

# Penetration Testing

White Hat Advisory

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# PEN TEST OVERVIEW

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# What We Will Look At

## Pen Test 101

What is it?

What it is not

Types of Pen Tests

### Procedure

Reconnaissance

Enumeration

Vulnerability Analysis

Exploitation

Reporting and Evaluation

### Testing Types

#### 15 Minute Pen Test

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



## What is it?

- The use of exploitive techniques to evaluate risk associated with system vulnerabilities.
- A simulated attack on a system or network at the request of the owner to evaluate the risk characteristics of an environment.

## What it is not!

- Malicious
- Hacking / Cracking
- Unauthorised



# Pen Testing

## FOCUS

Internet Systems and Services

Remote-access Solutions and Applications

## KEY

The key to a successful pen test is:

- 1) Clearly defined objectives, scope and goals.
- 2) Agreed upon limits and acceptable activities.

## TYPES

Zero Knowledge

Partial Knowledge

Full Knowledge



# PROCEDURE

- Reconnaissance
- Enumeration
- Vulnerability Analysis
- Exploitation
- Test Evaluation and Report

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# PROCEDURE > Reconnaissance

- Collecting freely available information to assist in the test
- Can include :
  - Theft
    - Lying to people
    - Tapping phones and networks
    - Compay's Website
    - Recruitment Advertisements
    - WHOIS Registration
    - DNS Lookups



# PROCEUDRE > Enumeration

- Obtaining information directly from the target's systems, applications and networks.
- Building a picture of a company's environment.
- e.g.: **Port Scanning** ; **Ping Sweeps** ; etc..
- Used in combination with data collected from the reconnaissance phase.

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# PROCEDURE > Vulnerability Analysis

- Compare the information collected with known vulnerabilities.
- Will form the basis for exploitation.
- Tools : Nessus ; Metasploit ; etc..



# PROCEDURE > Exploitation

- Running exploits discovered in the vulnerability phase.
- Can use tools to automatically run sets of exploits.
- Record vulnerabilities and method of exploit for reporting phase.



# PROCEDURE > Evaluation and Report

- Did the test results conflict with expectations ?
- Is the system reacting in a predictable way ?
- Document tactics, tools, methods of findings to assist in BC, DRP, as well as in implementing IDS and IPS.



# Testing Strategies

## **EXTERNAL**

Attacks on the network perimeter.

## **INTERNAL**

Attacks from within the perimeter.

Attempts to understand what could happen if the perimeter was penetrated.

## **BLIND**

Testing team has limited or no prior information of network.

## **DOUBLE-BLIND**

Testing done with no warning given to the IT staff.

## **TARGETED TESTING**

Both the testing team and the IT staff are given full information during the test.



# 15 Minute Pen Test

## Step 1 - Ping sweep for node discovery

```
$ nmap -sP 192.168.0.2-254
```

## Step 2 – High-invasive information of system

```
* nmap -A 192.168.0.x
```

## Step 3 – Vulnerability Analysis with Nessus

- default scan of 192.168.0.x with 'safety checks' selected
- export scan results as a NBE file



# 15 Minute Pen Test

## Step 4 – Exploitation with Metasploit

```
$ msfconsole  
> load db_sqlite3  
> db_create /tmp/temp1  
> db_import nessus_nbe <nbe_file>  
> db_autopwn -x -t (will list the modules to execute the exploit)  
> use <module>  
> show options  
> set payload windows/meterpreter/bind_tcp  
> show options  
> exploit
```

\* If the exploit was successful, the meterpreter prompt will now be displayed.  
meterpreter> help (displays options available)  
meterpreter> getuid (shows which system user you are currently pwning)



# 15 Minute Pen Test

## Step 6 - PWN3D!

If the exploit was successful, the meterpreter prompt will now be displayed.

```
meterpreter> help (displays options available)
```

```
meterpreter> getuid (shows which system user you are currently pwning)
```

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# RECONNAISSANCE

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# Overview

- Purpose of Reconnaissance
- Information to Attain
- Methods of Reconnaissance
  - Active
  - Passive



## Purpose of Reconnaissance

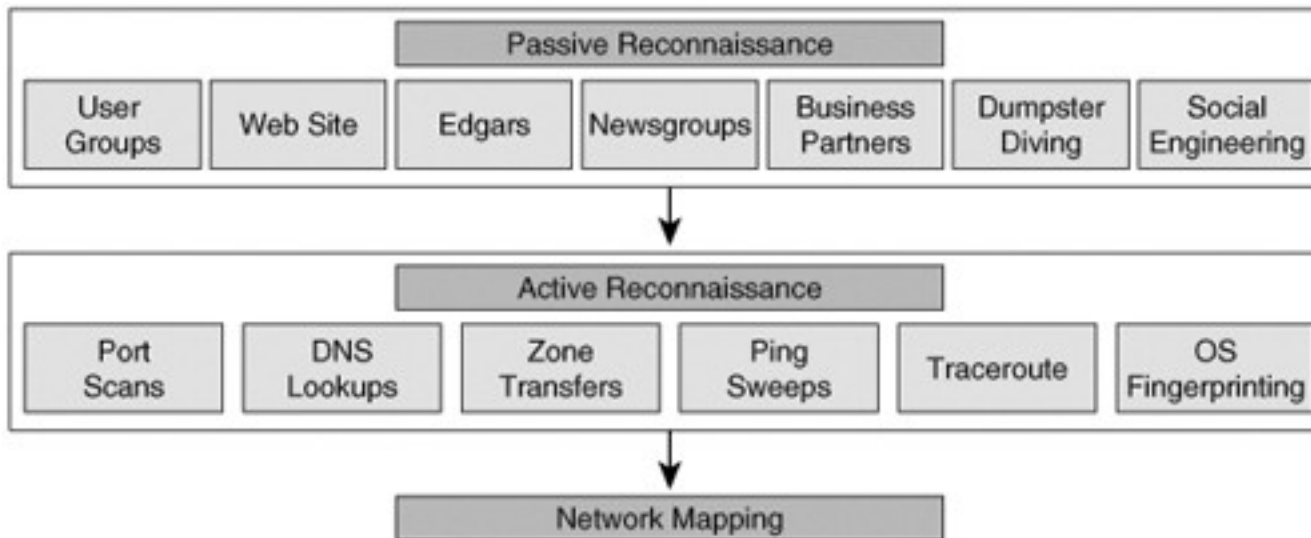
The information gained during reconnaissance will assist in building a high-level understanding of the company.

How will this help us?

- Business Functions?
- How big is this company?
- What type of servers can we expect to find?
- What type of services can we expect to find?
- How extensive can we expect the network to be?
- What type of data can we expect to find?



# The Reconnaissance Process



I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



## Information to Attain

- Locations
- Related companies and entities
- Phone numbers
- Contact names and email addresses
- Privacy or security policies
- IP Ranges
- Operating Systems
- Software in Use
- Employee Names
- Organisational Structures
- Business Partners

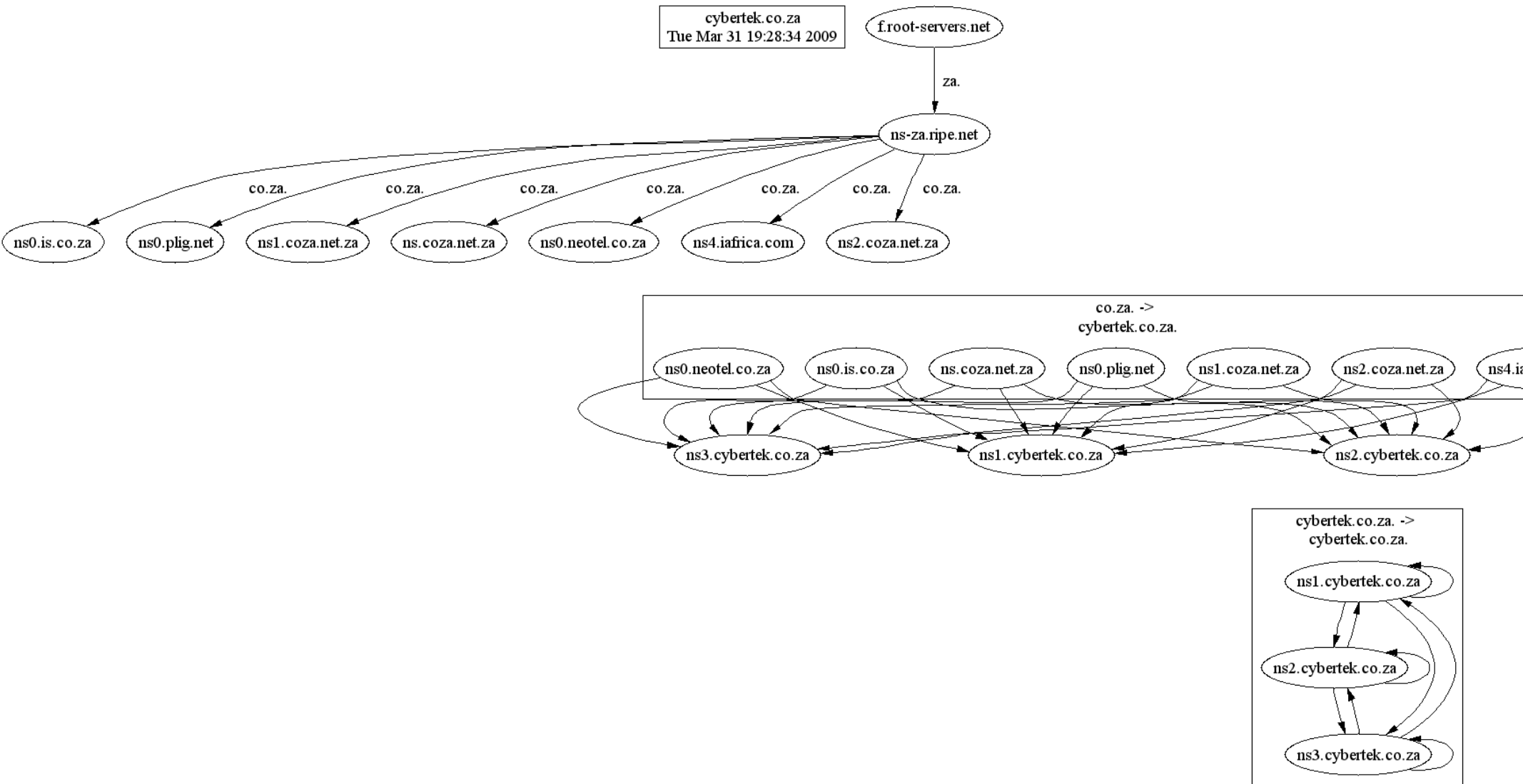


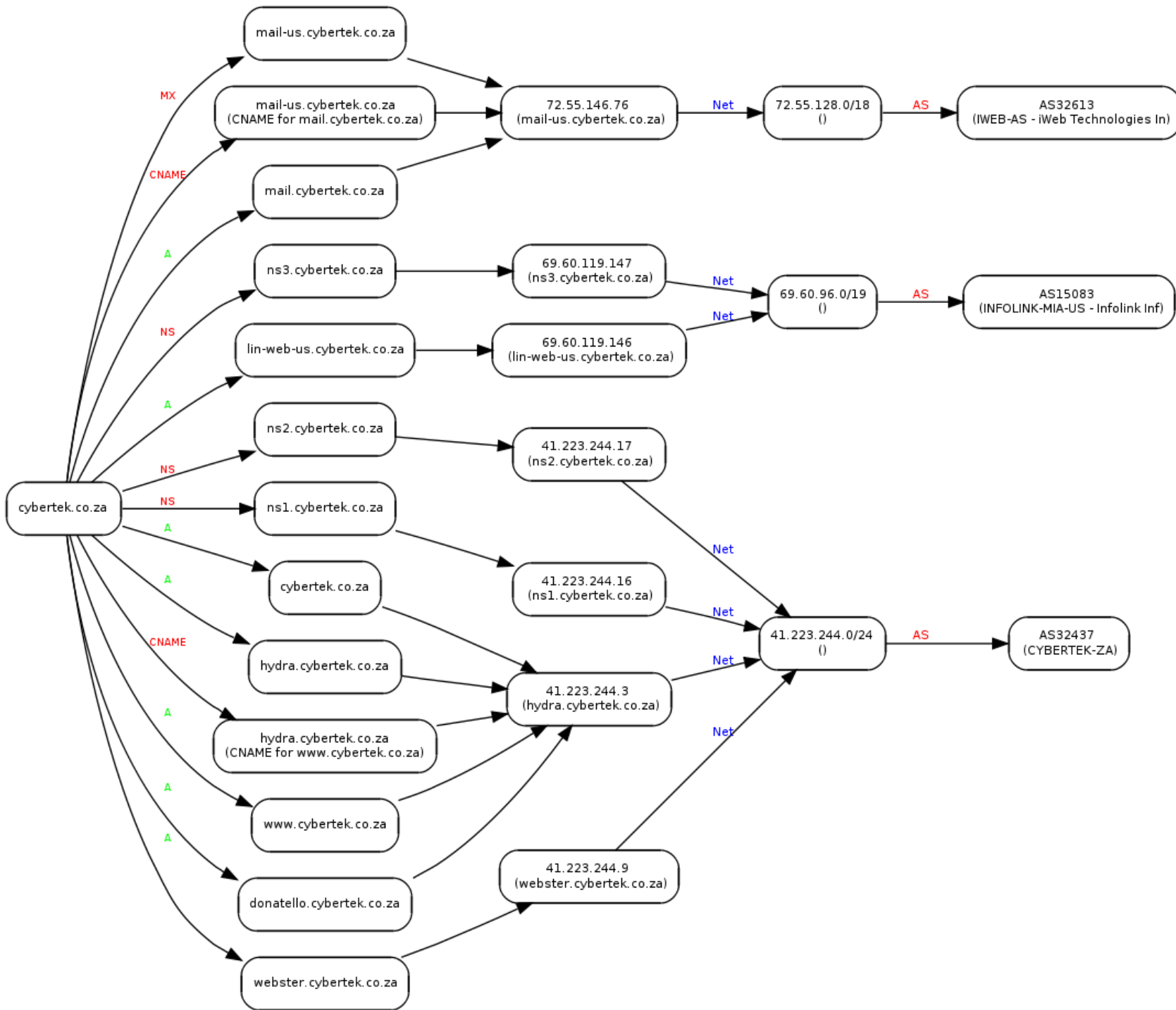
## PASSIVE Reconnaissance

- Company's website
- Whois Listing
- Host Names
- Website Hosting Historical Data  
<http://uptime.netcraft.com/up/graph>
- Subsidiary Websites / Products / Services
- Network Query Tools  
<http://www.windowspms.com>  
<http://www.serversniff.net>
- DNS Record Visualization  
<http://www.serversniff.net/domainreport.php>



# DNS Visualisation with serversniff.net





I n v e n i a m v i a m a u t f a c i a m



## **ACTIVE Reconnaissance**

- Fraudulent Support Phone Calls
- Theft
- Exploiting Friendships

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# ENUMERATION

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m



# Enumeration Overview

- Purpose and Goal of Enumeration
- Find Network Range
- Calculate Subnet Mask
- Enumerate Nodes on Network
- Port Scan and Service Enumeration



## Purpose and Goal

Before an attack can take place, we need to know what vulnerabilities we are going to exploit. One of the first steps to finding vulnerabilities is enumerating or listing services (software) on the company's hosts.

The purpose is thus to list :

- Hosts
- Services and Software per Host



## Finding The Network Range

The range of IP's assigned to a particular company is important, as we can use that as a starting point for enumerating important servers.

The best place to get this information is from WhoIs

### **Tools for IP range discovery:**

[www.sampade.org](http://www.sampade.org) (Excellent WhoIs Lookup)

[www.zonecut.net/dns](http://www.zonecut.net/dns) (Graphical DNS Zones)



## Calculate the Subnet Mask

The subnet mask for the IP range is needed as an input to many of the ping sweep and port scanning tools.

For those who don't think in binary, there are some **online tools for subnet mask calculation** :

[www.subnetonline.com/pages/subnet-calculators/subnetmask-calculator.php](http://www.subnetonline.com/pages/subnet-calculators/subnetmask-calculator.php)

<http://krow.net/dict/subnet.html>



## Enumerating Nodes

To work out what services we can exploit, we first need to work out what servers are connected to the internet. This is called **Host Discovery**. To do this, we can use a CLI tool called **nmap**.

### STEP 1 : Discovery Phase

**nmap -sP <network-range>**

The -sP tells nmap to perform a low-intensive ping sweep, and only worry about host discovery, and nothing else.

e.g.: **nmap -sP 41.223.244.0/22**



## Enumerating Nodes

Now that we have a list of hosts, we want to see from the IP addresses or host names which portion of the IP range is being used for important servers.

Once that is established, we want to see what ports are open on these nodes:

### STEP 2 : Port Scan

**nmap -sS <network-range>**

e.g. : nmap -sS 41.223.244.0/24



## Enumerating Services

We now have a list of ports open on the primary servers. From this, we can decide which hosts we would like to focus on, and run an intensive scan to do OS fingerprinting and detailed Service enumeration.

### STEP 3 : Service Enumeration

**nmap -A <host-ip-address>**

e.g.: nmap -A 41.223.244.3



## Enumeration

At the end of the enumeration stage we should have a short list of candidate hosts to exploit with an OS fingerprint done and service listings for each host.

From this, vulnerability analysis is done to narrow down the potential candidates to perform the exploitation on.



**Thank you for your attention**

I  
n  
v  
e  
n  
i  
a  
m  
v  
i  
a  
m  
a  
u  
t  
f  
a  
c  
i  
a  
m

