

Enumeration

Module 4

Engineered by **Hackers**. Presented by Professionals.



SECURITY NEWS



December 13, 2010 10:41 AM

Why Gawker's Security Breach Is So Bad

A group of hackers has infiltrated Nick Denton's Gawker Media empire in what some are calling the most damaging cyber security breach of a media company to date.

The usernames, emails and passwords of up to **1.3 million registered users** were published to the web over the weekend. The blogs under the Gawker Media umbrella include Gizmodo, Deadspin, Kotaku, Jezebel, i09, Jalopnik, Lifehacker and Fleshbot.

A group named "**Gnosis**" is taking responsibility for attack, telling Mediaite: "We went after Gawker because of their outright arrogance." Many suspect this in reference to the cyber attacks waged against Gawker in July, in which Gawker taunted hackers at 4Chan.org and flaunted its ability to withstand DDOS attacks.

The hacker group also sent a message to Gawker:

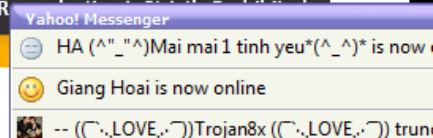
Your empire has been compromised, Your servers, Your database's, Online accounts and source code have all been ripped to shreds! You wanted attention, well guess what, You've got it now!

<http://www.theatlanticwire.com>



All Rights Reserved. R

Copyright © by EC-Council



Module Objectives

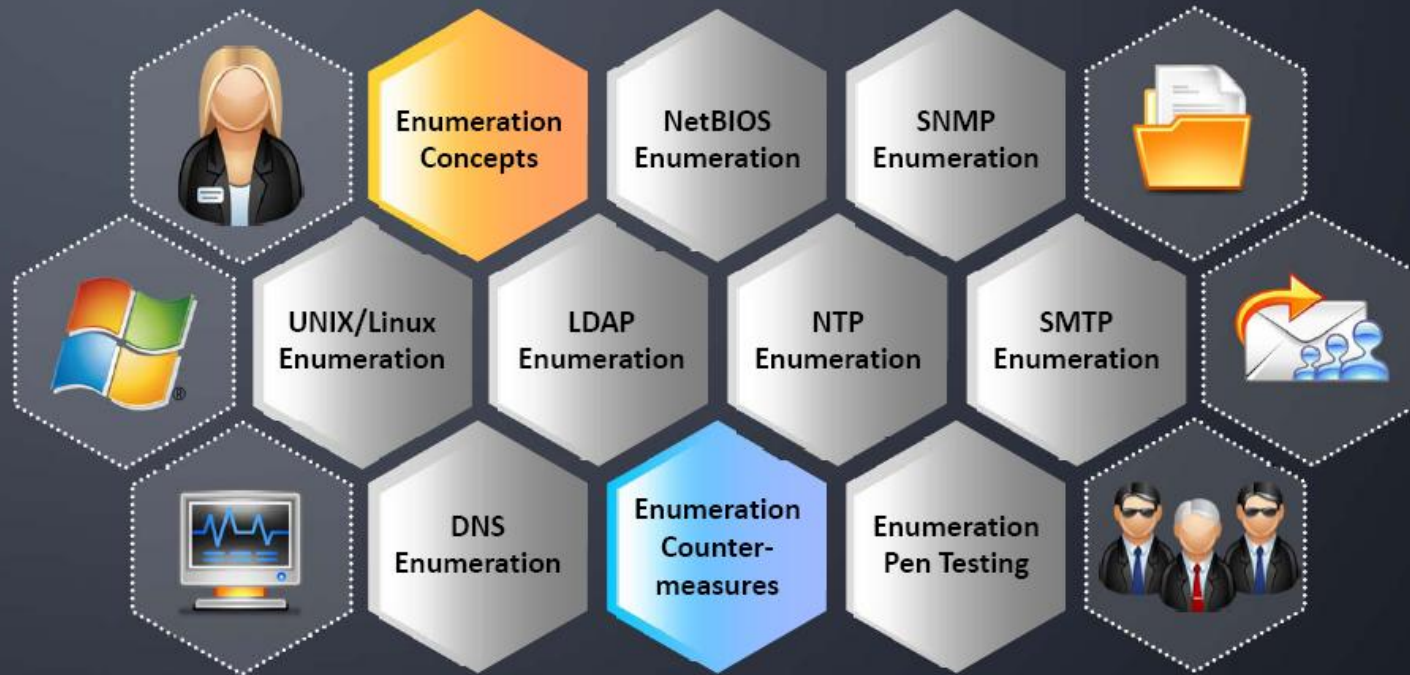
- Enumeration
- Techniques for Enumeration
- NetBIOS Enumeration
- Enumerating User Accounts
- SNMP Enumeration



- Unix/Linux Enumeration
- LDAP/Active Directory Enumeration
- NTP Enumeration
- SMTP and DNS Enumeration
- Enumeration Countermeasures

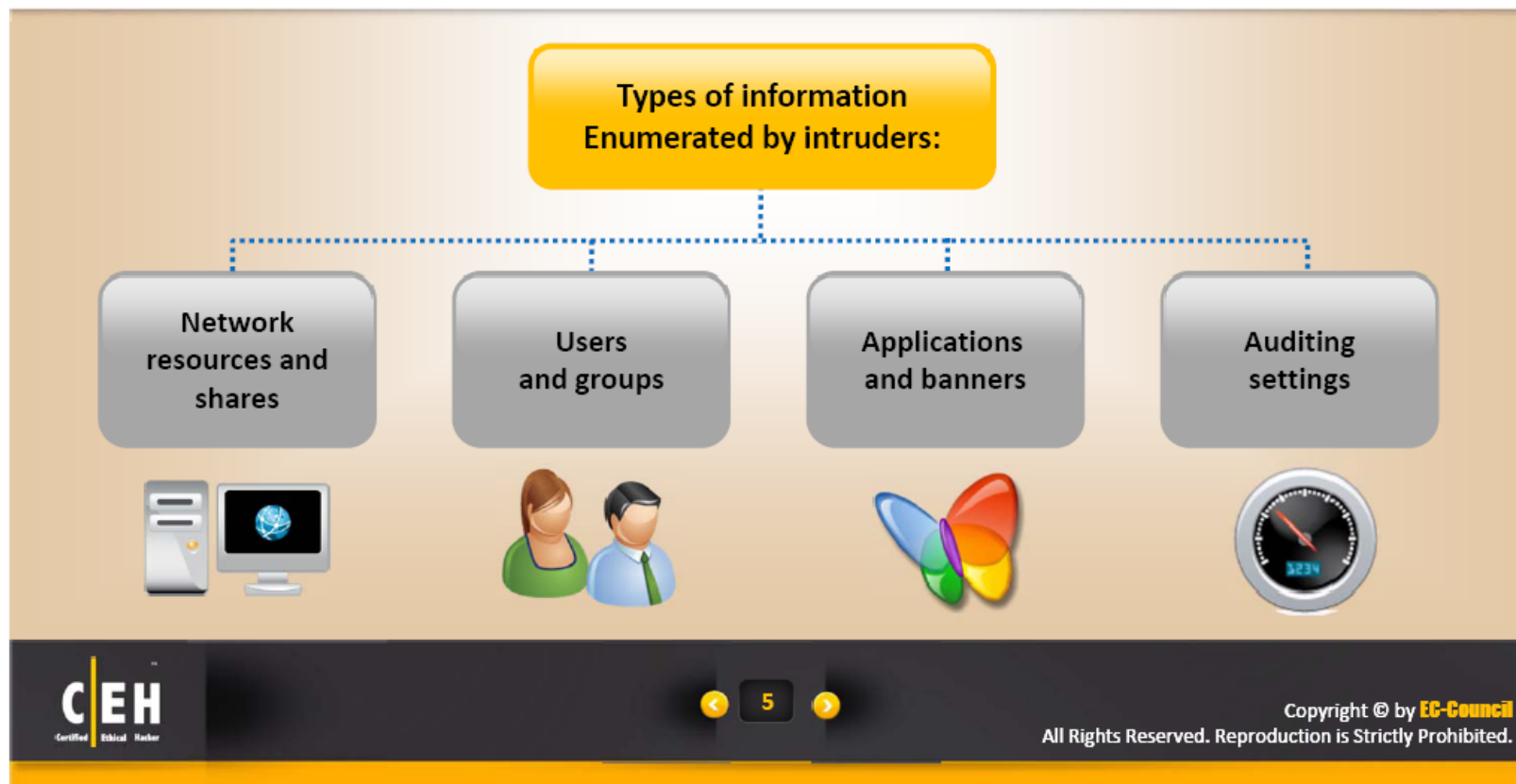


Module Flow

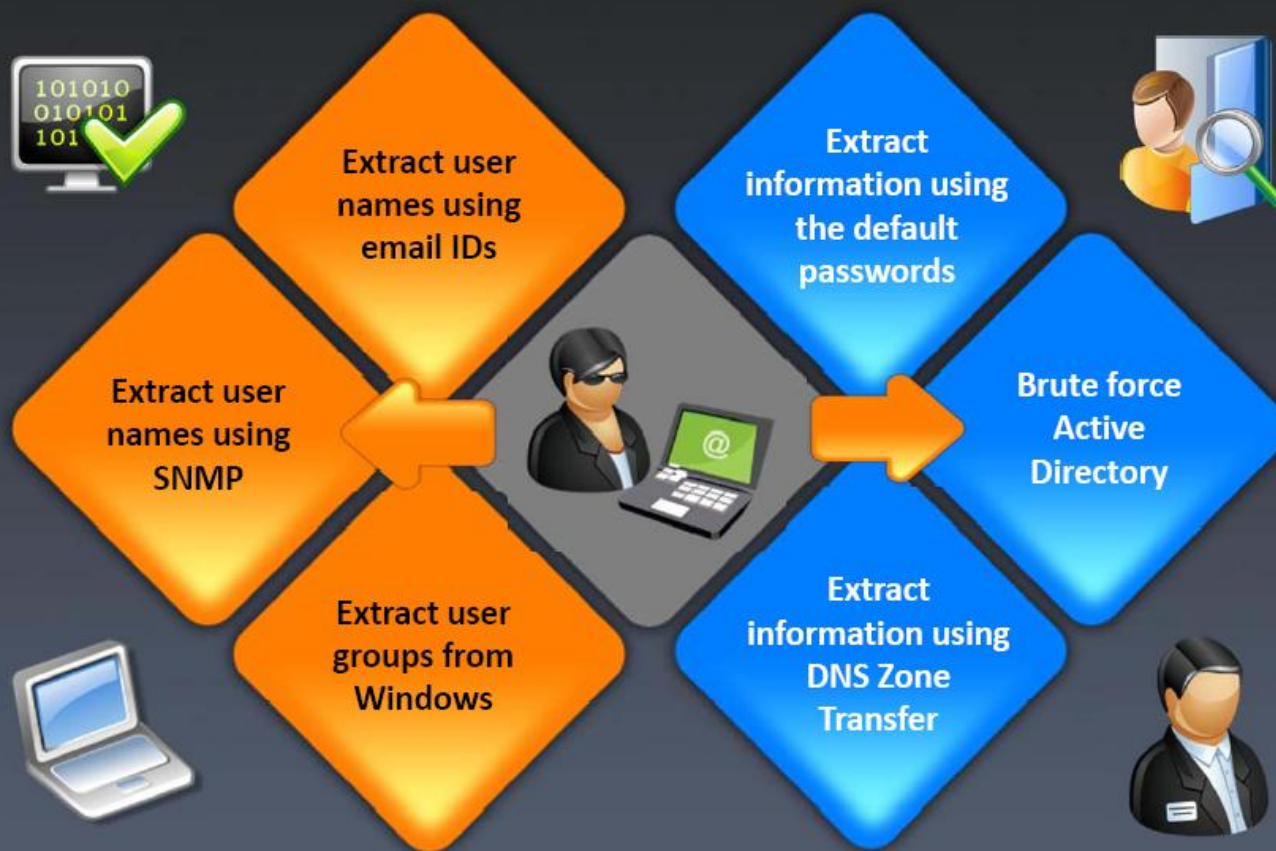


What is Enumeration?

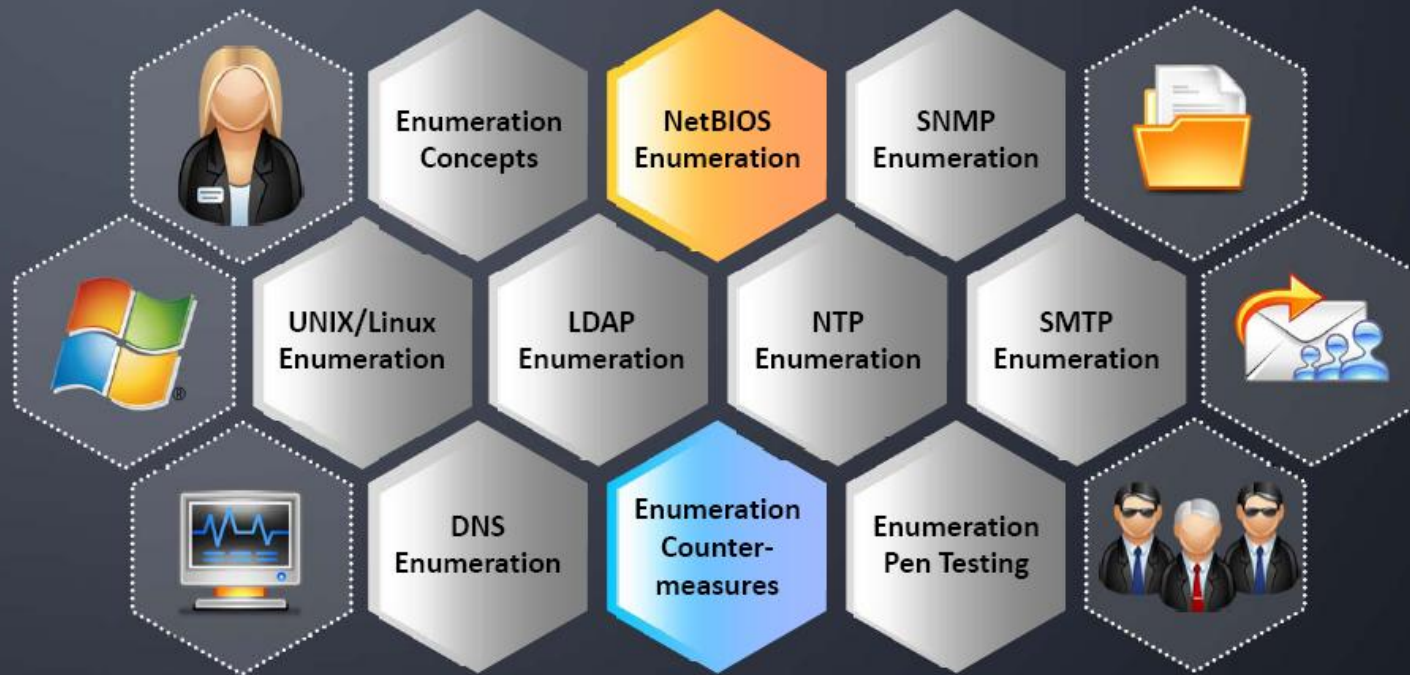
- Enumeration is defined as the process of **extracting user names**, machine names, network resources, shares, and services from a system
- Enumeration techniques are conducted in an **intranet environment**



Techniques for Enumeration



Module Flow



Netbios Enumeration

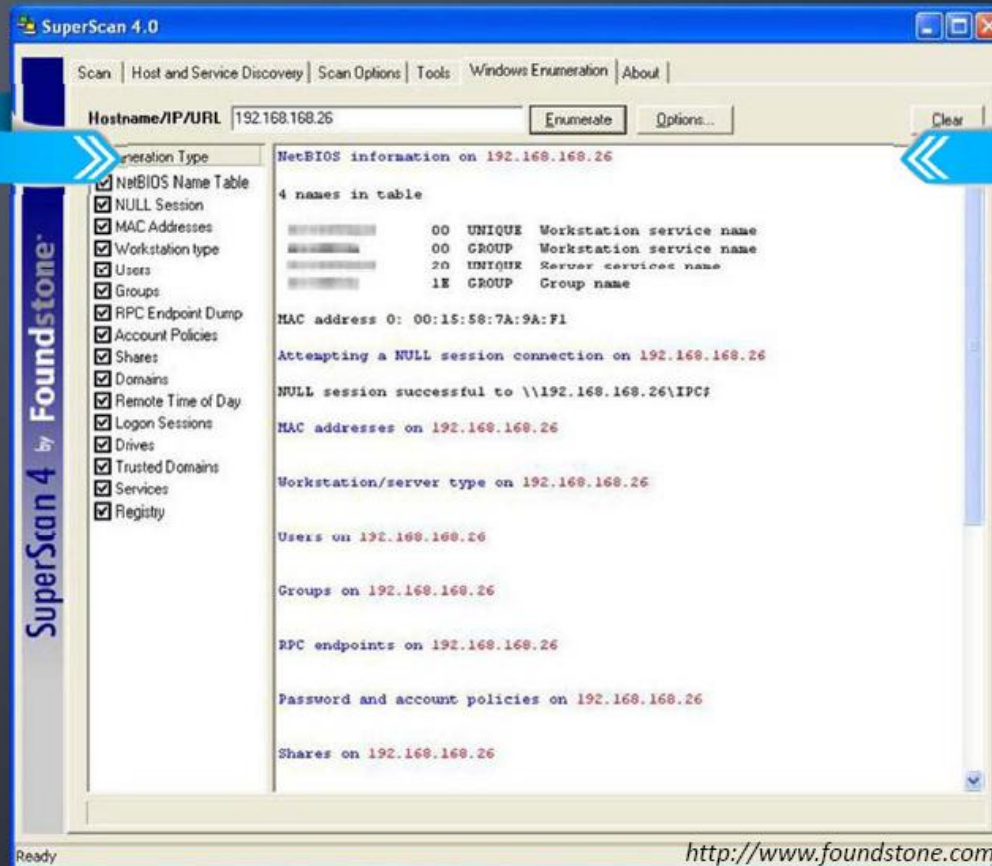
Attackers use the NetBios enumeration to obtain:

1. List of computers that belong to a domain
2. List of shares on the individual hosts on the network
3. Policies and passwords

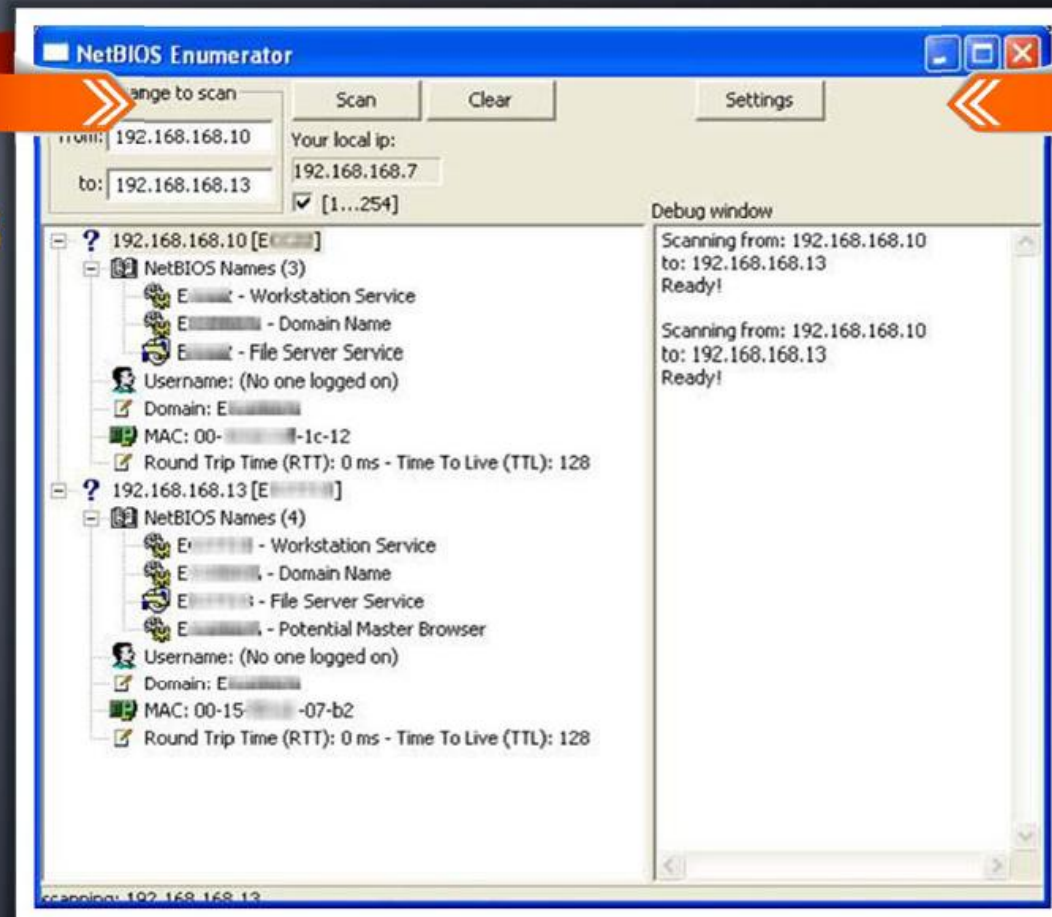


Port	Service
TCP 53	DNS zone transfer
TCP 135	Microsoft RPC Endpoint Mapper
TCP 137	NetBIOS Name Service (NBNS)
UDP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP/UDP 3368	Global Catalog Service

NetBIOS Enumeration Tool: SuperScan



NetBIOS Enumeration Tool: NetBIOS Enumerator



<http://nbtenum.sourceforge.net>



Enumerating User Accounts



PsExec

<http://technet.microsoft.com>



PsFile

<http://technet.microsoft.com>



PsGetSid

<http://technet.microsoft.com>



PsKill

<http://technet.microsoft.com>



PsInfo

<http://technet.microsoft.com>



PsList

<http://technet.microsoft.com>



PsLoggedOn

<http://technet.microsoft.com>



PsLogList

<http://technet.microsoft.com>

Enumerate Systems Using Default Passwords

default password list

Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

Search

Manufacturer:

Product:

Contribute to the default password list.

Add your own experience

Manufacturer: Product: Revision:

Protocol: Multi Access:

User ID: Password:

URL ID: <http://www.defaultpassword.com>

URL ID:

URL ID:

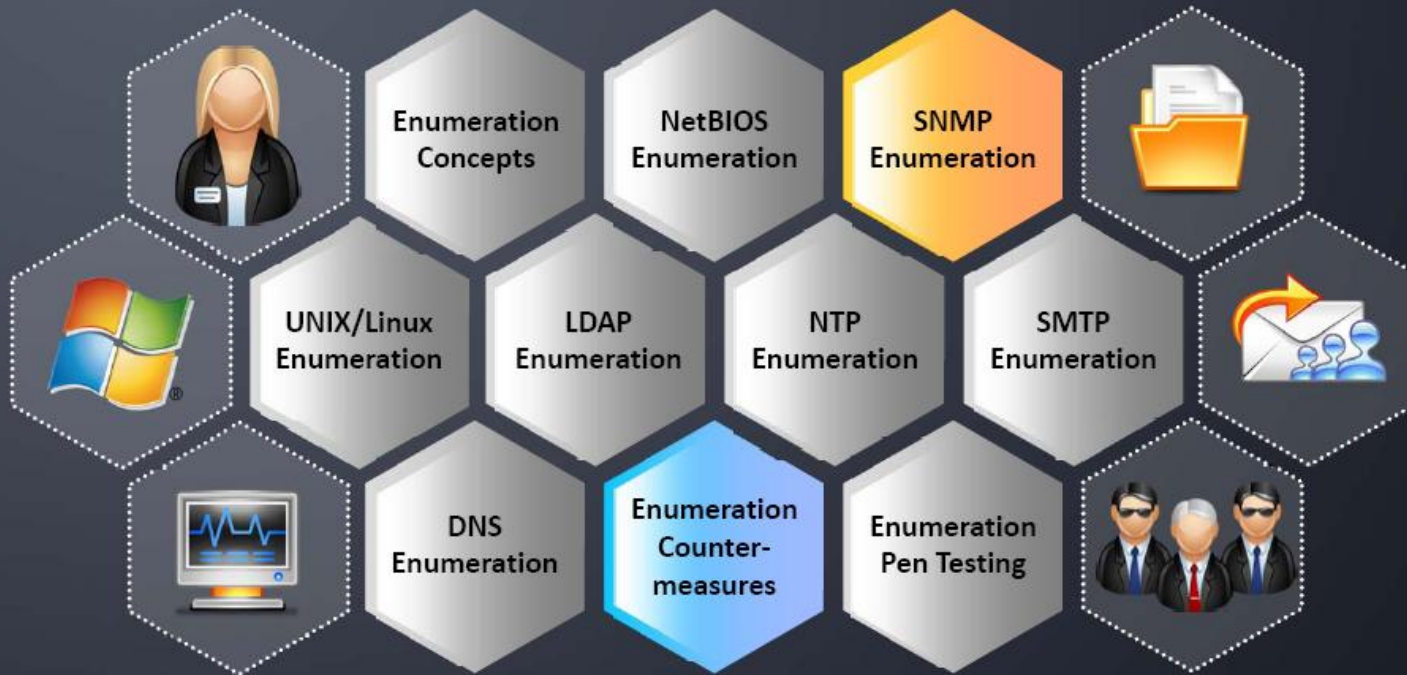


P A S W O R D

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

- Devices like switches, hubs, and routers might still be enabled with a “default password”
- Attackers gain access by using default and common passwords

Module Flow



SNMP (Simple Network Management Protocol) Enumeration



Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for **remote monitoring** and managing hosts, routers, and other devices on a network

Attackers enumerate SNMP to **extract information** about network resources such as hosts, routers, devices, shares, etc.,



SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer

The default community string that provides the monitoring or read capability is often **"public,"** whereas the default management or write community string is often **"private"**



SNMP enumeration uses these default community strings to extract information about a device using the read community string "public"



Management Information Base (**MIB**)



MIB is a virtual database containing **formal description of all the network objects** that can be managed using SNMP



The MIB database is hierarchical and each managed object in a MIB is addressed through **object identifiers (OID)**



MIB managed objects include **scalar objects** that define a single object instance and tabular objects that define group of related object instances



The OID includes the object's type such as counter, string, or address, access level such as read or read/write, size restrictions, and range information



SNMP manager uses the MIB as a **codebook** for translating the OID numbers into a human-readable display

SNMP Enumeration Tool: OpUtils Network Monitoring Toolset

ManageEngine OpUtils 5 Knowledge Base | Build# 57001 | Support | Settings | License | Talk Back | About | Help | Logout | admin

Home | Switch Port Mapper | IP Address Manager | Intranet Detection | Config File Manager | Network Monitor | Bandwidth Monitor | Wake On Lan | Reports | Admin

Alerts (665)

Address Monitoring | Network Monitoring | SNMP Tools | CISCO Tools | Custom Tools

Switch Port Mapper | Add Switch | Add Router | Scheduler | Settings | IP Address

Summary | History | Alerts | Switches | Groups | Routers | Reports | Audit

Select Criteria: All User | All Changes | All Period | All Action | Generate

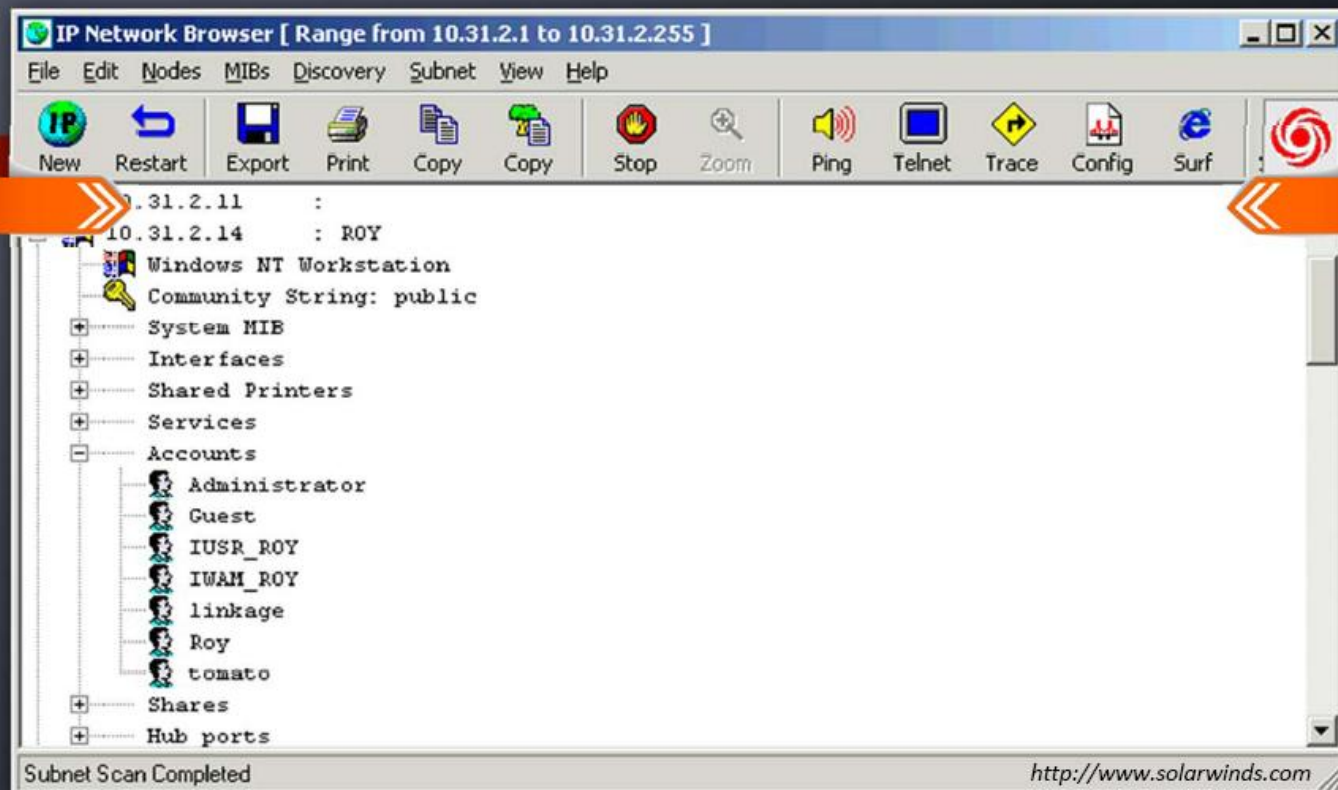
Export As: 1 - 14 of 14 | 25

Date	User	Action Performed	Changes In	Description
2009-11-03 20:12:25.103	admin	Modify	Others	Schduler has been enabled
2009-11-03 20:12:16.929	admin	Modify	Default Group	Schduler has been enabled for the group is Default Group
2009-11-03 20:12:02.828	admin	Add	cisco2011	cisco2011 has been manually added to the Routers list with SNMP community string
2009-11-03 20:10:21.439	admin	Modify	192.168.117.1	Physical location has been changed from [Not Defined] to test21 for port [22]
2009-11-03 20:10:14.995	admin	Modify	192.168.117.1	Physical location has been changed from [Not Defined] to test2 for port [9]
2009-11-03 20:09:55.664	admin	Modify	3com4400	3com4400 has been modified
2009-11-03 20:09:39.389	admin	Add	192.168.117.1	Added switch 192.168.117.1 manually to Default Group with ping sweep false
2009-11-03 20:09:33.076	admin	Add	foundry2402	Added switch foundry2402 manually to Default Group with ping sweep false
2009-11-03 20:09:26.639	admin	Add	procurve2524	Added switch procurve2524 manually to Default Group with ping sweep false
2009-11-03 20:09:20.7	admin	Add	oputils-w2k2	Added switch oputils-w2k2 manually to Default Group with ping sweep false
2009-11-03 20:09:16.981	admin	Add	3com4400	Added switch 3com4400 manually to Default Group with ping sweep false
2009-11-03 20:09:12.726	admin	Add	cisco2011	Added switch cisco2011 manually to Default Group with ping sweep false
2009-11-03 20:09:01.7	admin	Add	cisco2001	Added switch cisco2001 manually to Default Group with ping sweep false
2009-11-03 20:06:48.404	admin	Add	catalyst2900	Added switch catalyst2900 manually to Default Group with ping sweep false

© 2004-2009 Zoho Corp. | Report an Issue | Need Features | User Forums



SNMP Enumeration Tool: SolarWinds



SNMP Enumeration Tools



Getif SNMP MIB Browser
<http://www.wtcs.org>



LorientPro
<http://www.lorientpro.com>



OidView SNMP MIB Browser
<http://www.oidview.com>



SNMP Scanner
<http://www.secure-bytes.com>



iReasoning MIB Browser
<http://tl1.ireasoning.com>



Nsauditor Network Security Auditor
<http://www.nsauditor.com>

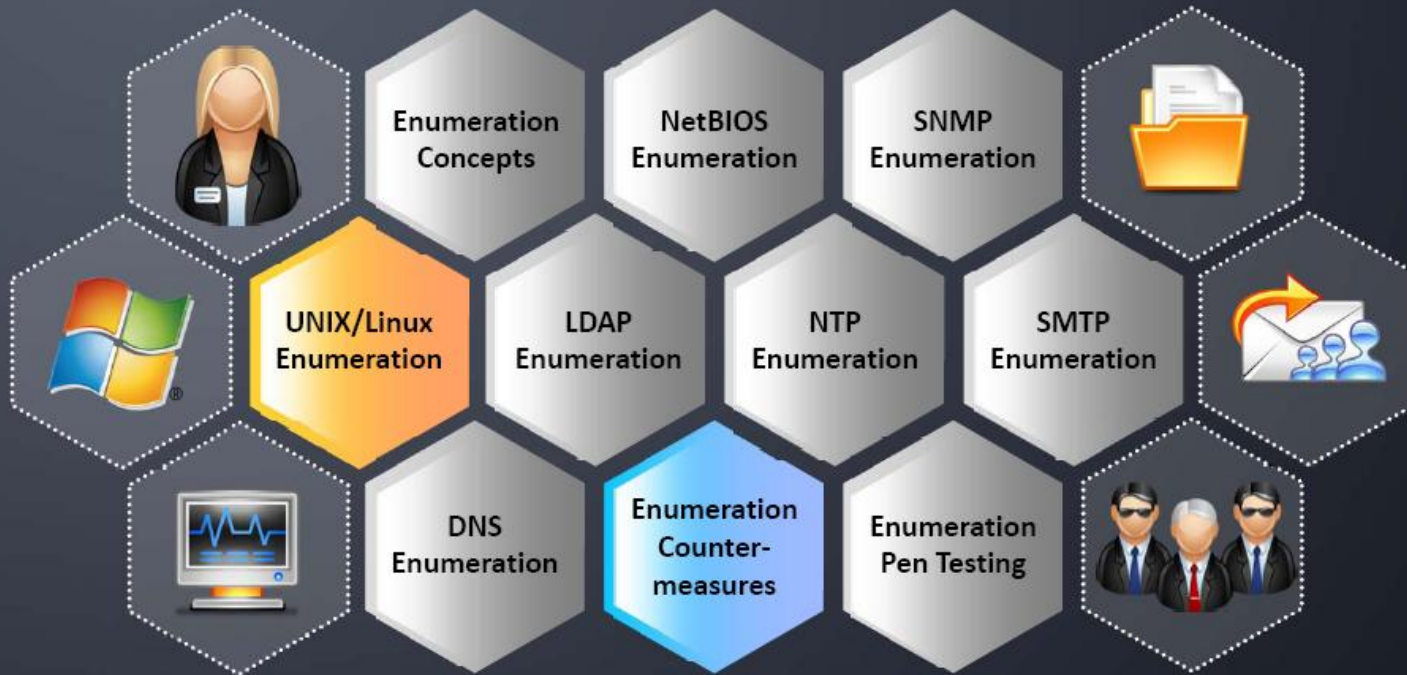


SNScan
<http://www.foundstone.com>



SoftPerfect Network Scanner
<http://www.softperfect.com>

Module Flow



UNIX/Linux Enumeration

Commands used to enumerate UNIX network resources are as follows:

showmount

1. Finds the shared directories on the machine

```
[root $] showmount -e  
19x.16x.xxx.xx
```

finger

1. Enumerates the user and the host
2. Enables you to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail

```
[root$] finger -l @target.hackme.com
```

rpcclient

1. Using rpcclient we can enumerate usernames on Linux and OS X

```
[root $] rpcclient $> netshareenum
```

rpcinfo (RPC)

1. Helps to enumerate Remote Procedure Call protocol
2. RPC protocol allows applications to communicate over the network

```
[root] rpcinfo -p 19x.16x.xxx.xx
```



```

sh-3.2$ enum4linux.pl -r 192.168.2.55
Starting enum4linux v0.8.2 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr  2 14:14:35 2008

----- Target information -----
Target ..... 192.168.2.55
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

----- Enumerating Workgroup/Domain on 192.168.2.55 -----
[+] Got domain/workgroup name: WORKGROUP

----- Getting domain SID for 192.168.2.55 -----
Domain Name: WORKGROUP
Domain Sid: S-0-0
[+] Host is part of a workgroup (not a domain)

----- Session Check on 192.168.2.55 -----
[+] Server 192.168.2.55 allows sessions using username '', password ''

----- Users on 192.168.2.55 via RID cycling (RIDS: 500-550,1000-1050) -----
[I] Assuming that user "administrator" exists
[+] Got SID: S-1-5-21-1801674531-1482476501-725345543 using username '', password ''
S-1-5-21-1801674531-1482476501-725345543-500 W2KSQL\Administrator (Local User)
S-1-5-21-1801674531-1482476501-725345543-501 W2KSQL\Guest (Local User)
S-1-5-21-1801674531-1482476501-725345543-513 W2KSQL\None (Domain Group)
S-1-5-21-1801674531-1482476501-725345543-1000 W2KSQL\TsInternetUser (Local User)
S-1-5-21-1801674531-1482476501-725345543-1001 W2KSQL\IUSR_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1002 W2KSQL\IWAM_PORTCULLIS (Local User)
S-1-5-21-1801674531-1482476501-725345543-1004 W2KSQL\mark (Local User)
S-1-5-21-1801674531-1482476501-725345543-1005 W2KSQL\blah (Local User)
S-1-5-21-1801674531-1482476501-725345543-1006 W2KSQL\basic (Local User)

enum4linux complete on Wed Apr  2 14:14:40 2008

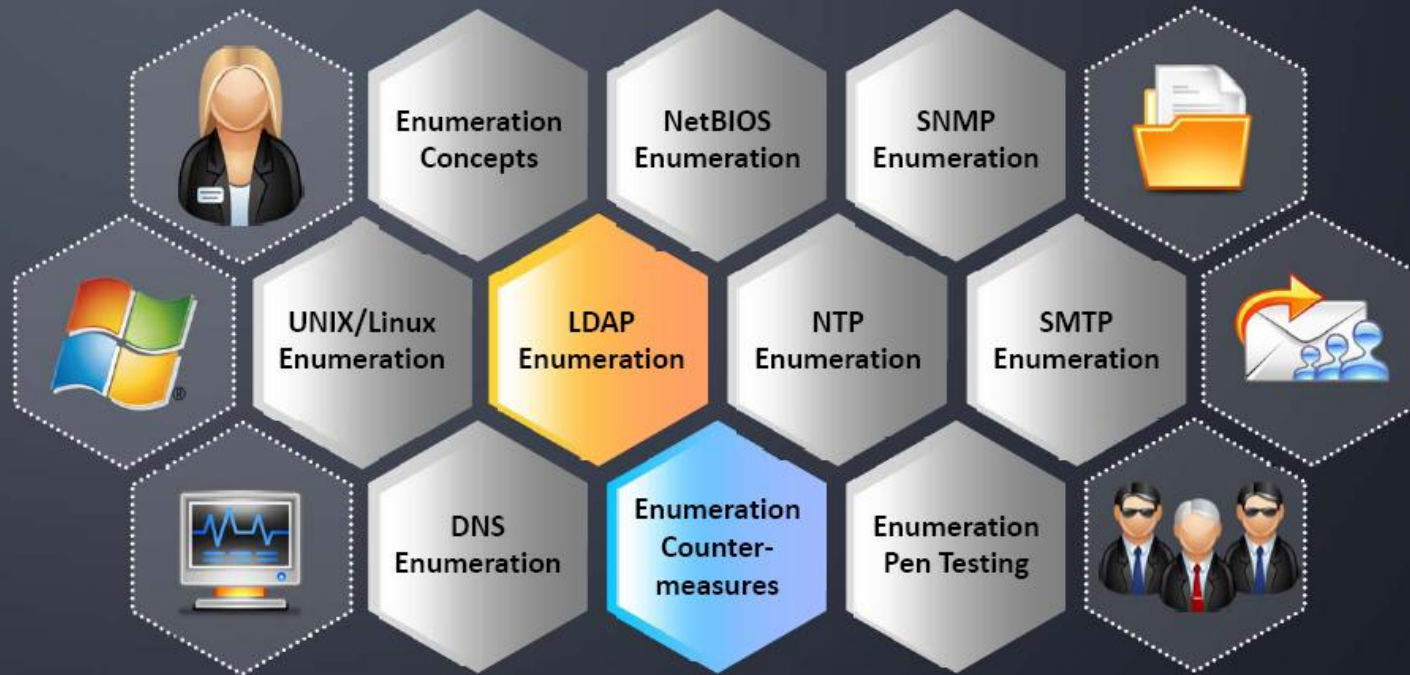
```

Linux Enumeration Tool: **Enum4linux**

<http://labs.portcullis.co.uk>



Module Flow



LDAP Enumeration



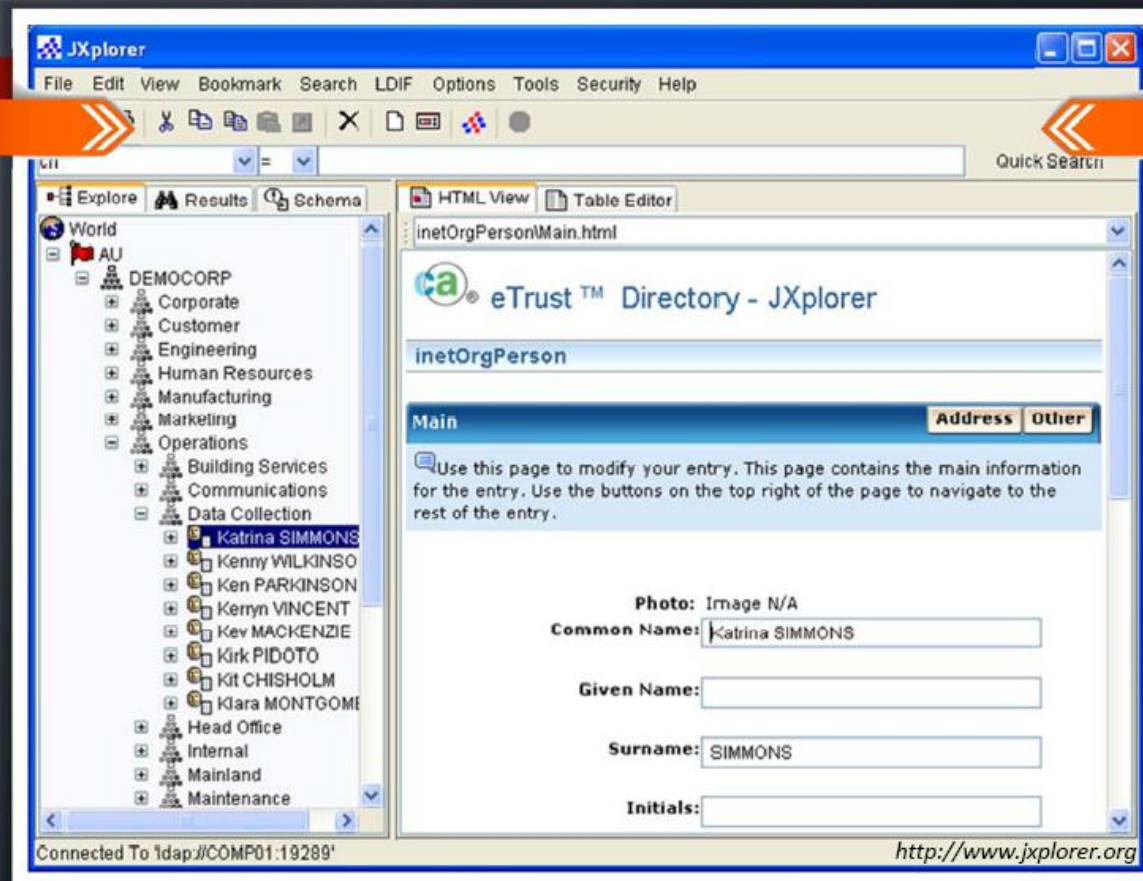
←..... The Lightweight Directory Access Protocol is a protocol used to access the directory listings within **Active Directory** or from other directory services

←..... A directory is compiled in a **hierarchical and logical format**, like the levels of management and employees in a company

←..... It tends to be tied into the **Domain Name System** to allow the integrated quick lookups and fast resolution of queries

←..... It runs on **port 389** and tends to conform to a distinct set of rules Request for comments (RFC's) like other protocols

LDAP Enumeration Tool: JXplorer



LDAP Enumeration Tool



Symlabs LDAP Browser
<http://symlabs.com>



Softerra LDAP Administrator
<http://www.ldapadministrator.com>



LDAP Admin Tool
<http://www.ldapsoft.com>



LDAP Browser Editor
<http://www.openchannelsoftware.com>



LDAP Account Manager
<http://www.ldap-account-manager.org>



LDAP Explorer Tool
<http://ldaptool.sourceforge.net>

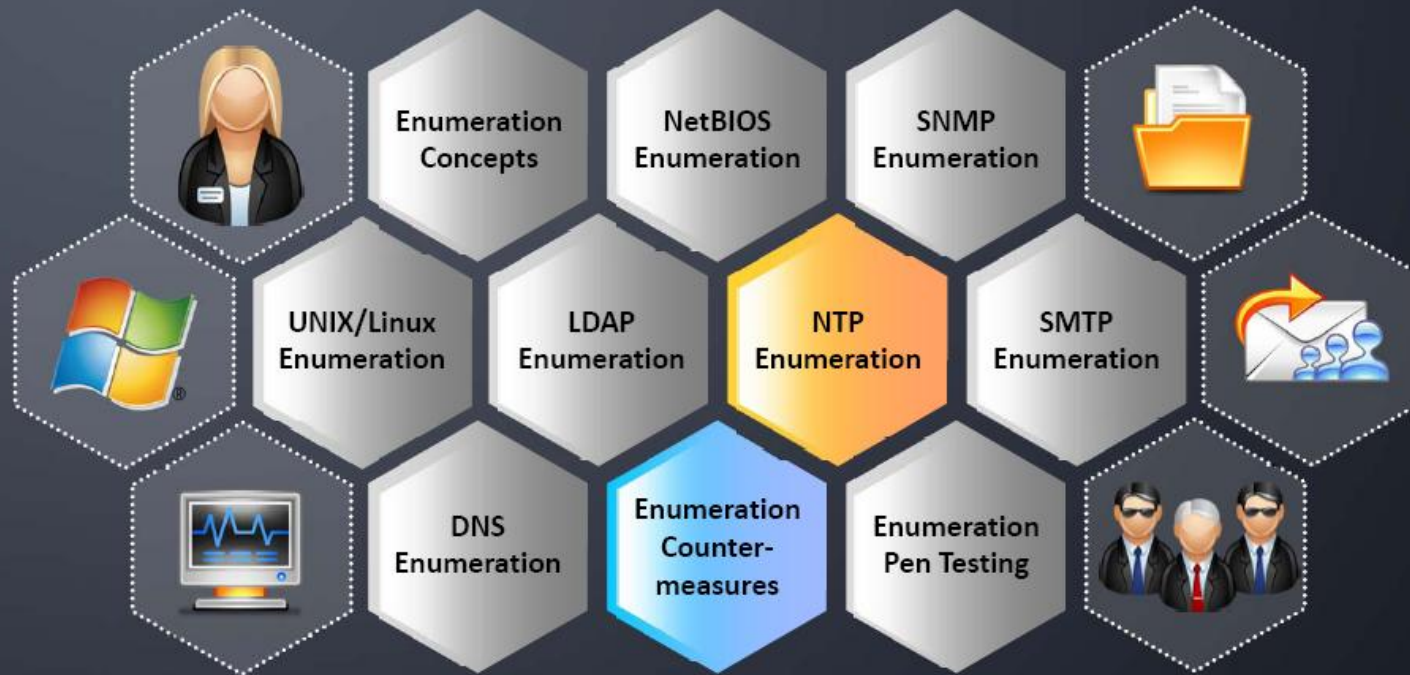


LEX - The LDAP Explorer
<http://www.ldapexplorer.com>



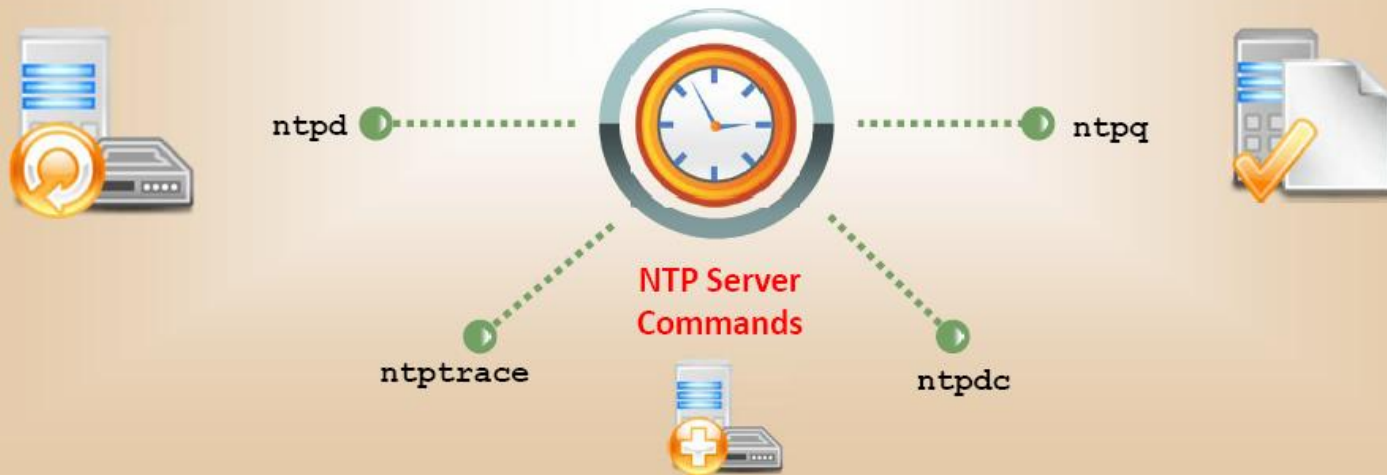
ldp.exe
<http://www.microsoft.com>

Module Flow



NTP Enumeration

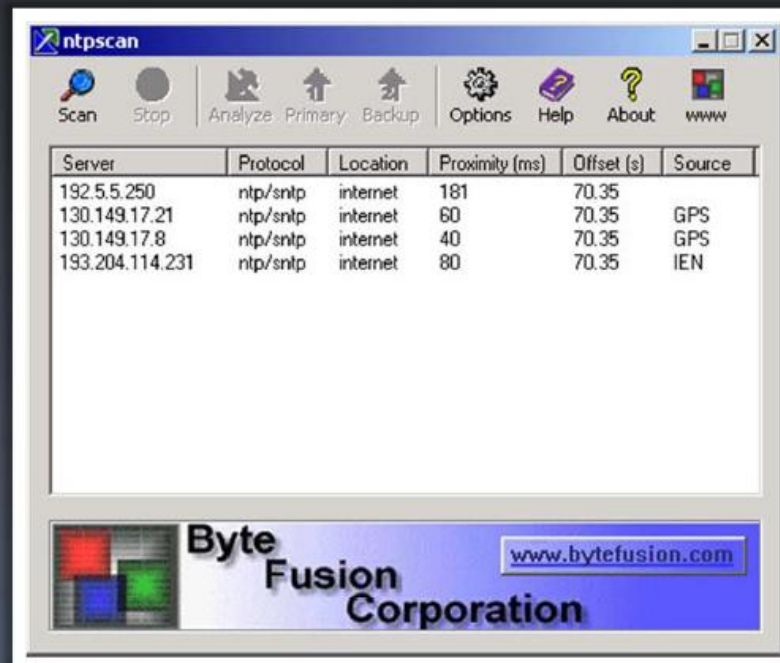
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers
- It uses **UDP port 123** as its primary means of communication
- NTP can maintain time to within **10 milliseconds (1/100 seconds)** over the public Internet
- It can achieve accuracies of **200 microseconds** or better in local area networks under ideal conditions



NTP Server Discovery Tool:

NTP Server Scanner

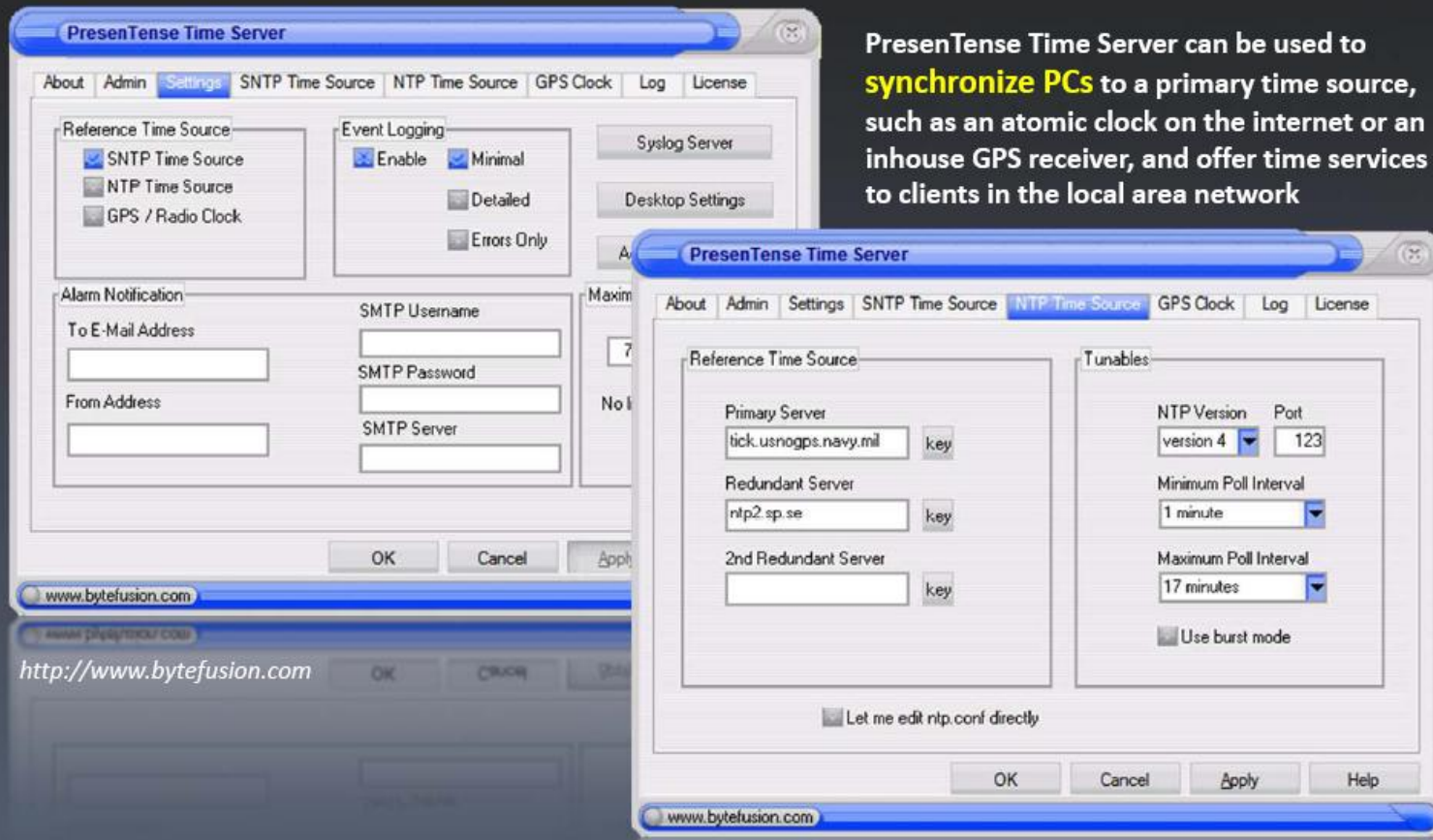
- NTP Server Scanner helps you easily **locate NTP and SNTP servers** on your network or the internet
- It helps administrators in **setting and configuring time management** on their networks
- It automatically scans and displays available servers



<http://www.bytefusion.com>

NTP Server: **PresenTense Time Server**

PresenTense Time Server can be used to **synchronize PCs** to a primary time source, such as an atomic clock on the internet or an inhouse GPS receiver, and offer time services to clients in the local area network



NTP Enumeration Tools



Presentense Time Client
<http://www.bytefusion.com>



Presentense NTP Auditor
<http://www.bytefusion.com>



LAN Time Analyser
<http://www.bytefusion.com>



NTP Time Server Monitor
<http://www.meinberg.de>



NTP Server Checker
<http://www.galsys.co.uk>



NTP Time Server Monitor
<http://www.meinberg.de>

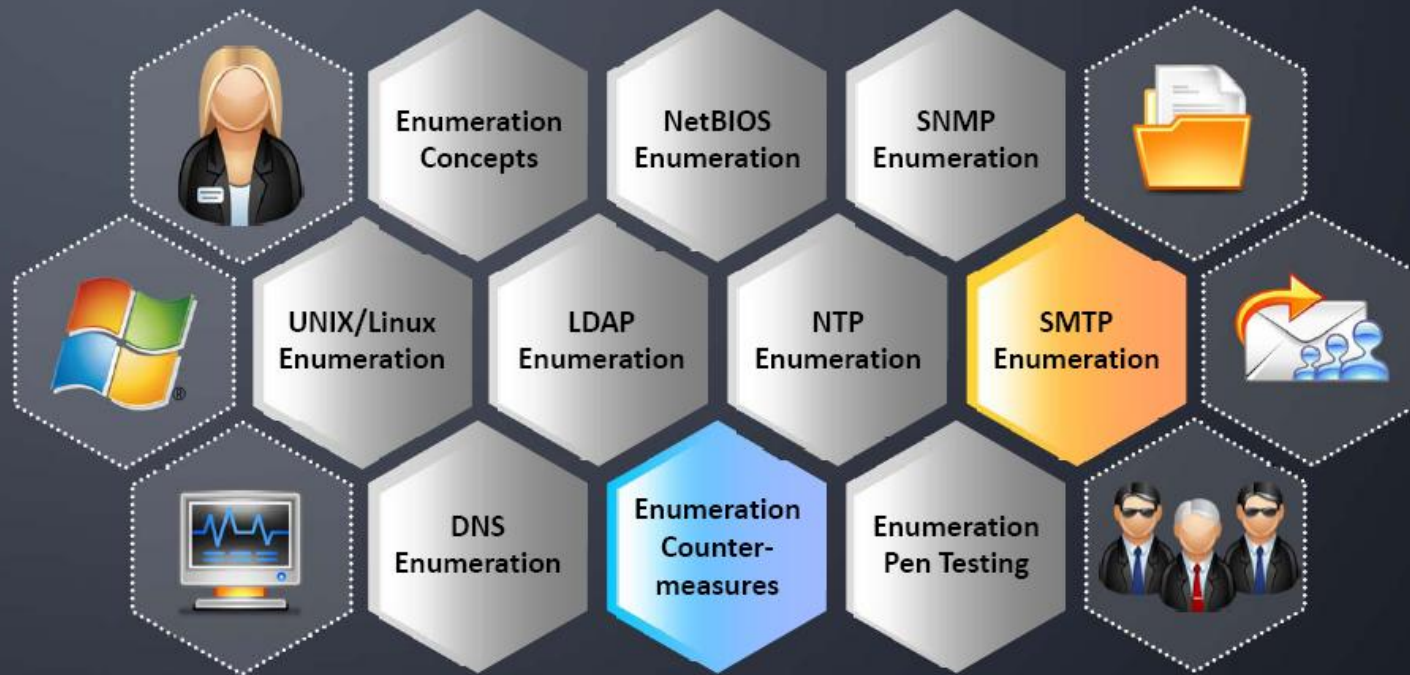


Time Watch
<http://www.blue-series.com>



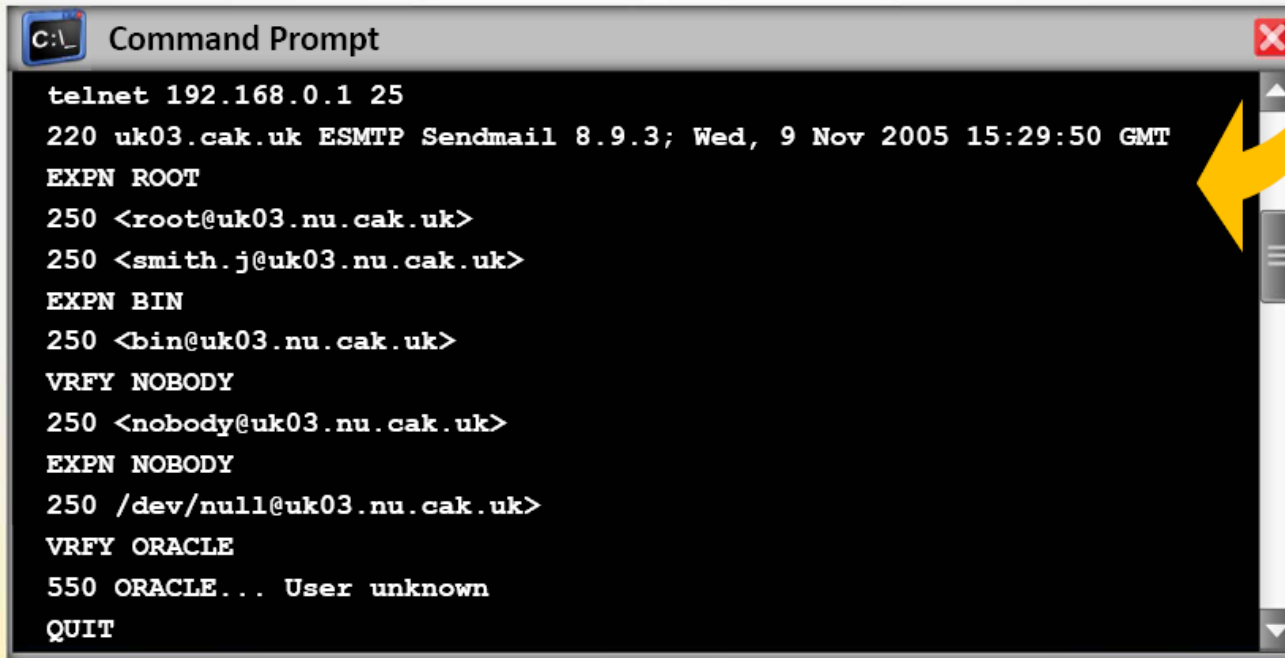
AtomSync
<http://www.emtec.com>

Module Flow



SMTP Enumeration

Attackers can directly interact with SMTP via the telnet prompt:



```
C:\_ Command Prompt
telnet 192.168.0.1 25
220 uk03.cak.uk ESMTP Sendmail 8.9.3; Wed, 9 Nov 2005 15:29:50 GMT
EXPN ROOT
250 <root@uk03.nu.cak.uk>
250 <smith.j@uk03.nu.cak.uk>
EXPN BIN
250 <bin@uk03.nu.cak.uk>
VERFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VERFY ORACLE
550 ORACLE... User unknown
QUIT
```


SMTP Enumeration Tool: NetScanTools Pro

SMTP Email Generator and Relay Test Use this tool to send test email messages with SMTP. Check SMTP servers for open relays without sending email using 17 common relay tests.

SMTP outgoing mail server name (server.domain.com or IP address - required)
someweirdomain.com

Send Test Message
Stop Sending Message
Message Settings

Global Test Settings
HELO login ID: DellXP
SMTP Port: 25
Network Timeout: 60 Seconds
 Enable Logging
View Log File
Delete Log File

Email Relay Testing

Start SMTP Relay Test

Your Sending Domain Name: junkdomain.com

Stop Relay Test

View Relay Test Results

View Results as Text
View Results in Web Browser

Tests to run

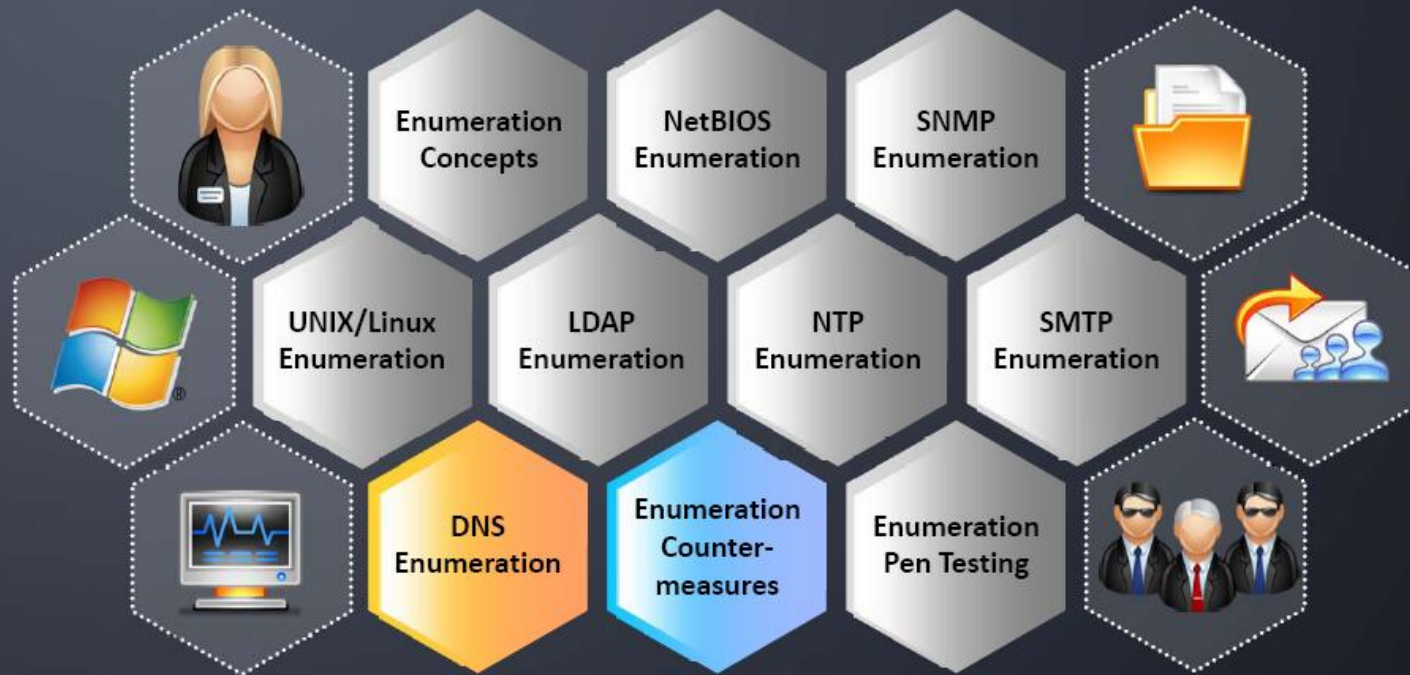
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	10
<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	11
<input checked="" type="checkbox"/>	3	<input checked="" type="checkbox"/>	12
<input checked="" type="checkbox"/>	4	<input checked="" type="checkbox"/>	13
<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	14
<input checked="" type="checkbox"/>	6	<input checked="" type="checkbox"/>	15
<input checked="" type="checkbox"/>	7	<input checked="" type="checkbox"/>	16
<input checked="" type="checkbox"/>	8	<input checked="" type="checkbox"/>	17
<input checked="" type="checkbox"/>	9		

NetScanTool Pro's SMTP Email Generator and Email Relay Testing Tools are designed for testing the process of sending an email message through an SMTP server and performing relay tests by communicating with a SMTP server

<http://www.netscantools.com>



Module Flow



DNS Zone Transfer Enumeration

Using **nslookup**

- It is a process of locating the DNS server and the records of a target network
- An attacker can **gather** valuable network information such as DNS server names, hostnames, machine names, user names, etc
- In a DNS zone transfer enumeration, an attacker tries to **retrieve** a copy of the entire zone file for a domain from a DNS server

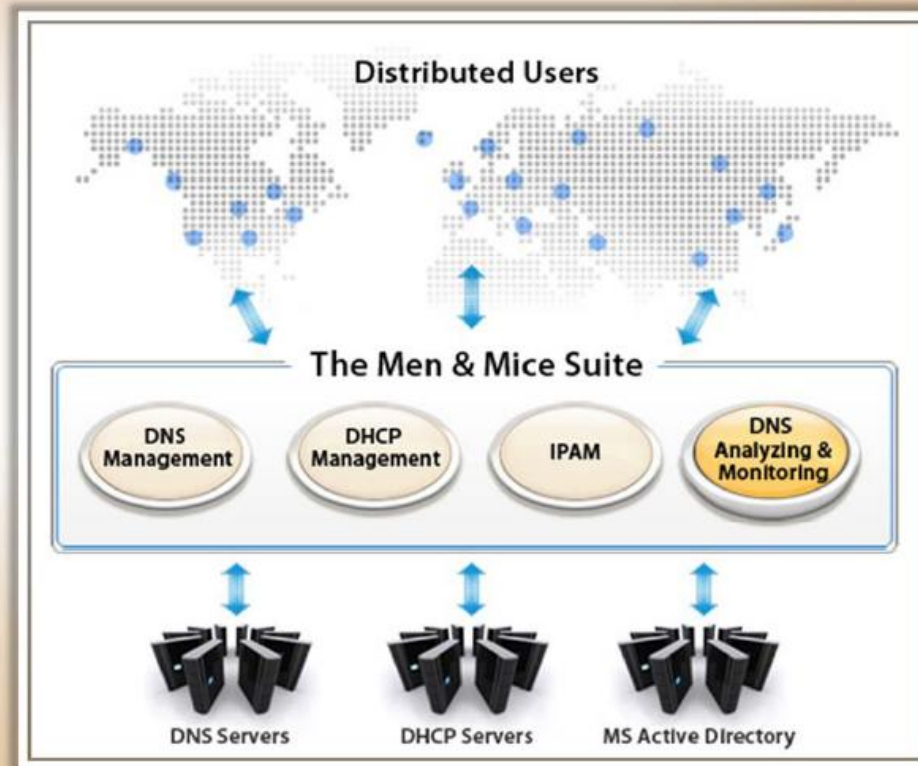


```
C:\>nslookup
Default Server: ns1.example.com
Address: 10.219.100.1
> server 192.168.234.110
Default Server: corp-dc.example2.org
Address: 192.168.234.110
> ls -d example2.org
[[192.168.234.110]]
example2.org. SOA corp-dc.example2.org admin.
example2.org. A 192.168.234.110
example2.org. NS corp-dc.example2.org
.
_gc._tcp SRV priority=0, weight=100, port=3268, corp-dc.example2.org
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.example2.org
_kpasswd._tcp SRV priority=0, weight=100, port=464, corp-dc.example2.org
```



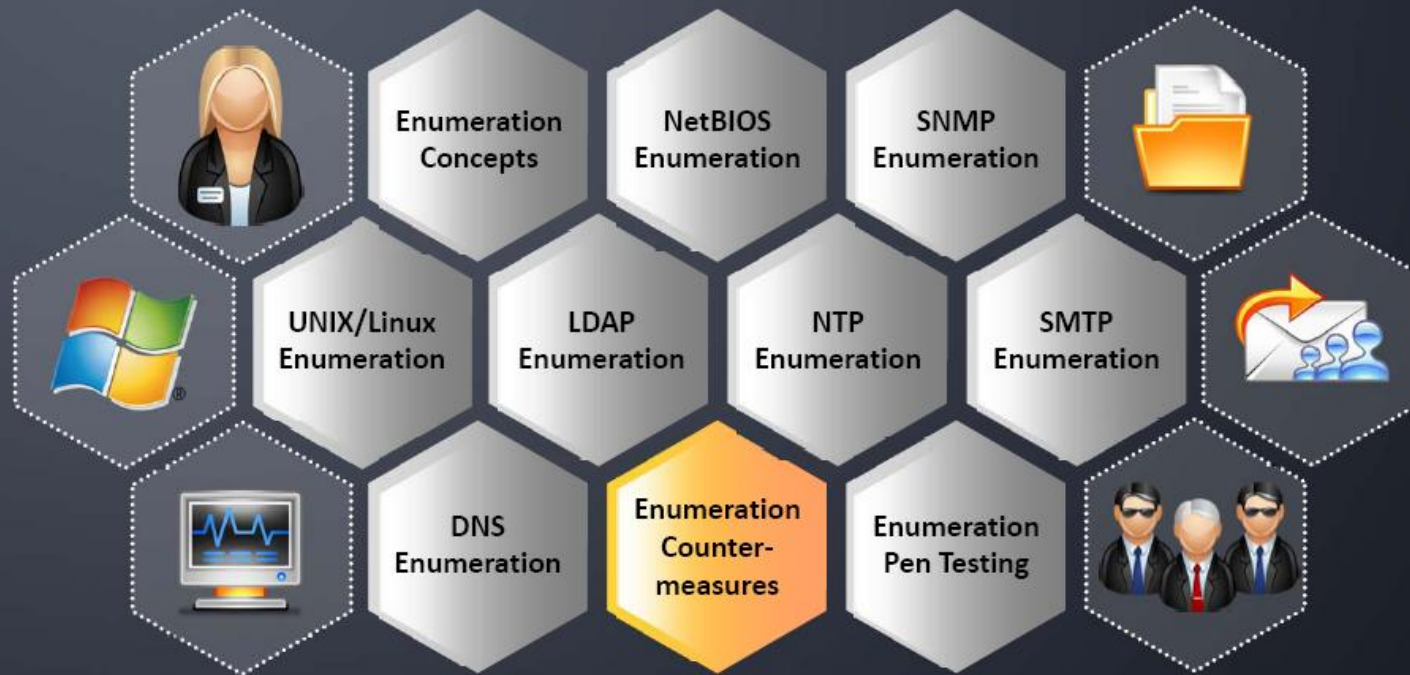
DNS Analyzing and Enumeration Tool: The Men & Mice Suite

- The Men & Mice Suite provides comprehensive DNS analysis and AD monitoring capabilities
- It performs over 80 different tests on the DNS configuration and **enumerates** and **reports** any issue that might affect the health of your DNS



<http://www.menandmice.com>

Module Flow





Enumeration Countermeasures

SNMP

- Remove the **SNMP agent** or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default **"public" community's name**
- Upgrade to **SNMP3**, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Access to null session pipes, null session shares, and IPSec filtering should also be restricted

DNS

- Configure all **name servers** to disallow the DNS zone transfers to the untrusted hosts
- Ensure that **nonpublic hostnames are not referenced to IP addresses** within the DNS zone files of publicly accessible DNS servers
- Ensure that HINFO and other records **do not appear in DNS zone files**
- Provide standard network administration contact details **in Network Information Center databases** to prevent social engineering and war dialing attacks



Enumeration Countermeasures

SMTP

- **Configure SMTP servers** either to ignore email messages to unknown recipients or to send responses that do not include these types of information:
 - Details of **mail relay systems** being used (such as Sendmail or MS Exchange)
 - **Internal IP address** or host information
- **Ignore emails to unknown recipients** by configuring SMTP servers

LDAP

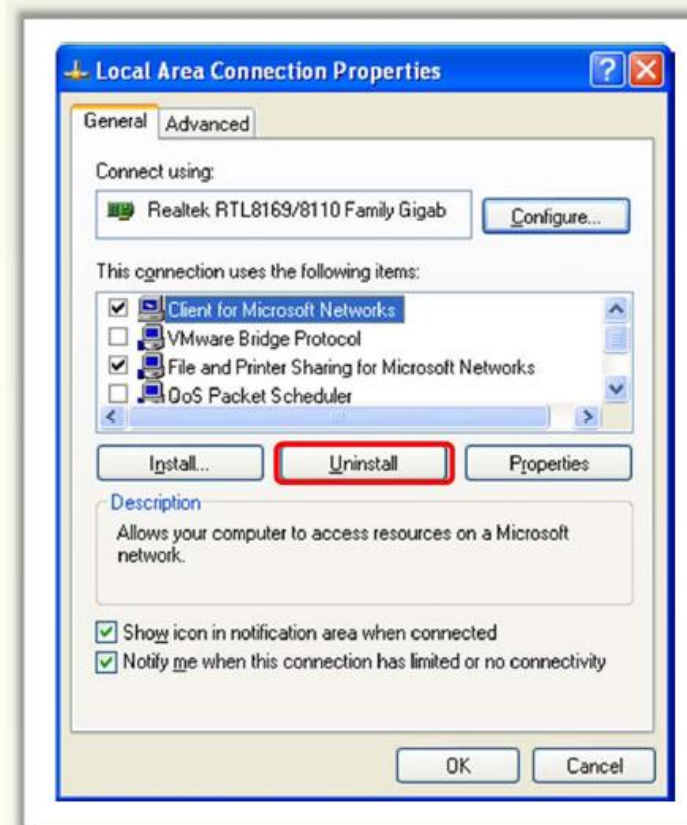
- **Use NTLM** or Basic authentication to limit access to known users only
- By default, LDAP traffic is transmitted unsecured; **use SSL technology** to encrypt the traffic
- Select a **username different** from your email address and enable **account lockout**



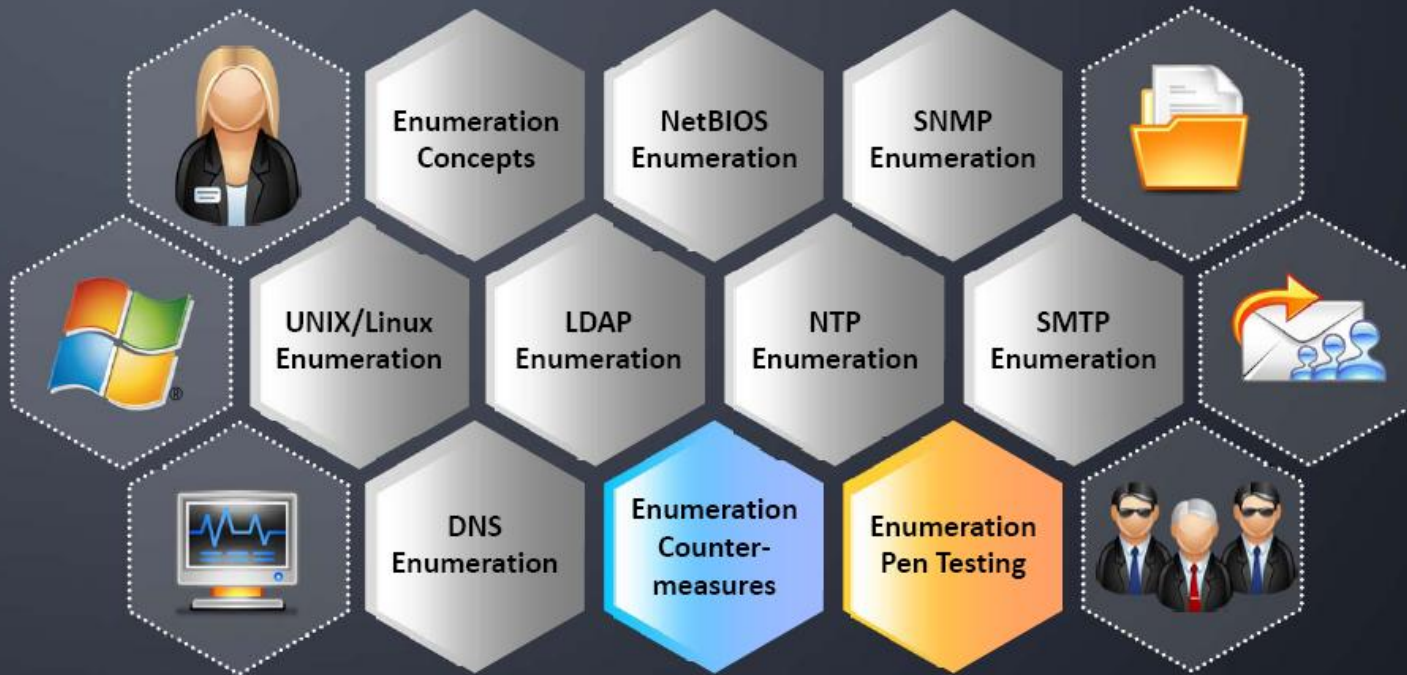
SMB Enumeration Countermeasures

Disabling SMB

- Go to **Local Area Connection Properties**
- Select the **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** check boxes, and click **Uninstall**
- Follow the uninstall steps



Module Flow

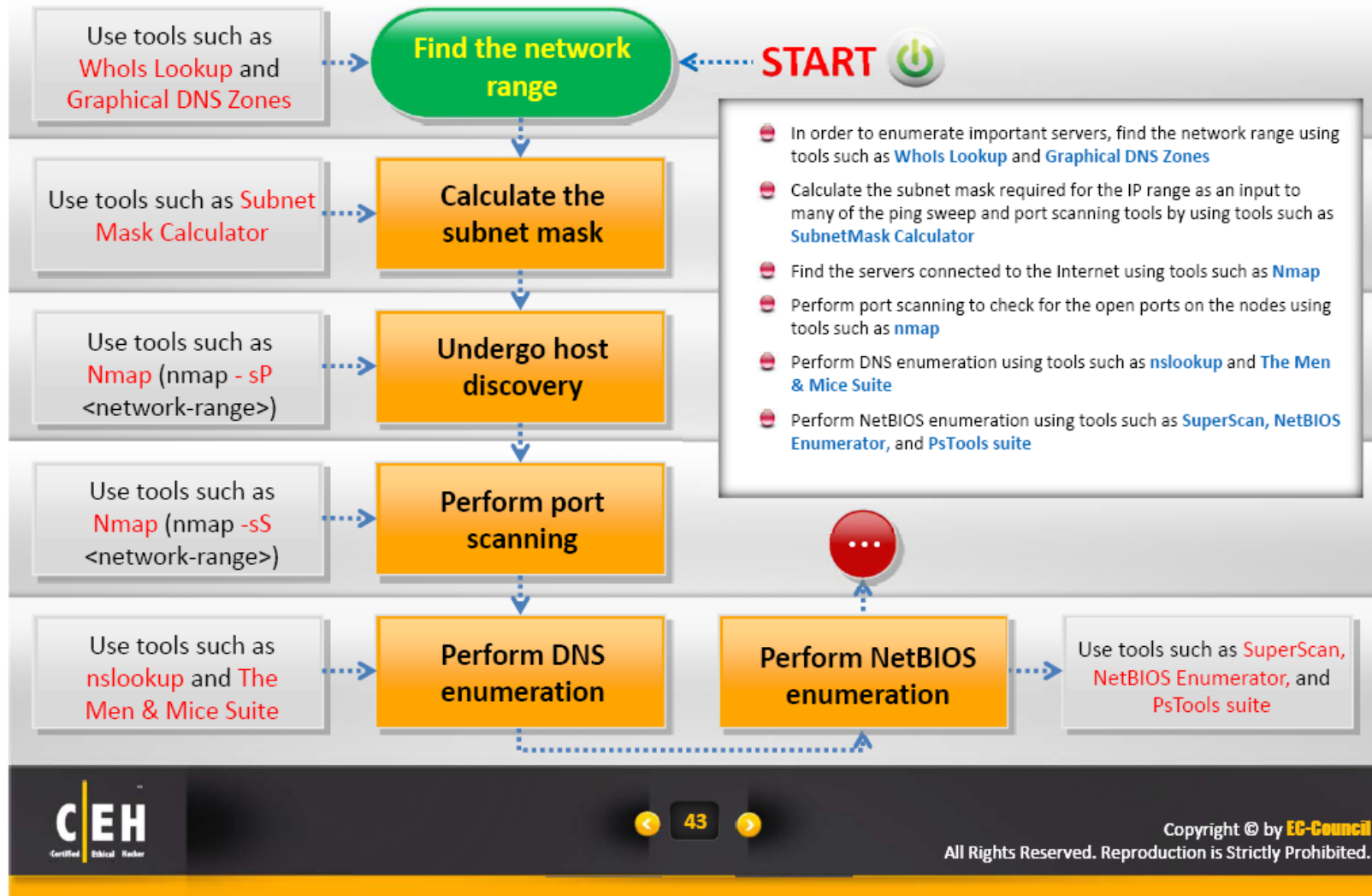


Enumeration **Pen Testing**

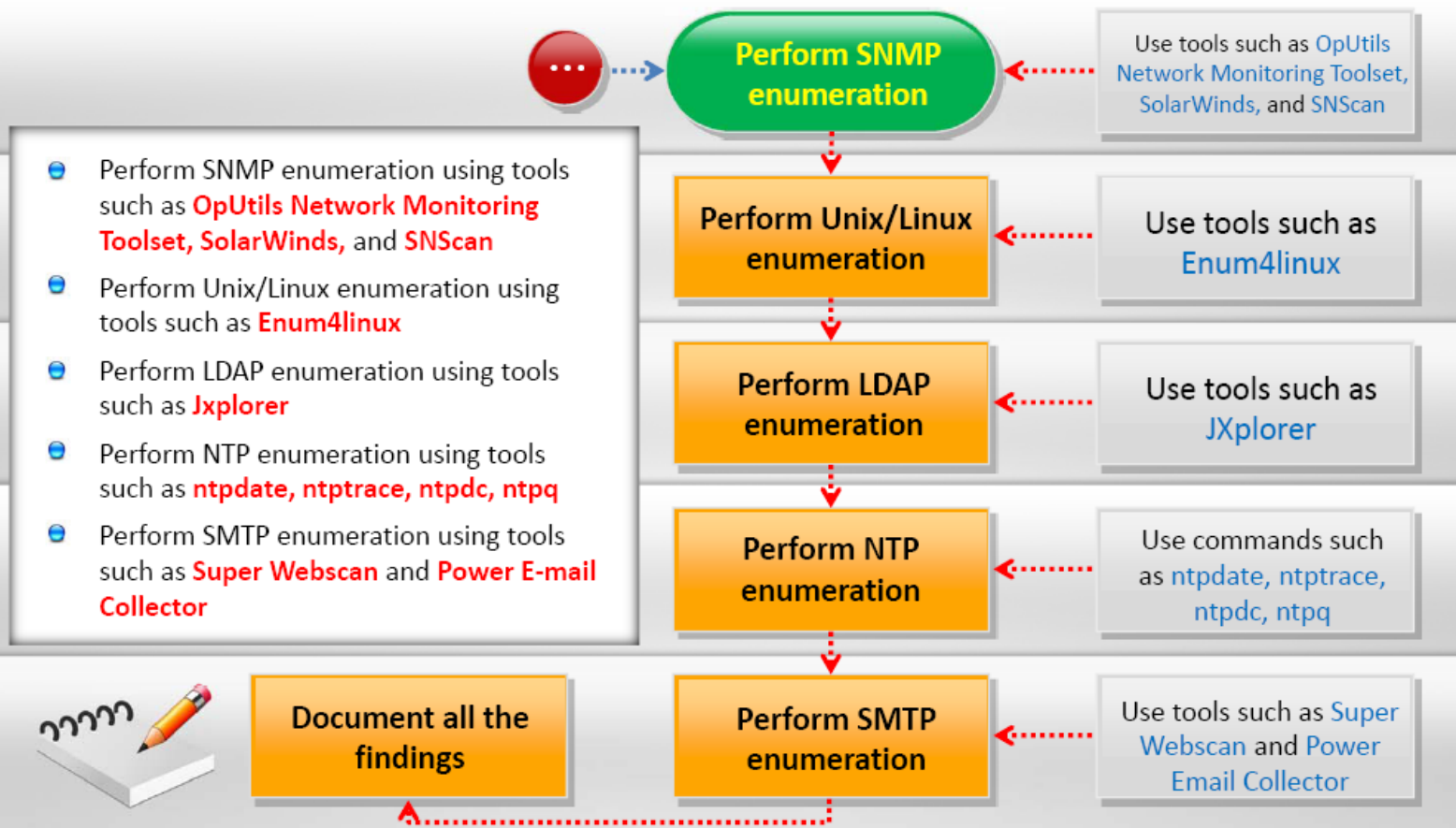
- It is to identify valid **user accounts** or **poorly-protected resource shares** using active connections to systems and directed queries. The information can be **users and groups, network resources and shares, and applications**
- It is used in combination with **data collected** in the **reconnaissance phase**



Enumeration Pen Testing



Enumeration Pen Testing



Module Summary



- Enumeration is defined as the process of extracting usernames, machine names, network resources, shares, and services from a system
- Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for remote monitoring and managing hosts, routers, and other devices on a network
- MIB provides a standard representation of the SNMP agent's available information and where it is stored
- The Lightweight Directory Access Protocol (LDAP) is a protocol used to access the directory listings within Active Directory or from other directory services
- Network Time Protocol (NTP) is designed to synchronize clocks of networked computers
- Devices like switches, hubs, and routers might still be enabled with a "default password"

Quotes

“The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.”

- **Eric Schmidt**,
Chairman and CEO,
Google