Advanced Network Security
Art of Penetrating Deep Inside

Sanoop Thomas
Head Security Trainer and Researcher
Institute of Information Security
Network Intelligence India Pvt. Ltd
iisecurity.in | niiconsulting.com
sanoop.thomas@iisecurity.in

OWASP
31st Aug 2013

The OWASP Foundation
http://www.owasp.org

Speakers Profile

Sanoop Thomas

- Head Security Trainer & Researcher
- Was a java developer, I still build codes

- Advisories & Papers Published

  http://www.exploit-db.com/author/?a=5893

  http://packetstormsecurity.com/files/author/10600/

  http://niiconsulting.com/checkmate/author/sanoop/

Agenda

- Penetration Testing Methodology
- Pre-Engagement Plans
- Advanced Network Mapping
- Network Scanning in Real World
- Exploiting the Enterprise
- Pentest Report

What is penetration testing ?

This term is often confused with Security Audit or Assessments

It's a systematic probing of applications, hosts, networks and other technologies, and see how deeper we can go inside

A WarGame between RED team and BLUE team

Testing Methodologies

- Client →

  "Please provide quote for black-box penetration test"

- ISSP →

  "Please provide list of IP addresses and URLs, test account credentials etc."

Testing Methodologies Evolved

- Client →

  "Please provide quote for black-box penetration test"

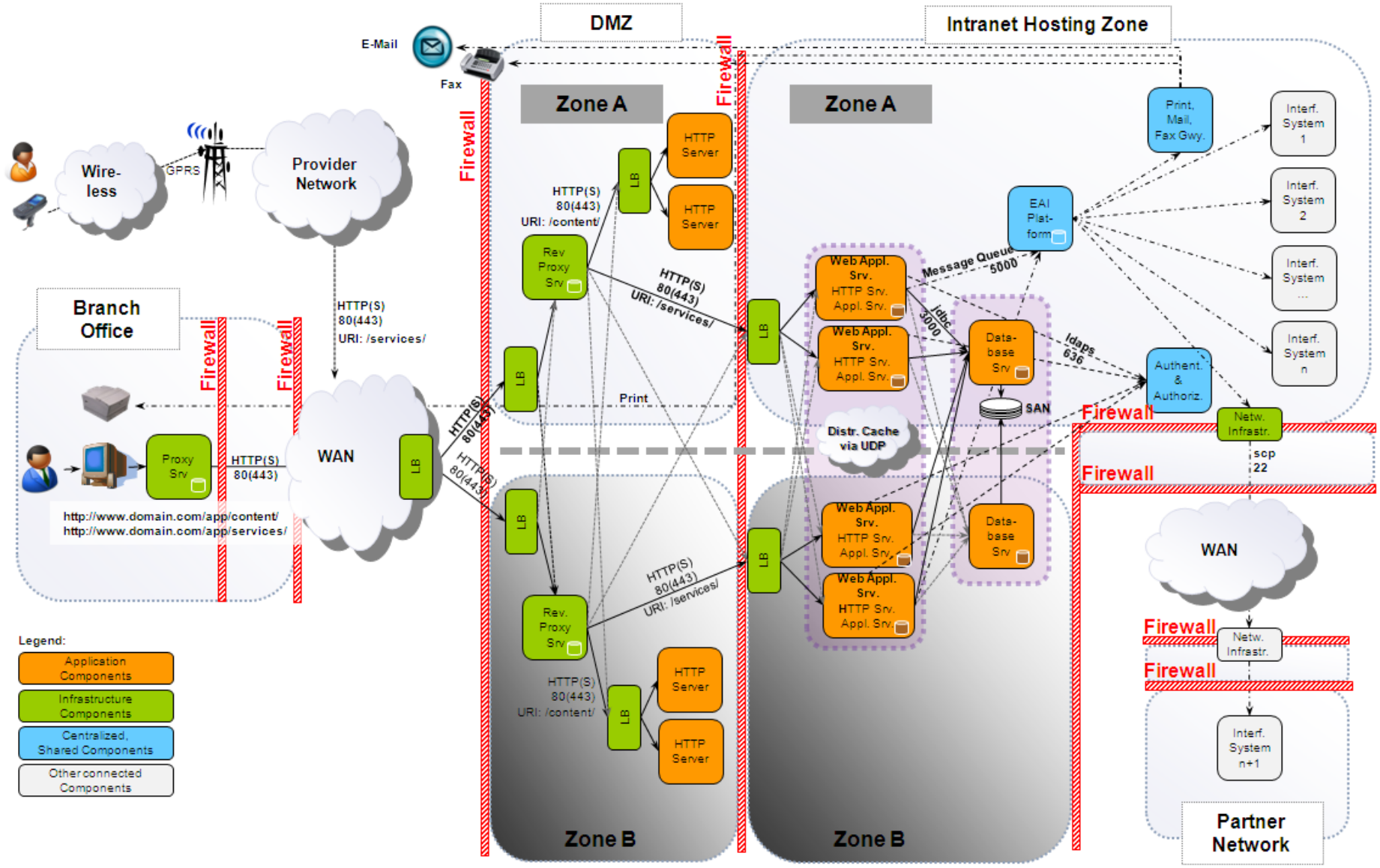
- ISSP →

  "Hang on..."

  "I'd first like to know…"

  1. Objective assessment
  2. Value of asset
  3. Impact of attack
  4. Previous incidents

How big is Your Network



Case Study - Scenario

- Internal Attack and Penetration
- Server VA already done
- Client has hardened some parts
- Services still running (port scan)
- Oracle database is present
- Our laptops are connected to the network
- Aim is to gain full control of the server

Port Scan Result

21 File Transfer [Control]
23 Telnet
25 Simple Mail Transfer
79 Finger
512 Remote process execution
513 Remote Login
514 Remote Shell
1521 Oracle8i Listener / nCube License Manager

Finger

- Finger service running by default
- Command “finger –l @hostname”

```
Login    Name          Tty      Idle    Login Time        Where
ofsa403  pts/1         1:10     Wed Jun   2 04:42       10.1.9.16
```

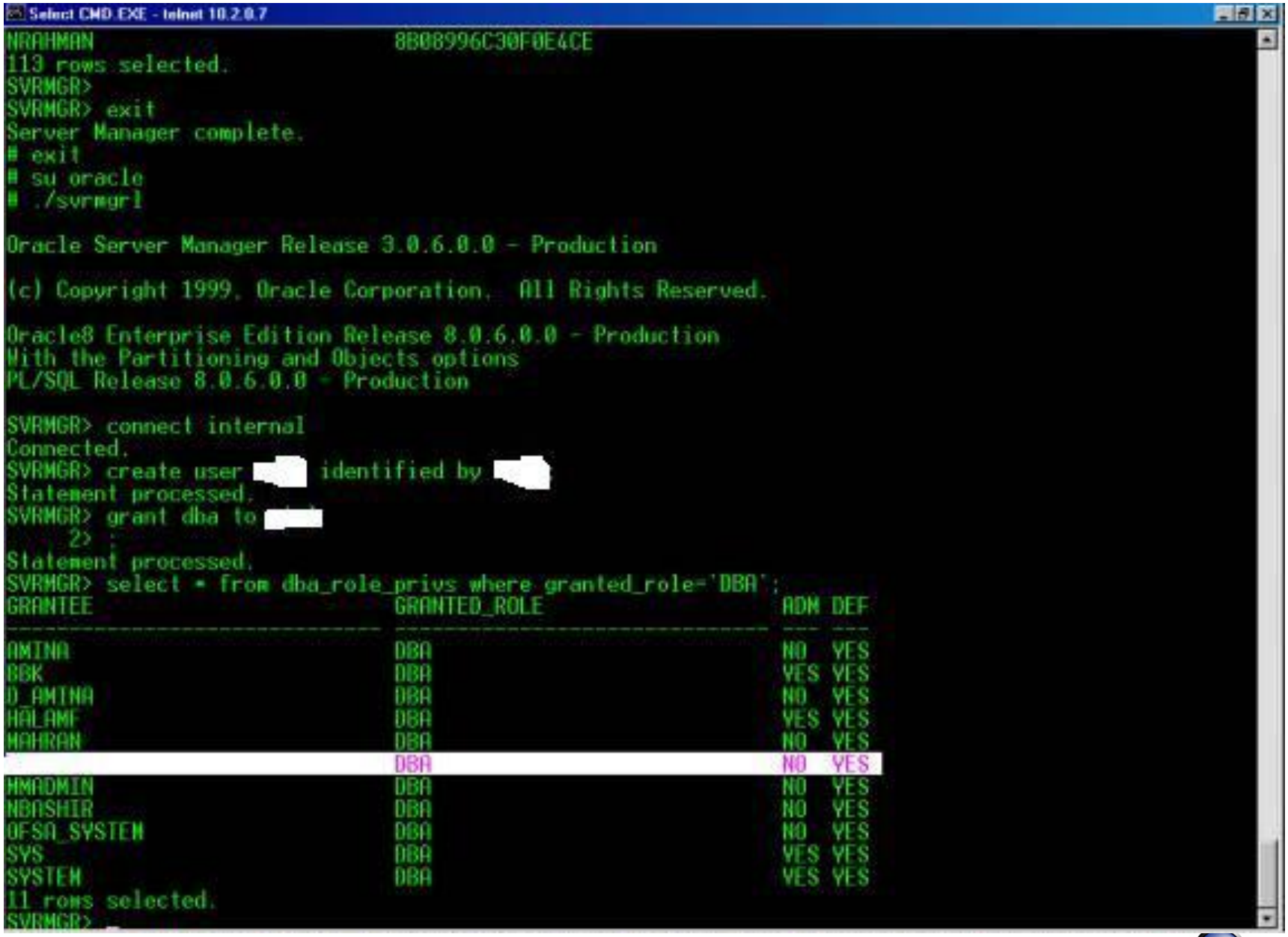
- Reveals a user ‘ofsa403’
- Probably application account
- Password attempt reveals ‘joe’ account
- Username and password are the same
- Command prompt available, but with normal user account ($), not super-user (#)

Privilege Escalation

- Some more attempts with ‘su’ command to gain root privileges – no success
- View contents of /etc/passwd
- Reveals other user ID 0 accounts – super-user accounts as:
  - Amina
  - Ofsaload
  - Odmadmin
  - Odm
- Use ‘su’ to gain elevate privileges
- Attack succeeds with username ‘ofsaload’, and password is the hostname of the machine ‘ofsa’
- Super-user privileges gained on Unix system

Found Oracle

- Change to Oracle directory ‘cd $ORACLE_HOME’
- Try to execute ‘svrmgrl’ as super-user
- Command is successful
- But connect internal/oracle does not succeed
- So switch to oracle user ‘su oracle’
- Execute ‘svrmgrl’ again, and full access to Oracle database with ‘connect internal/oracle’
- Backdoor DBA account created successfully


Select CMD.EXE - telnet 10.2.0.7
NRAHMAN 8B08996C30F0E4CE
113 rows selected.
SVRMGR>
SVRMGR> exit
Server Manager complete.
exit
su oracle
./svrmgrl
Oracle Server Manager Release 3.0.6.0.0 - Production
(c) Copyright 1999, Oracle Corporation. All Rights Reserved.
Oracle8 Enterprise Edition Release 8.0.6.0.0 - Production
With the Partitioning and Objects options
PL/SQL Release 8.0.6.0.0 - Production
SVRMGR> connect internal
Connected.
SVRMGR> create user [redacted] identified by [redacted]
Statement processed.
SVRMGR> grant dba to [redacted]
2> ;
Statement processed.
SVRMGR> select * from dba_role_privs where granted_role='DBA';
GRANTEE GRANTED_ROLE ADM DEF
AMINA DBA NO YES
BBK DBA YES YES
D_AMINA DBA NO YES
HALAMF DBA YES YES
MAHRAN DBA NO YES
[redacted] DBA NO YES
MMADMIN DBA NO YES
NBASHIR DBA NO YES
OFSA_SYSTEM DBA NO YES
SYS DBA YES YES
SYSTEM DBA YES YES
11 rows selected.
SVRMGR>

Phases of Pentest

- Intelligence Gathering
  - What we call as "Recon"
- Network Mapping
  - Identifying WHAT is in network
- Vulnerability Discovery
  - It's not just scanning
- Exploitation
- Reporting

Recon Phase

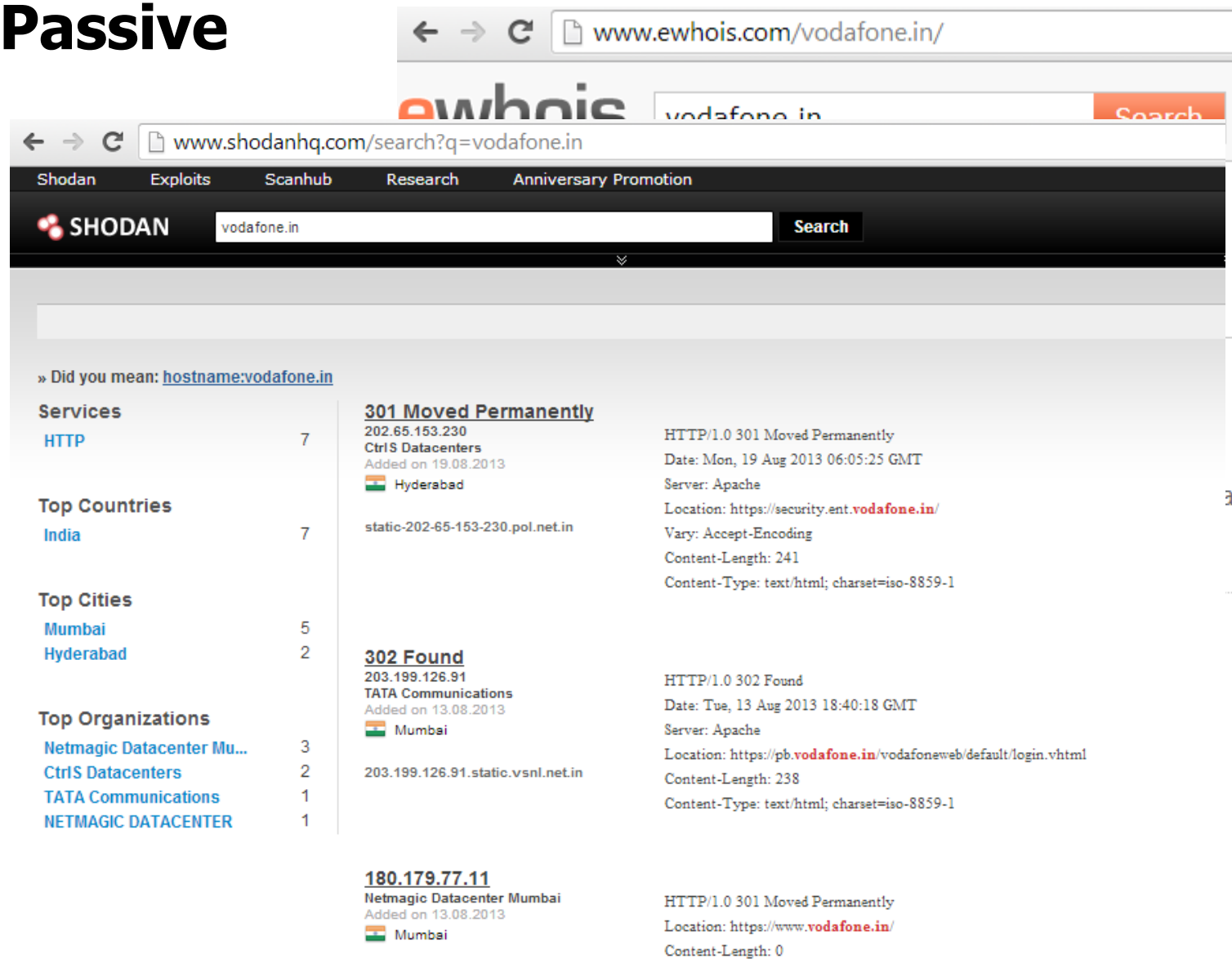
- A survey to know more about the target systems
- It can be done actively and passively
- Active – sending probe request
- Passive – see information in public, or analyzing probe responses, without making direct contact with the targets

What you should do in “Recon” ?

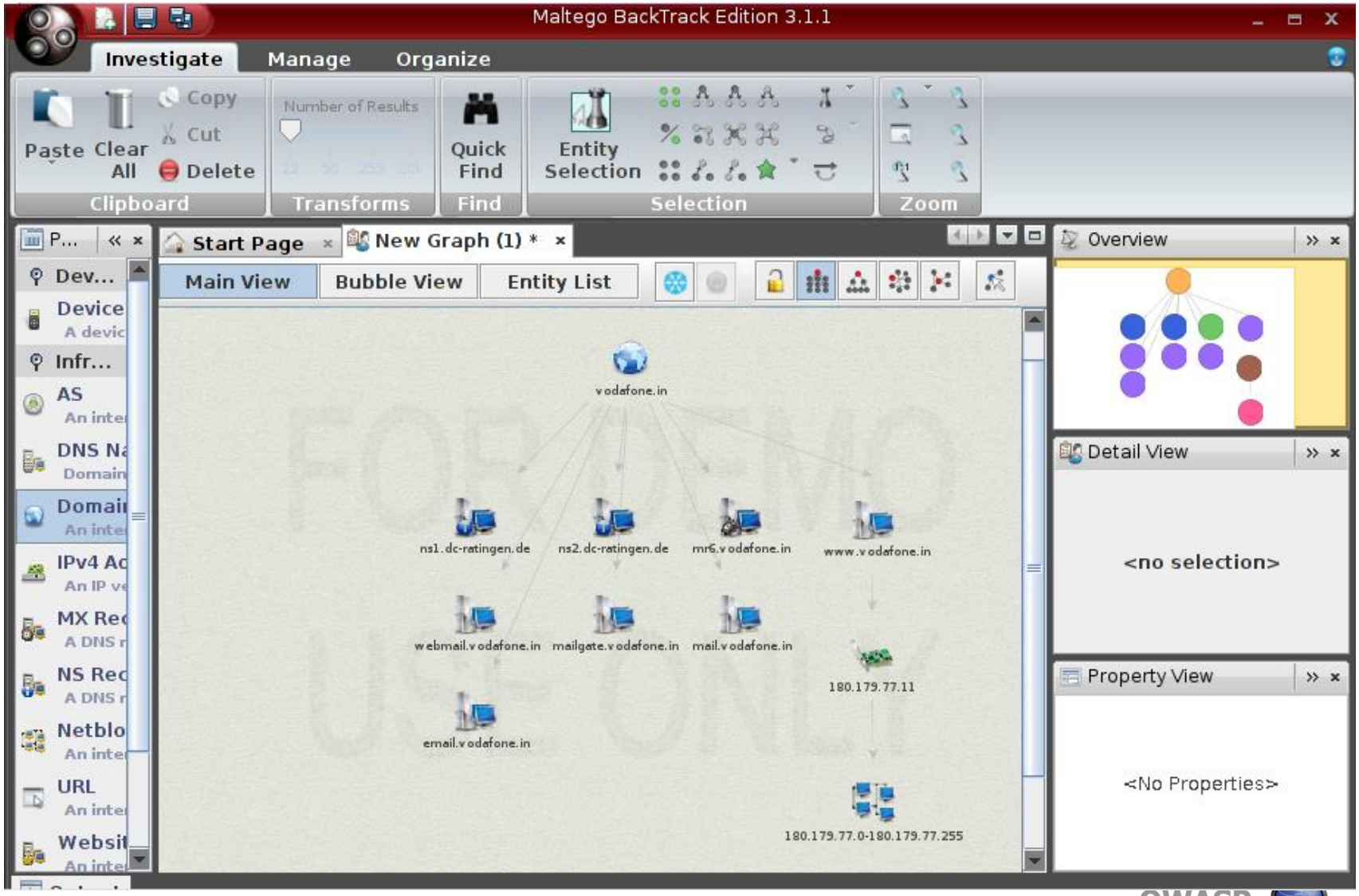
- It’s slightly beyond than collecting IPs
- Rather validate the scope
- Host Enumeration
  - whois, DNS, Reverse DNS, Analytics Lookup
  - www.robtex.com
  - ewhois.com
  - shodanhq.com

- We’ll take vodafone for example (no offensive acts)

Passive


www.ewhois.com/vodafone.in/
ewhois
vodafone.in
Search
www.shodanhq.com/search?q=vodafone.in
Shodan
Exploits
Scanhub
Research
Anniversary Promotion
SHODAN
vodafone.in
Search
» Did you mean: hostname:vodafone.in
Services
HTTP 7
Top Countries
India 7
Top Cities
Mumbai 5
Hyderabad 2
Top Organizations
Netmagic Datacenter Mu... 3
CtrlS Datacenters 2
TATA Communications 1
NETMAGIC DATACENTER 1
301 Moved Permanently
202.65.153.230
CtrlS Datacenters
Added on 19.08.2013
Hyderabad
static-202-65-153-230.pol.net.in
HTTP/1.0 301 Moved Permanently
Date: Mon, 19 Aug 2013 06:05:25 GMT
Server: Apache
Location: https://security.ent.vodafone.in/
Vary: Accept-Encoding
Content-Length: 241
Content-Type: text/html; charset=iso-8859-1
302 Found
203.199.126.91
TATA Communications
Added on 13.08.2013
Mumbai
203.199.126.91.static.vsnl.net.in
HTTP/1.0 302 Found
Date: Tue, 13 Aug 2013 18:40:18 GMT
Server: Apache
Location: https://pb.vodafone.in/vodafoneweb/default/login.vhtml
Content-Length: 238
Content-Type: text/html; charset=iso-8859-1
180.179.77.11
Netmagic Datacenter Mumbai
Added on 13.08.2013
Mumbai
HTTP/1.0 301 Moved Permanently
Location: https://www.vodafone.in/
Content-Length: 0
atalogs Today

Data Relationship



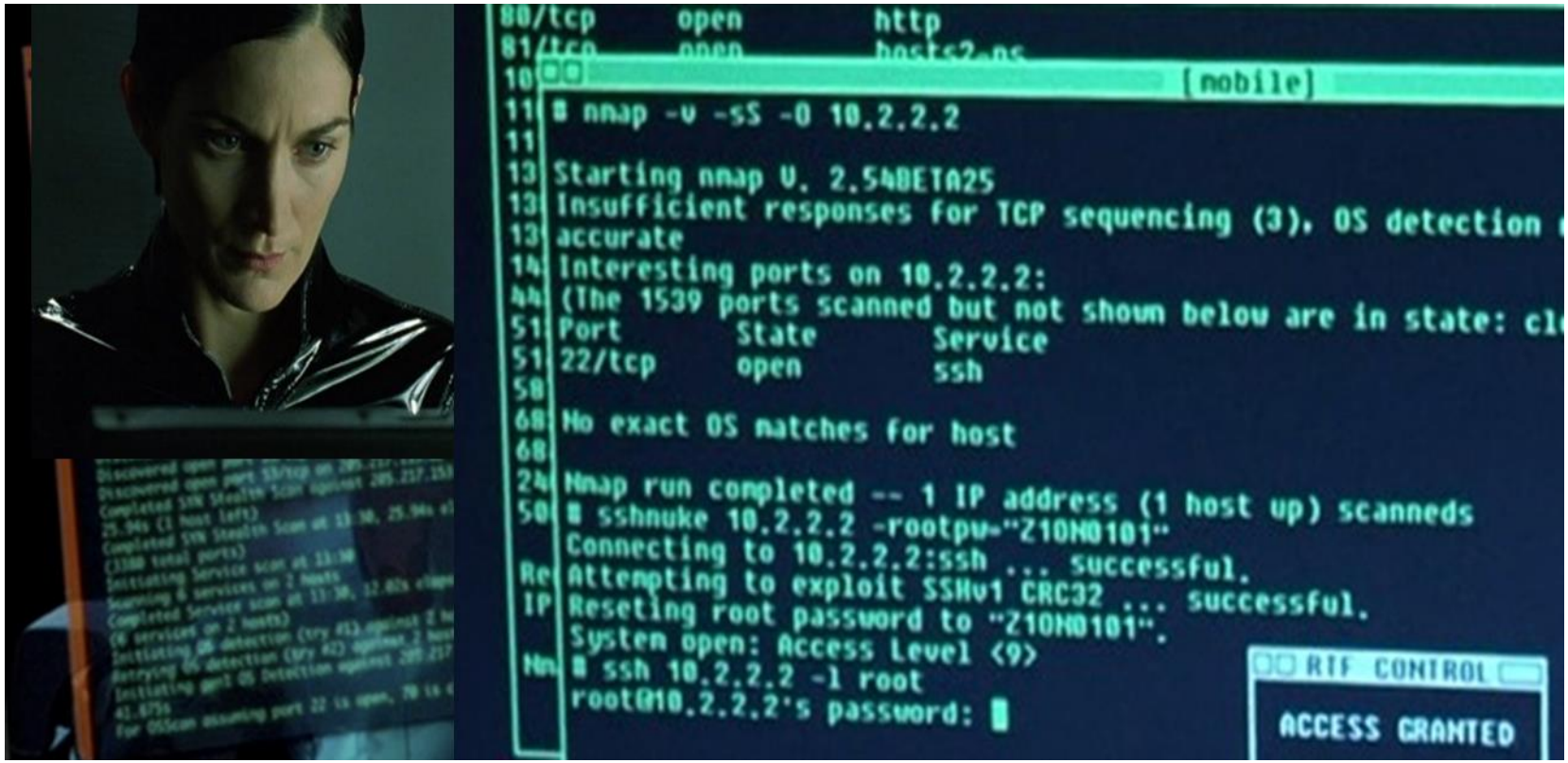
Recon-ng

```
recon-ng > show modules

  Discovery
```

```
recon-ng > load recon/contacts/gather/http/web/jigsaw
recon-ng [jigsaw] > set COMPANY vodafone.in
COMPANY => vodafone.in
recon-ng [jigsaw] > run
[*] Gathering Company IDs...
[*] Query: http://www.jigsaw.com/FreeTextSearchCompany.xhtml?opCode=search&freeText=vodafone.in
[*] Unique Company Match Found: 2030353
[*] Gathering Contact IDs for Company '2030353'...
[*] Query: http://www.jigsaw.com/SearchContact.xhtml?rpage=1&opCode=showCompDir&companyId=2030353
[*] Fetching BotMitigationCookie...
[*] Query: http://www.jigsaw.com/SearchContact.xhtml?rpage=1&opCode=showCompDir&companyId=2030353
[*] Query: http://www.jigsaw.com/SearchContact.xhtml?rpage=2&opCode=showCompDir&companyId=2030353
[*] Gathering Contacts...
[*] [45999551] Reji Abraham - President (New Delhi, DL - India)
[*] [44926790] Sandip Das - Deputy Managing Director (New Delhi, DL - India)
[*] [44926827] Rajesh Dongre - Chief Operating Officer of Rajasthan (New Delhi, DL - India)
[*] [44927224] Sanjoy Mukherjee - Head of Operations-North (New Delhi, DL - India)
[*] [29794167] Gaurav Khera - Deputy Manager Information Technology Outsourcing (New Delhi, DL - India)
[*] [29794174] Nirupmay Kumar - Head Information Technology (New Delhi, DL - India)
[*] [29794176] Nihar Mishra - Senior Vice President Head of Corporate Informatio… (New Delhi, DL - India)
[*] [29794184] Ashutosh Aggarwal - Senior Manager-Information Technology B S S-E A I (New Delhi, DL - India)
[*] [45577952] Mike Bearns - President (New Delhi, DL - India)
[*] [29794185] Fenil Sha - Manager-information Technology (New Delhi, DL - India)
[*] [29794154] Amit Gangopadhyay - Data-Center and Technology Infrastructure Incharge (New Delhi, DL - India)
[*] [29794156] Dipesh Sheth - Head Information Technology Maharashtra and Goa (New Delhi, DL - India)
[*] [29794177] Abdul Hameed Khan - Head-Information Technology M P Circle and Informa… (New Delhi, DL - India)
[*] [29794182] Vipin Kaushik - Head-Information Technology (New Delhi, DL - India)
[*] [29794164] Jayanta Chatterjee - Information Technology Head (New Delhi, DL - India)
[*] 15 total contacts found.
```

Network Mapping – Like in the Movies



How Nmap Works ?

- Step 1 : Nmap do a DNS lookup
- Step 2 : Nmap checks the IP is alive (ping)
- Step 3 : Nmap do reverse DNS lookup
- Step 4 : Nmap executes the scan

Obstacles while “Nmap”ing

- Firewalls
- Ping is not allowed ← Nmap fails in the 2st step
- Intrusion Detections/Preventions System
- Different setup for different enterprise

Evasion Techniques

- Firewalls usually blocks **"ping"**
  - Ping means ICMP Type 8 Code 0 (echo request)
- Control the scanning speed
- Fragmentation Theory
- Adding random data
- Randomizing the hosts/port
- Decoy Scanning
- Source port
  - Scans originate from port 53 (DNS) are not blocked in firewalls

Beyond Traditional Nmap Scan

- nmap -A scanme.nmap.org

```
C:\Users\SANOOP>nmap -A scanme.nmap.org

Starting Nmap 6.40 ( http://nmap.org ) at 2013-08-28 17:42 India Standard Time
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.30s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   3.00 ms   192.168.15.100
2   39.00 ms  ABTS-mum-Static-001.117.169.122.airtelbroadband.in (122.169.117.1)

3   ...
4   30.00 ms  125.18.13.137
5   153.00 ms 125.62.187.193
6   154.00 ms 40gigabitethernet1-1.core1.lon1.he.net (195.66.224.21)
7   278.00 ms 10gigabitethernet10-4.core1.nyc4.he.net (72.52.92.241)
8   290.00 ms 10gigabitethernet9-7.core1.sjc2.he.net (184.105.213.197)
9   332.00 ms 10gigabitethernet3-2.core3.fmt2.he.net (184.105.222.13)
10  291.00 ms linode-llc.10gigabitethernet7-6.core3.fmt2.he.net (65.49.10.218)
11  291.00 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.13 seconds

C:\Users\SANOOP>
```

Nmap Scripts

- Amazing addition in Nmap
- 450+ scripts for penetrating into multiple technologies
  - Enumeration
  - Denial Of Services
  - Brute force
  - Exploit
  - Version & Vulnerability Detection
  - Malwares
  - …and lot more

See more : nmap.org/nsedoc/

What Are Nmap Scripts

- Written in LUA language
  - Other Applications : Wireshark, Angry Bird, world of warcraft
- Conditional based execution
- Aggressive scan will not execute all scripts
- Many “http” based scripts in the latest release

NSE Skelton

```
description =[[this is a test on port 80]]
author = “owasp”
categories =  {"safe", "discovery"}

require "shortport"

portrule = shortport.port_or_service({80,8080,443},{"http"},{"tcp"})

action = function(host,port)
    return "Webserver found on port "..port.number
end
```

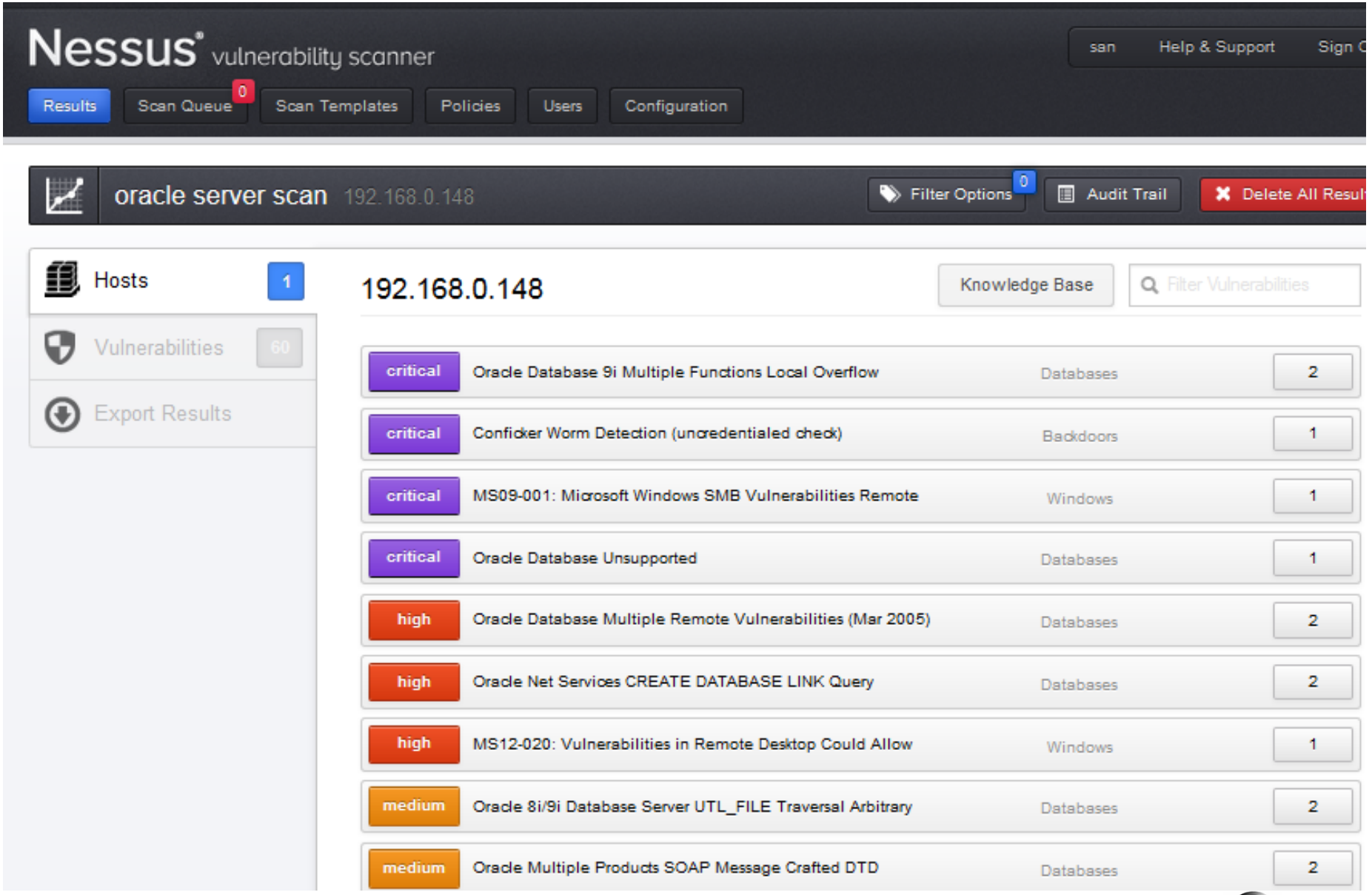
Use NSE Smartly

- nmap --script http-auth example.com
- nmap --script http-* example.com
- nmap --script http-* and not brute example.com
- nmap --script http-* and ftp-* example.com

Discovering Vulnerability

- Automated Scanners
  - Nessus, GFI, Nexpose, OpenVAS

- What to do a vulnerability definition is not available in scanners
  - Vulnerability Databases
    - Exploit-db
    - Security focus
    - OSVDB
    - CVE Detaills


Nessus vulnerability scanner
san
Help & Support
Sign
Results
Scan Queue
0
Scan Templates
Policies
Users
Configuration
oracle server scan 192.168.0.148
Filter Options
0
Audit Trail
Delete All Result
Hosts
1
Vulnerabilities
60
Export Results
192.168.0.148
Knowledge Base
Filter Vulnerabilities
critical
Oracle Database 9i Multiple Functions Local Overflow
Databases
2
critical
Conficker Worm Detection (uncredentialed check)
Backdoors
1
critical
MS09-001: Microsoft Windows SMB Vulnerabilities Remote
Windows
1
critical
Oracle Database Unsupported
Databases
1
high
Oracle Database Multiple Remote Vulnerabilities (Mar 2005)
Databases
2
high
Oracle Net Services CREATE DATABASE LINK Query
Databases
2
high
MS12-020: Vulnerabilities in Remote Desktop Could Allow
Windows
1
medium
Oracle 8i/9i Database Server UTL_FILE Traversal Arbitrary
Databases
2
medium
Oracle Multiple Products SOAP Message Crafted DTD
Databases
2

Exploiting the Enterprise

- Common Services
  - SNMP
  - SMTP
  - Administration Service – Telnet, SSH
  - FTP
  - VPN
  - Database – Oracle/MS SQL
  - Webservers – IIS, Apache, Web Logic

SNMP Issues

- It uses community string
  - Community String = Password
- Defaults
  - Public = read only
  - Private = read and write

SNMPWALK

```
root@bt:~# snmpwalk -c public -v 2c 192.168.15.131
SNMPv2-MIB::sysDescr.0 = STRING: Linux ubuntu 3.2.0-23-generic-pa
P Tue Apr 10 22:19:09 UTC 2012 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (54592) 0:09:05.
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: ubuntu
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Ba
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIB
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompli
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGr
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architectu
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing
```


Database

- Crown Jewel of an Enterprise
- Oracle issues
  - Hundreds of defaults

    www.vulnerabilityassessment.co.uk/default_oracle_passwords.htm
  - Service ID enumeration
  - TNS Lister Security Issues

- Demo

VPN Testing - Blackbox

- Step 1 : Service Enumeration
- Step 2 : Service Endpoint Fingerprinting
- Step 3 : Force switch to aggressive mode
- Step 4 : Crack

- Tools of trade : ike-scan, ike-probe, ike-crack

- Demo

Exploit the Enterprise (cont..)

- Metasploit Framework
- A Framework which can
  - Use precooked exploits, auxiliary etc.
  - Select appropriate payloads
  - Do a ton of post exploitation modules
- But the challenge is
  - Antivirus

Exploit the Enterprise

Demo

Scenario Based Attack

Project Report

- Most difficult part (atleast for me)
- What it should contain:
  - Vulnerability Description
  - Vulnerability Analysis
  - PoC of Attack
  - Impact Analysis
  - Recommendations

Report - Summary Section

- Background of testing
  - Reason of why the project has initiated
  - Objective defined and validated in the scope
  - Other information shared with the testing team
- Testing Metrics
  - # of systems
  - # of time taken
  - # of vulnerabilities identified
  - … and more

Report - Technical Section

- Reconnaissance Outputs and Observations
- Vulnerability Classification Levels
  - Critical/High/Medium/Low
- Technical Details of each vulnerability
  - Vulnerability Identification Scenarios
  - Details of Exploitable Vulnerabilities
  - Countermeasures to fix
  - Proof of successful exploitation

Reporting - References

An Excellent diagram on what all need to be present in reporting

http://www.pentest-standard.org/index.php/Reporting

Conclusion

- A good pentester is one with a creative skillsets and updated knowledge
- Today hackers don’t take over the technology; rather they take over your business.
- Stop securing the devices; start securing your information inside it.

Thank You

Sanoop Thomas
@s4n7h0
sanoop.thomas@iisecurity.in