Enumeration
Module 4

Engineered by Hackers. Presented by Professionals.
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 1.8 million registered users were published to the web over the weekend. The blogs under the Gawker Media umbrella include Gizmodo, Deadspin, Kotaku, Jezebel, io9, 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 be ripped to shreds! You wanted attention, well guess what, You've got it now!

http://www.theatlanticwire.com
**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
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**.

Types of information Enumerated by intruders:

- Network resources and shares
- Users and groups
- Applications and banners
- Auditing settings
Techniques for Enumeration:

- Extract user names using email IDs
- Extract information using the default passwords
- Brute force Active Directory
- Extract information using DNS Zone Transfer
- Extract user names using SNMP
- Extract user groups from Windows
Netbios Enumeration

Attacks 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

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 53</td>
<td>DNS zone transfer</td>
</tr>
<tr>
<td>TCP 135</td>
<td>Microsoft RPC Endpoint Mapper</td>
</tr>
<tr>
<td>TCP 137</td>
<td>NetBIOS Name Service (NBNS)</td>
</tr>
<tr>
<td>UDP 139</td>
<td>NetBIOS Session Service (SMB over NetBIOS)</td>
</tr>
<tr>
<td>TCP 445</td>
<td>SMB over TCP (Direct Host)</td>
</tr>
<tr>
<td>UDP 161</td>
<td>Simple Network Management protocol (SNMP)</td>
</tr>
<tr>
<td>TCP/UDP 389</td>
<td>Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td>TCP/UDP 3368</td>
<td>Global Catalog Service</td>
</tr>
</tbody>
</table>
NetBIOS Enumeration Tool: SuperScan
NetBIOS Enumeration Tool: NetBIOS Enumerator

http://nbt_enum.sourceforge.net

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Enumerating User Accounts

- **PsExec**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsFile**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsGetSid**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsKill**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsInfo**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsList**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsLoggedOn**
  - [http://technet.microsoft.com](http://technet.microsoft.com)

- **PsLogList**
  - [http://technet.microsoft.com](http://technet.microsoft.com)
Enumerate Systems Using Default Passwords

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

http://www.defaultpassword.com

Password

ABCDEFGHIJKLMNOPQRSTUVWXYZ
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

![Screenshot of the OpUtils tool interface](http://www.manageengine.com)

### Select Criteria
- **Date**
- **User**
- **Action Performed**
- **Changes in**
- **Description**

<table>
<thead>
<tr>
<th>Date</th>
<th>User</th>
<th>Action Performed</th>
<th>Changes in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>Others</td>
<td>Scheduler has been enabled</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>Default Group</td>
<td>Scheduler has been enabled for the group is Default Group</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>cisco2001</td>
<td>cisco2001 has been manually added to the routers list with SNMP community string</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>192.168.117.1</td>
<td>Physical location has been changed from [Not Defined] to test21 for port 22</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>192.168.117.1</td>
<td>Physical location has been changed from [Not Defined] to test2 for port 23</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>3com4400</td>
<td>3com4400 has been modified</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>192.168.117.1</td>
<td>Added switch 192.168.117.1 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>foundry2402</td>
<td>Added switch foundry2402 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>procurev2524</td>
<td>Added switch procurev2524 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>oputils-w2k2</td>
<td>Added switch oputils-w2k2 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>3com4400</td>
<td>Added switch 3com4400 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>cisco2011</td>
<td>Added switch cisco2011 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>cisco2001</td>
<td>Added switch cisco2001 manually to Default Group with ping sweep false</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>admin</td>
<td>Modify</td>
<td>catalyst2900</td>
<td>Added switch catalyst2900 manually to Default Group with ping sweep false</td>
</tr>
</tbody>
</table>

© 2004-2009 ZOHO Corp.

http://www.manageengine.com

All Rights Reserved. Reproduction is Strictly Prohibited.
SNMP Enumeration Tool: **SolarWinds**
SNMP Enumeration Tools

- Getif SNMP MIB Browser
  - http://www.wtcs.org

- OidView SNMP MIB Browser
  - http://www.oidview.com

- iReasoning MIB Browser
  - http://tl1.ireasoning.com

- SNScan
  - http://www.foundstone.com

- LoriotPro
  - http://www.loriotpro.com

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

- Nsauditor Network Security Auditor
  - http://www.nsauditor.com

- SoftPerfect Network Scanner
  - http://www.softperfect.com
Module Flow

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing
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

**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) ----- 
[?] Assuming that user "administrator" exists
[+] Got SID: 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

http://labs.portcullis.co.uk

Linux Enumeration Tool: Enum4linux
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 confirm to a distinct set of rules. Request for comments (RFC's) like other protocols.
LDAP Enumeration Tool: **JXplorer**

![JXplorer LDAP Enumeration Tool](image)

http://www.jxplorer.org
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
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 Commands:
- ntpd
- ntpq
- ntptrace
- ntpdc
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.

![NTP Server Scanner](ntpscan)

http://www.bytefusion.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
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.

http://www.bytefusion.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
NTP Enumeration Tools

- **PresenTense Time Client**
  - [http://www.bytefusion.com](http://www.bytefusion.com)

- **LAN Time Analyser**
  - [http://www.bytefusion.com](http://www.bytefusion.com)

- **NTP Server Checker**
  - [http://www.galsys.co.uk](http://www.galsys.co.uk)

- **Time Watch**
  - [http://www.blue-series.com](http://www.blue-series.com)

- **PresenTense NTP Auditor**
  - [http://www.bytefusion.com](http://www.bytefusion.com)

- **NTP Time Server Monitor**
  - [http://www.meinberg.de](http://www.meinberg.de)

- **NTP Time Server Monitor**
  - [http://www.meinberg.de](http://www.meinberg.de)

- **AtomSync**
  - [http://www.emtei.com](http://www.emtei.com)
Module Flow

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
SMTP Enumeration

Attackers can directly interact with SMTP via the telnet 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>
VRFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VRFY ORACLE
550 ORACLE... User unknown
QUIT
```
SMTP Enumeration Tool: NetScanTools Pro

NetScanTools 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.
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

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Module Flow

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- UNIX/Linux Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP Enumeration
- DNS Enumeration
- Enumeration Countermeasures
- Enumeration Pen Testing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
**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 SNMPv3**, 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
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**

1. **Find the network range**
   - Use tools such as **Whols Lookup** and **Graphical DNS Zones**

2. **Calculate the subnet mask**
   - Use tools such as **Subnet Mask Calculator**

3. **Undergo host discovery**
   - Use tools such as **Nmap** (nmap -sP <network-range>)

4. **Perform port scanning**
   - Use tools such as **Nmap** (nmap -sS <network-range>)
   - Use tools such as **nslookup** and **The Men & Mice Suite**

5. **Perform DNS enumeration**
   - Use tools such as **nslookup and The Men & Mice Suite**

6. **Perform NetBIOS enumeration**
   - Use tools such as **SuperScan, NetBIOS Enumerator, and PsTools suite**

**Steps:**
- In order to enumerate important servers, find the network range using tools such as **Whols Lookup** and **Graphical DNS Zones**
- Calculate the subnet mask required for the IP range as an input to many of the ping sweep and port scanning tools by using tools such as **SubnetMask Calculator**
- Find the servers connected to the Internet using tools such as **Nmap**
- Perform port scanning to check for the open ports on the nodes using tools such as **nmap**
- Perform DNS enumeration using tools such as **nslookup** and **The Men & Mice Suite**
- Perform NetBIOS enumeration using tools such as **SuperScan, NetBIOS Enumerator, and PsTools suite**

**Copyright © by EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.
Enumeration Pen Testing

Perform SNMP enumeration using tools such as OpUtils Network Monitoring Toolset, SolarWinds, and SNScan
Perform Unix/Linux enumeration using tools such as Enum4Linux
Perform LDAP enumeration using tools such as JXplorer
Perform NTP enumeration using tools such as ntpdate, ntptrace, ntpdc, ntpq
Perform SMTP enumeration using tools such as Super Webscan and Power E-mail Collector

Use tools such as OpUtils Network Monitoring Toolset, SolarWinds, and SNScan
Use tools such as Enum4Linux
Use tools such as JXplorer
Use commands such as ntpdate, ntptrace, ntpdc, ntpq
Use tools such as Super Webscan and Power E-mail Collector

Document all the findings
Perform SMTP enumeration
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.”
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