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!

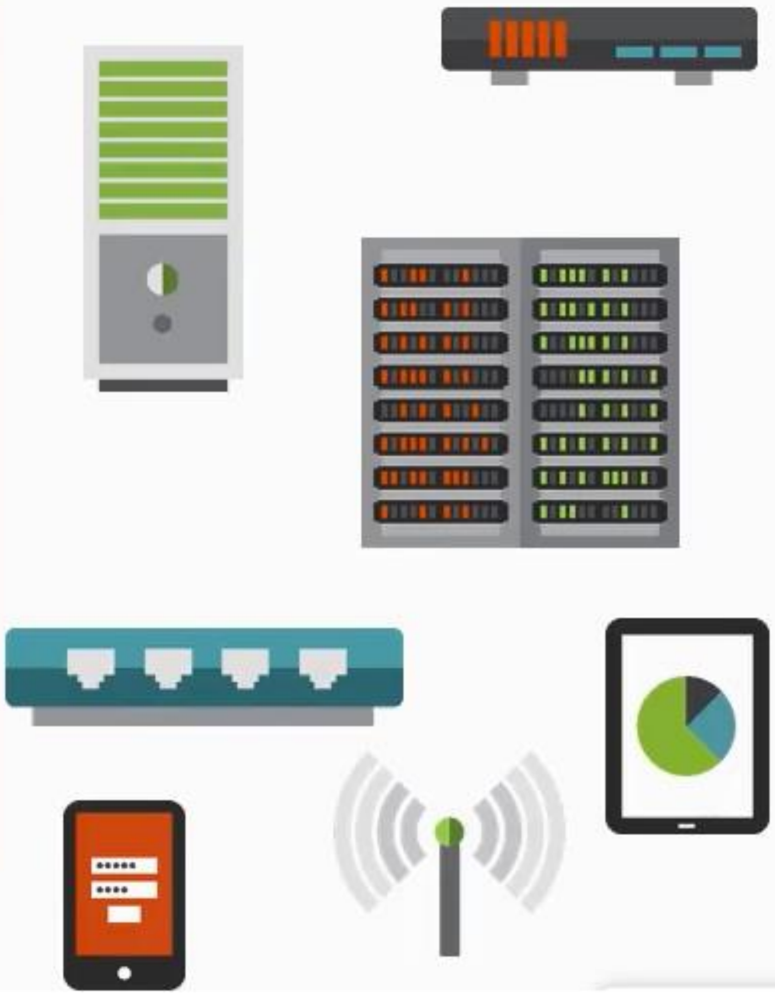
DNS zone transfers	TCP 53
SMTP	TCP 25
MS RPC Endpoint	TCP 135
Global Catalog Service	TCP/UDP 3368
NetBIOS Naming Service	TCP 137
LDAP	TCP/UDP 389
SMB over NetBIOS	TCP 139
SNMP	UDP 161
SMB over TCP	TCP 445

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

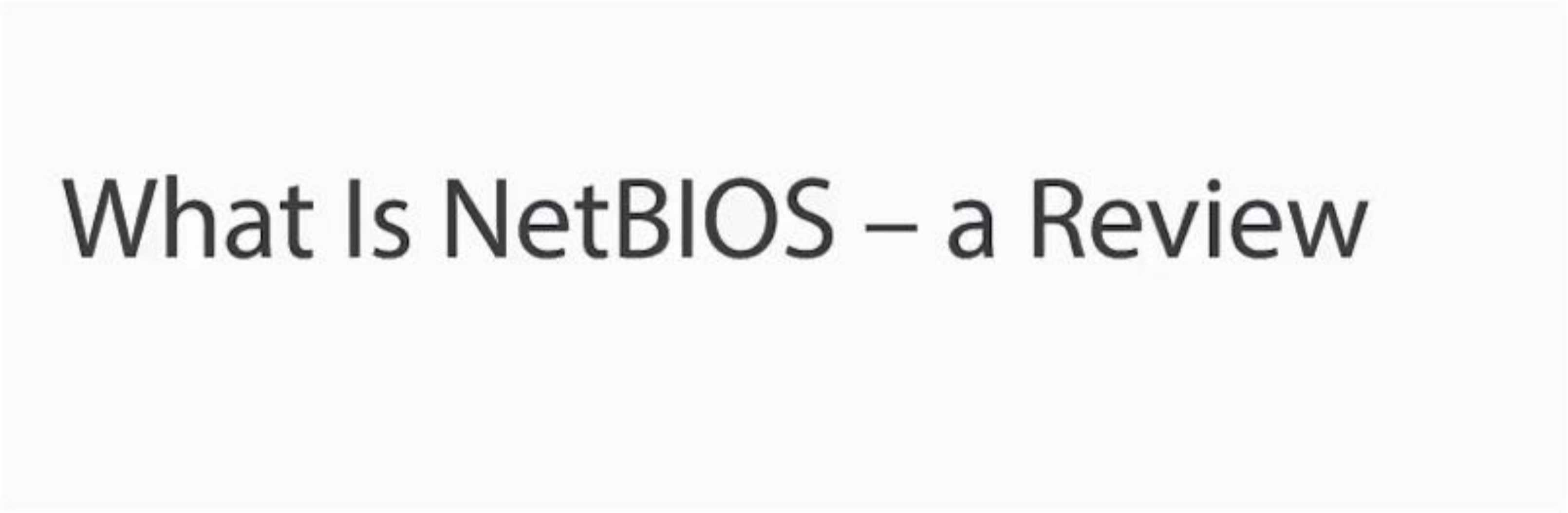
Complacency Will Be Your Downfall

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



The "Art of Misdirection"

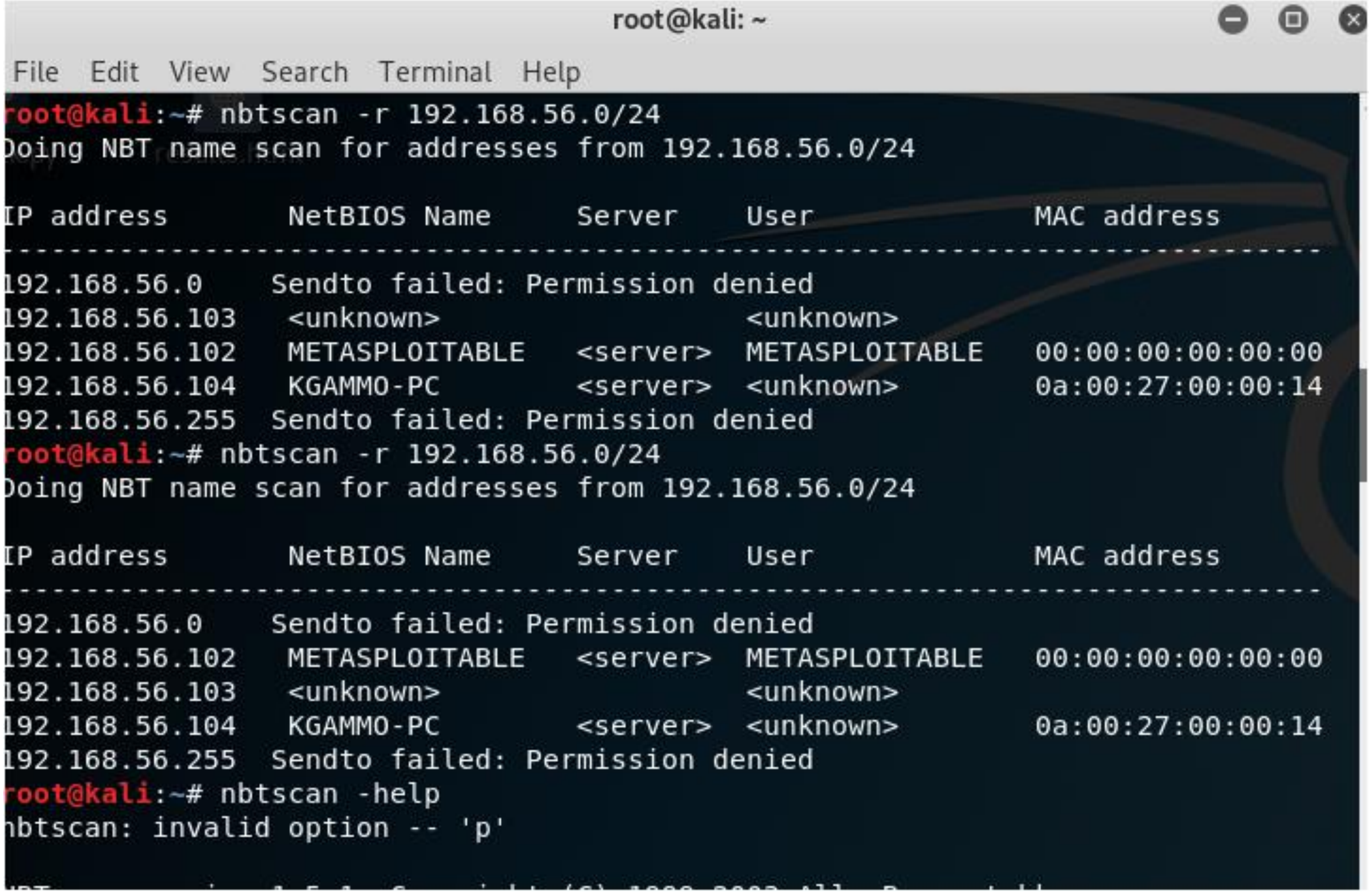
- What's the default SSID for a Linksys wireless router?
- What would someone "assume" if I used the username of "root"?
- What if I named my Samsung Tablet "iPad"?



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

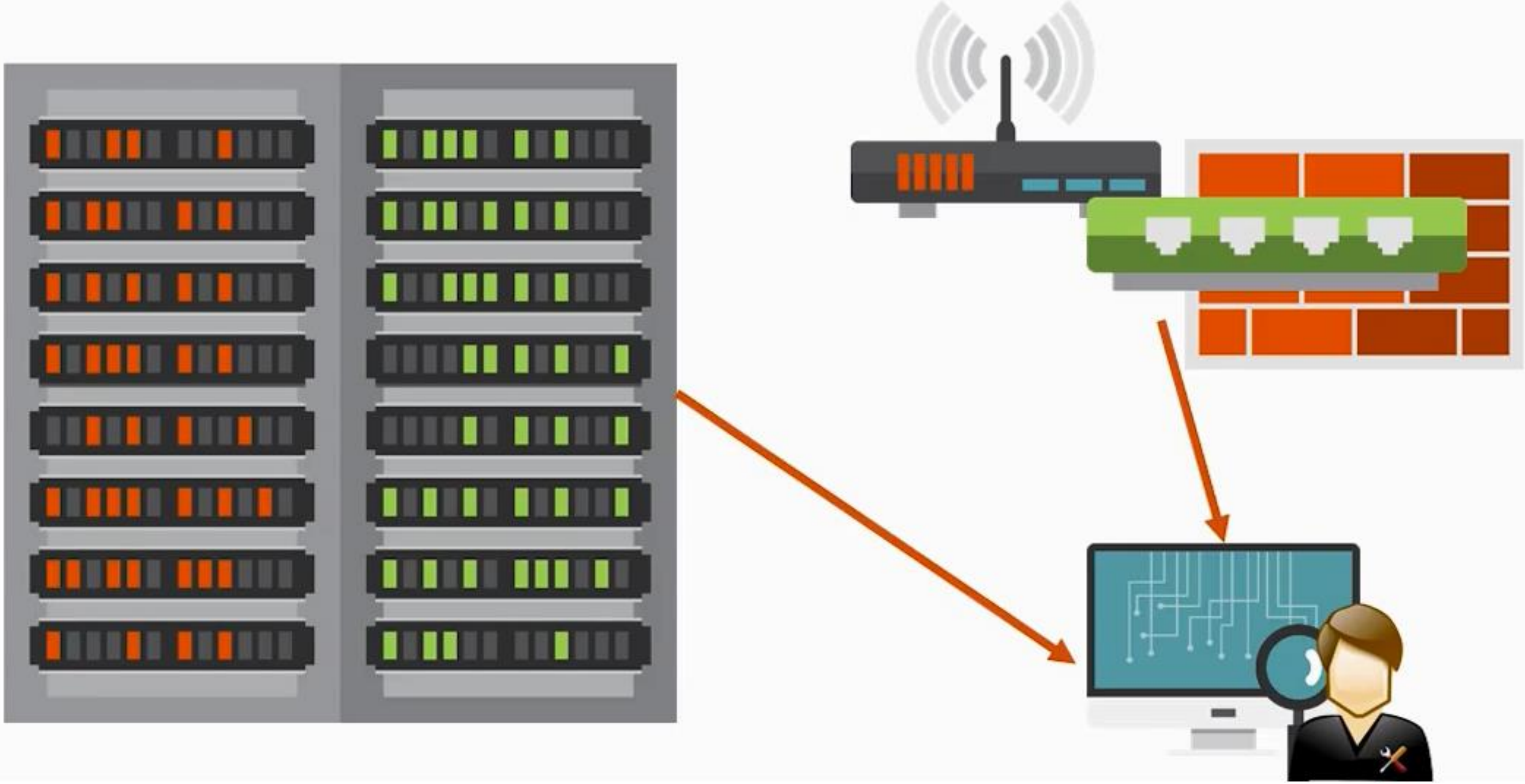


```
root@kali:~# nbtscan -r 192.168.56.0/24
Doing NBT name scan for addresses from 192.168.56.0/24

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!

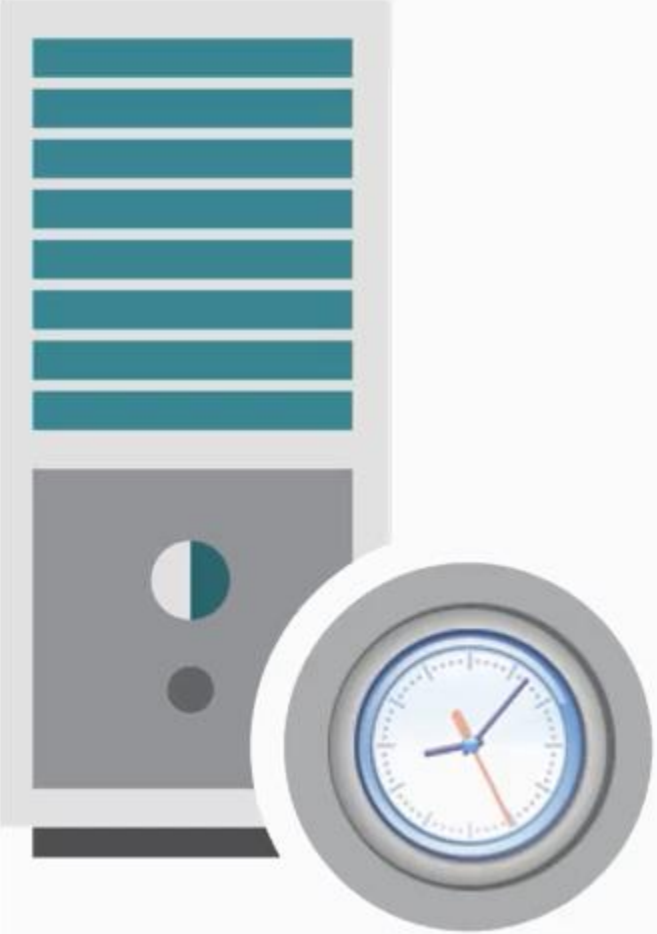
❑ What Is NTP?

❑ 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

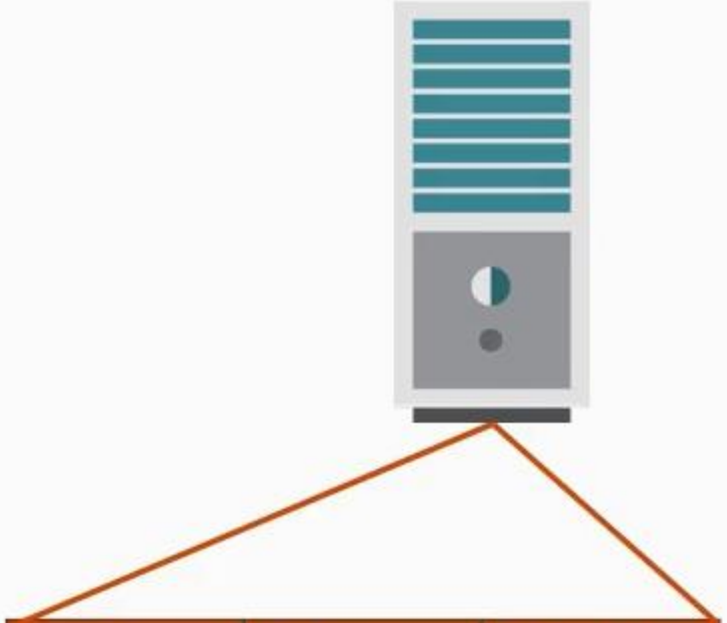
- ❑ Private Networks / 200µs
- ❑ Public Networks / 10ms

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

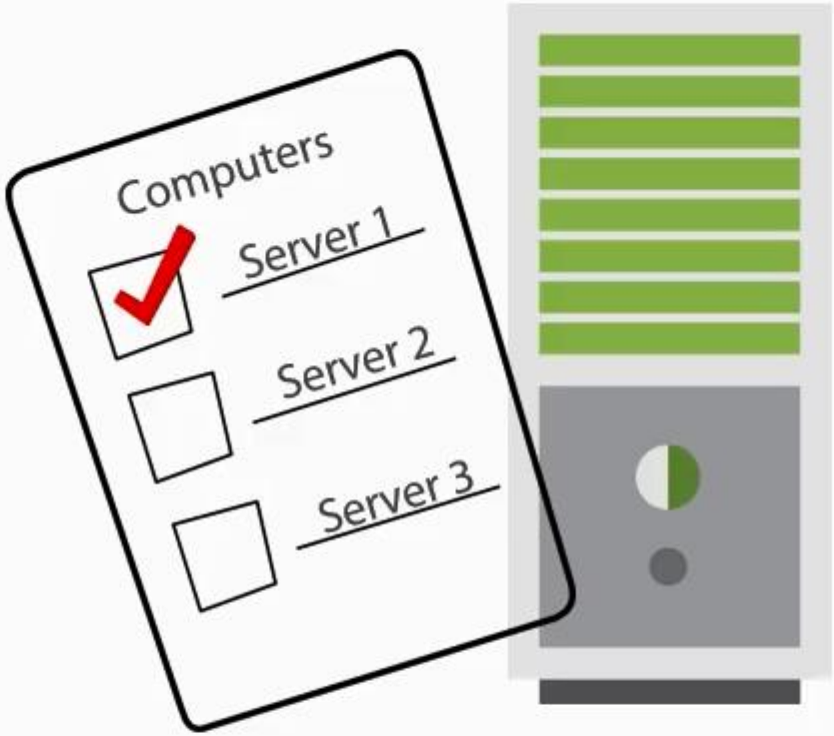
Behind DNS

Ports

- ❑ UDP 53
- ❑ TCP 53*

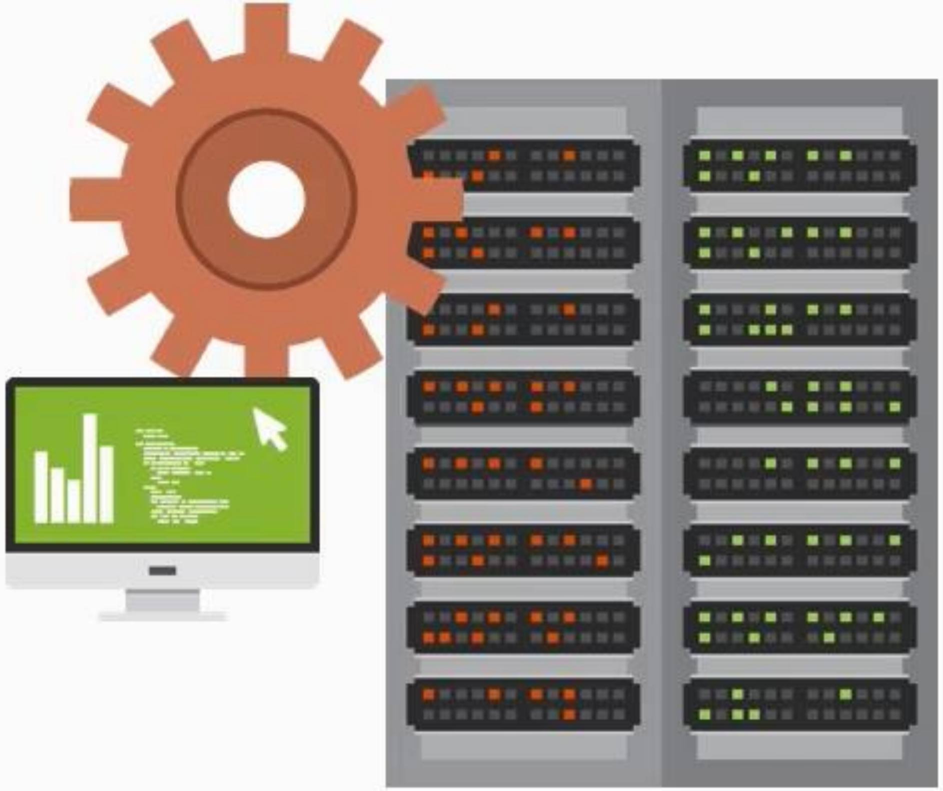
Records

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



What Can We Learn from DNS

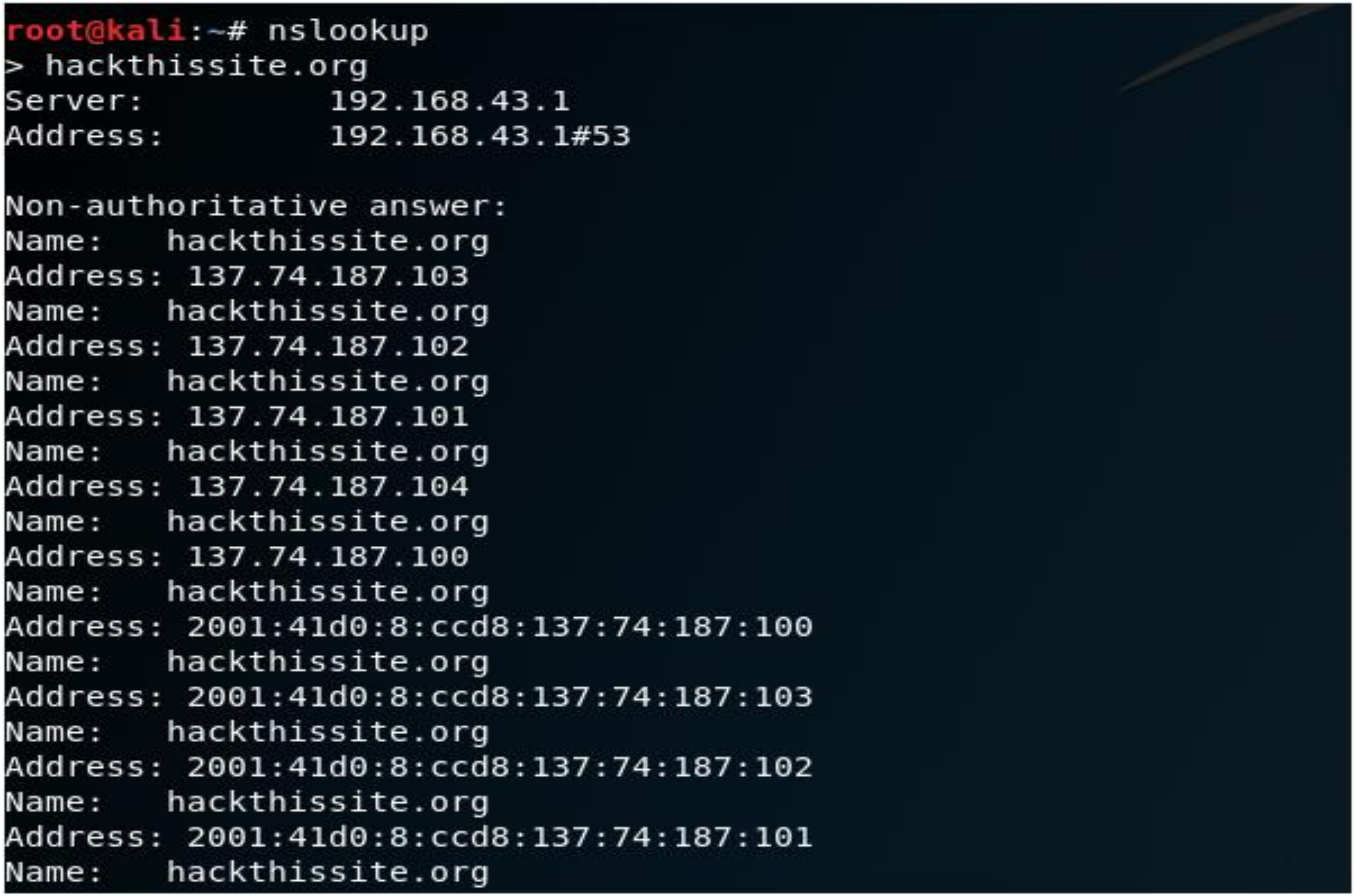
- The “Mother-load”
- Servers
- Workstations
- Services => servers



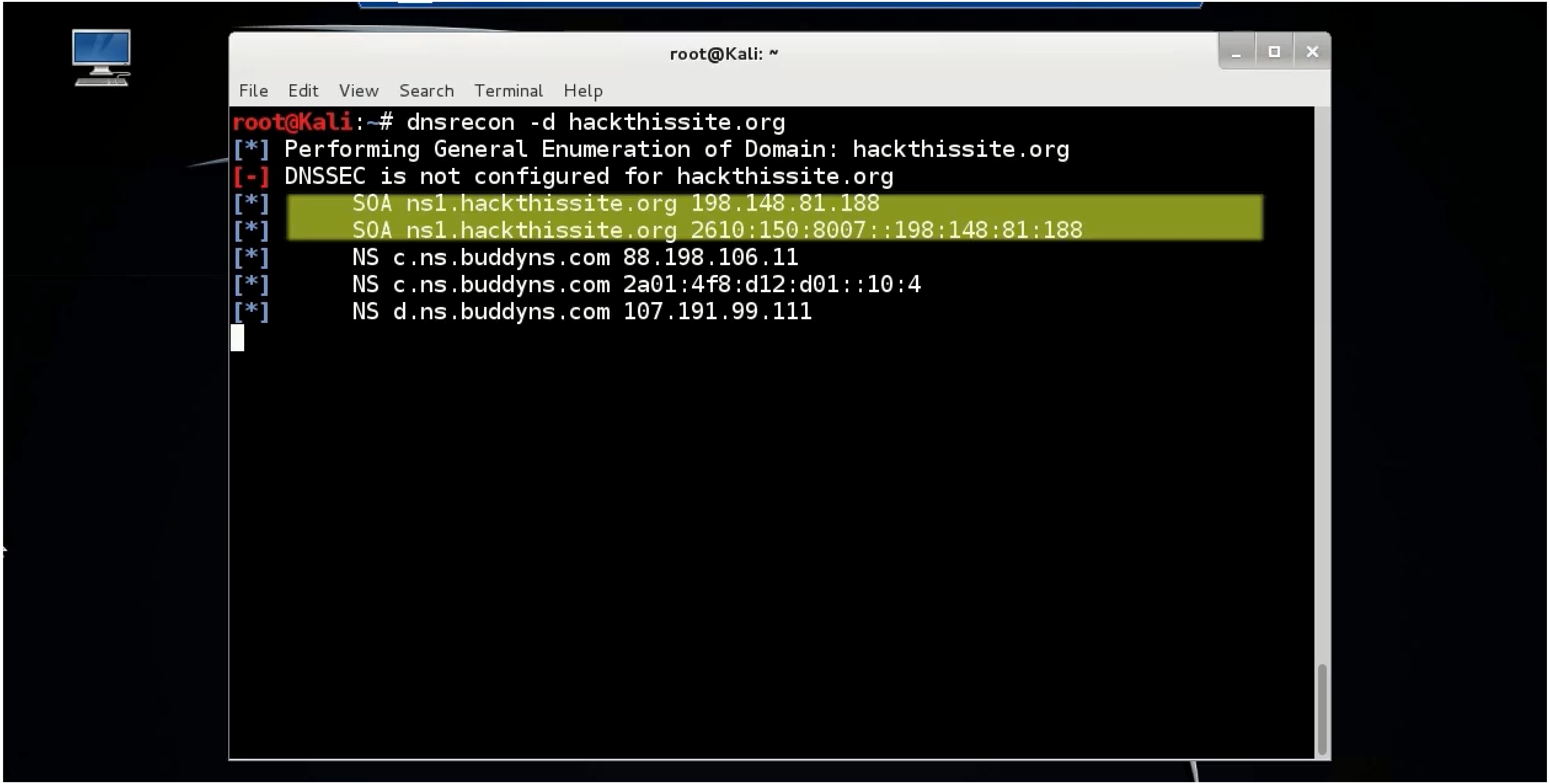
DEMO: Enumeration via DNS

Using NSLookup and DNSRecon we'll:

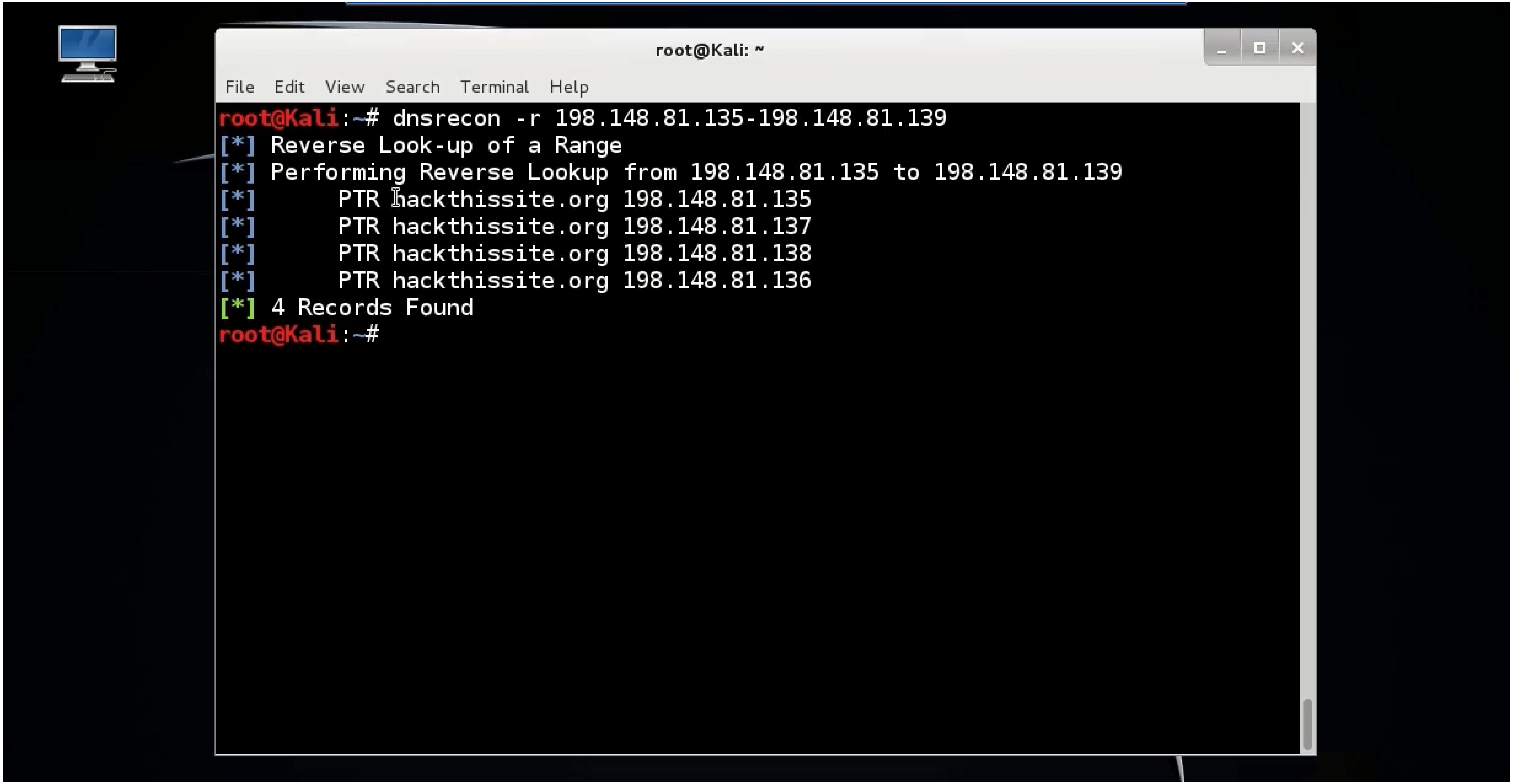
- □ Discover records
- □ Zone transfer
- □ Reverse lookup
- □ Domain brute-force
- □ Zone-walk
- □ Cache snooping



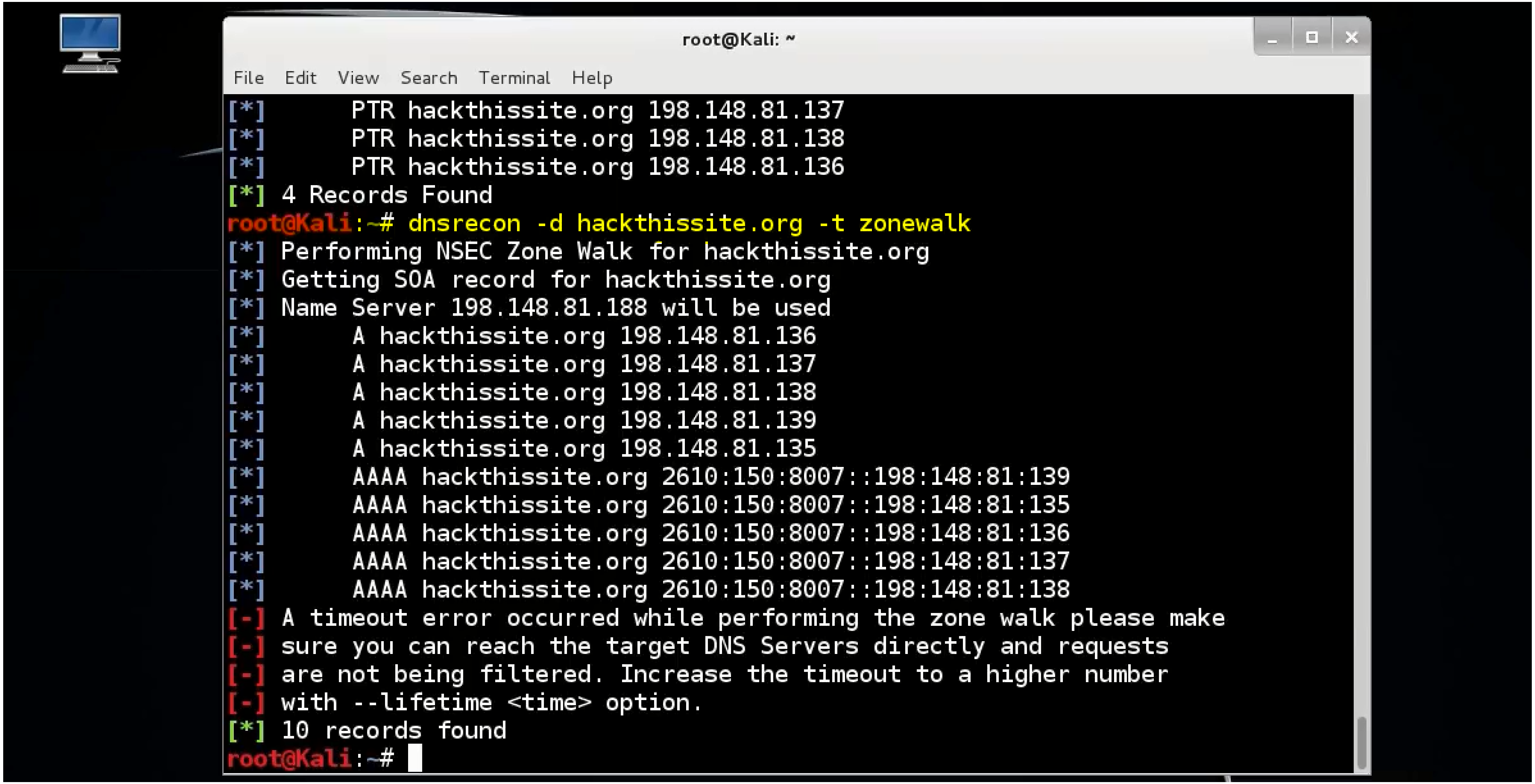
```
root@kali:~# nslookup
> hackthissite.org
Server:         192.168.43.1
Address:        192.168.43.1#53

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:~# 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:~# 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:~#
```



```
[*]      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:~# 
```