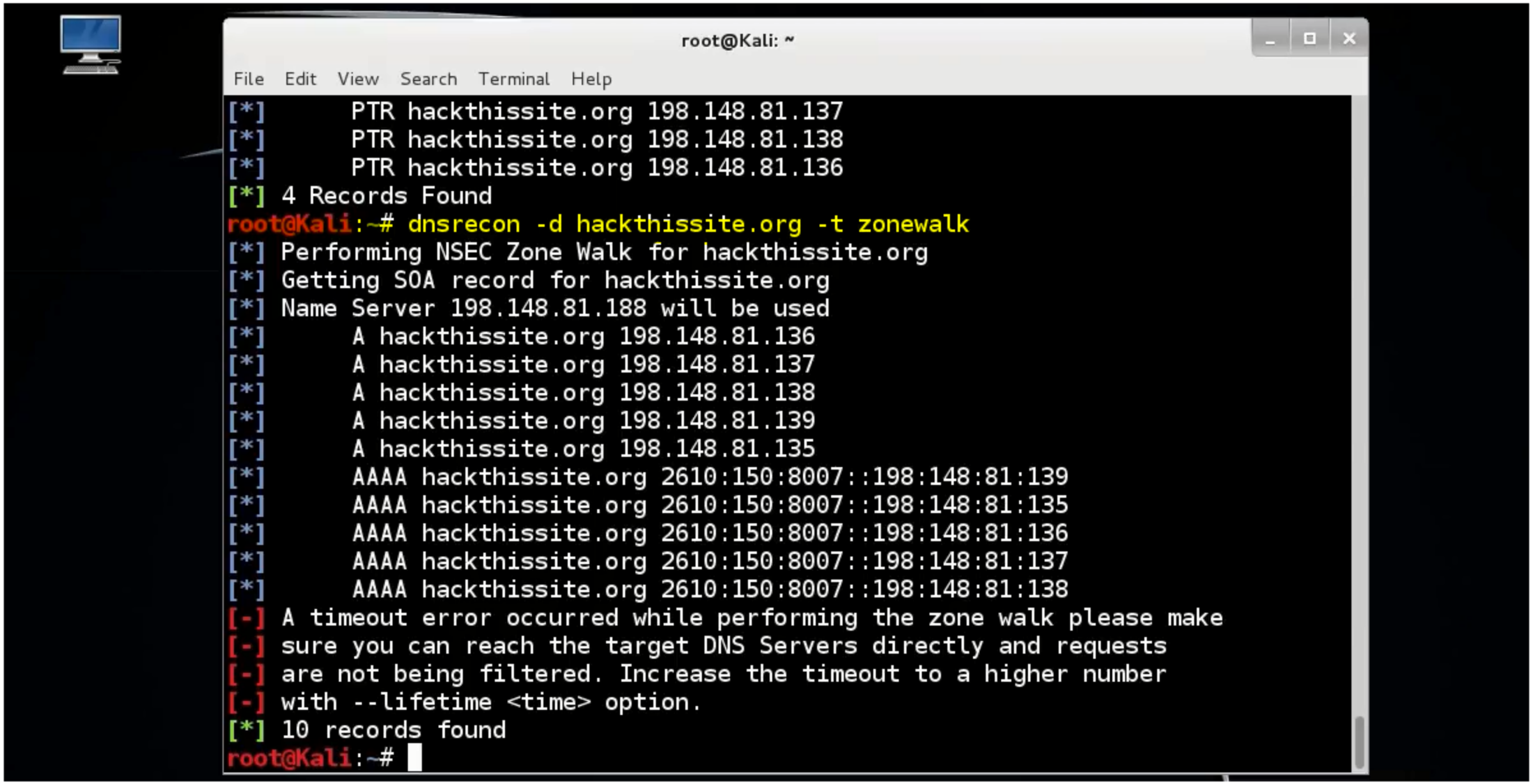
Using NSLookup and DNSRecon we'll:

- Discover records
- Zone transfer
- Reverse lookup
- Domain brute-force
- Zone-walk
- Cache snooping

```
root@kali:~# nslookup
> hackthissite.org
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   hackthissite.org
Address: 137.74.187.103
Name:   hackthissite.org
Address: 137.74.187.102
Name:   hackthissite.org
Address: 137.74.187.101
Name:   hackthissite.org
Address: 137.74.187.104
Name:   hackthissite.org
Address: 137.74.187.100
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:100
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:103
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:102
Name:   hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:101
Name:   hackthissite.org
```


root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# dnsrecon -d hackthissite.org
[*] Performing General Enumeration of Domain: hackthissite.org
[-] DNSSEC is not configured for hackthissite.org
[*] SOA ns1.hackthissite.org 198.148.81.188
[*] SOA ns1.hackthissite.org 2610:150:8007::198:148:81:188
[*] NS c.ns.buddyns.com 88.198.106.11
[*] NS c.ns.buddyns.com 2a01:4f8:d12:d01::10:4
[*] NS d.ns.buddyns.com 107.191.99.111


root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# dnsrecon -r 198.148.81.135-198.148.81.139
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 198.148.81.135 to 198.148.81.139
[*] PTR hackthissite.org 198.148.81.135
[*] PTR hackthissite.org 198.148.81.137
[*] PTR hackthissite.org 198.148.81.138
[*] PTR hackthissite.org 198.148.81.136
[*] 4 Records Found
root@Kali:~#


root@Kali: ~
File Edit View Search Terminal Help
[*] PTR hackthissite.org 198.148.81.137
[*] PTR hackthissite.org 198.148.81.138
[*] PTR hackthissite.org 198.148.81.136
[*] 4 Records Found
root@Kali:~# dnsrecon -d hackthissite.org -t zonewalk
[*] Performing NSEC Zone Walk for hackthissite.org
[*] Getting SOA record for hackthissite.org
[*] Name Server 198.148.81.188 will be used
[*] A hackthissite.org 198.148.81.136
[*] A hackthissite.org 198.148.81.137
[*] A hackthissite.org 198.148.81.138
[*] A hackthissite.org 198.148.81.139
[*] A hackthissite.org 198.148.81.135
[*] AAAA hackthissite.org 2610:150:8007::198:148:81:139
[*] AAAA hackthissite.org 2610:150:8007::198:148:81:135
[*] AAAA hackthissite.org 2610:150:8007::198:148:81:136
[*] AAAA hackthissite.org 2610:150:8007::198:148:81:137
[*] AAAA hackthissite.org 2610:150:8007::198:148:81:138
[-] A timeout error occurred while performing the zone walk please make
[-] sure you can reach the target DNS Servers directly and requests
[-] are not being filtered. Increase the timeout to a higher number
[-] with --lifetime <time> option.
[*] 10 records found
root@Kali:~#

Find Subdomains :: Online Penetration Testing Tools | Ethical Hacking Tools – Iceweasel

Find Subdomains :: Onlin...

https://pentest-tools.com/information-gathering/find-subdomains-of-domain

Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Information Gathering
- Google Hacking
- Find Subdomains
- Find VHosts
- ICMP Ping
- Whois Lookup

Web Application Testing

Infrastructure Testing

Scan Result » Find Subdomains

Params: hackthissite.org

Raw output Save as pdf

Searching for subdomains - method 1 of 3 ...
Found 0 subdomains (total 0 unique)

Searching for subdomains - method 2 of 3 ...
Found 40 subdomains (total 40 unique)

Searching for subdomains - method 3 of 3 ...
Found 1 subdomains (total 40 unique)

Total 40 unique subdomains found:

Resolving names ...

You should also try
- Google Hacking
- Find VHosts
- Web Server Scan