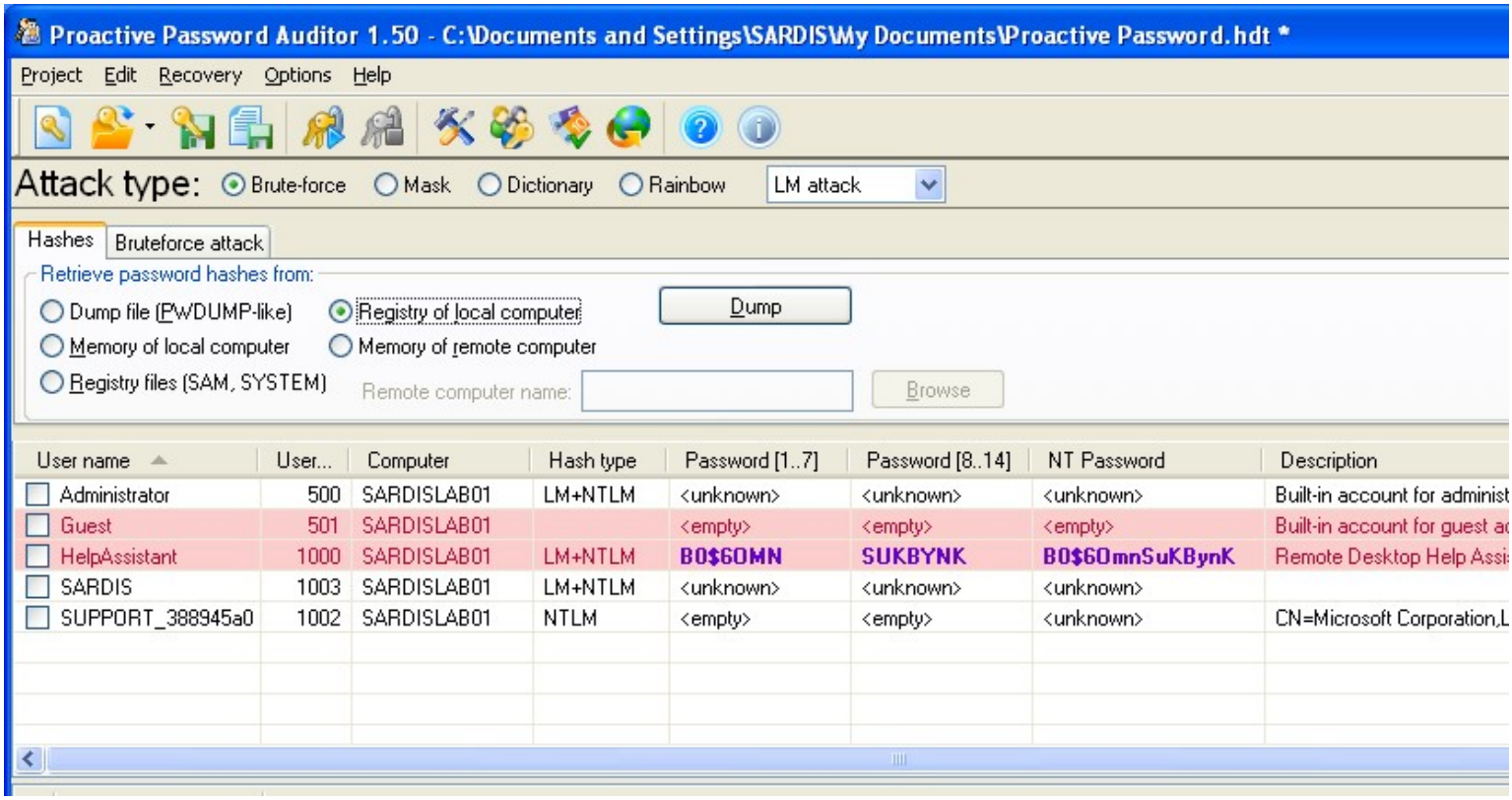
**Tool 1 – Password Integrity Verification Tool**
Proactive Password Auditor
http://www.elcomsoft.com/download/ppa.zip
Do a Memory Dump of the Local Computer
Crack some of the immediate passwords, notice the speed, and screen capture after completion



**Tool 2 – Network Enumeration/Discovery**

Whois, Nslookup, Tracert, & Dig

A) Whois via a Web Browser of some web site
B) Nslookup using native Windows XP
C) Tracert using native Windows XP
D) Dig using Roadkil's v1.1 –
E) Ipconfig /all

Screen capture of all four

Consider how these tools may allow enumeration of the network being probed, consider how ICMP is used and how it may be mitigated in key places like firewalls

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\SARDIS>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : sardislab01
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : dhcp.scis.nova.edu

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dhcp.scis.nova.edu
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-11-43-9F-B4-C2
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 137.52.55.30
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 137.52.55.1
        DHCP Server . . . . . . . . . . . : 137.52.128.11
        DNS Servers . . . . . . . . . . . : 137.52.128.11
        Primary WINS Server . . . . . . . : 137.52.128.12
        Secondary WINS Server . . . . . . : 137.52.128.13
        Lease Obtained. . . . . . . . . . : Thursday, July 14, 2005 12:36:58 PM
        Lease Expires . . . . . . . . . . : Monday, July 18, 2005 12:36:58 PM

C:\Documents and Settings\SARDIS>
```

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: sedlack.com

   Created on..............: 15 Apr 1999 10:00:00
   Expires on..............: 15 Apr 2011 10:00:00

Registrant Info:
   Derek J. Sedlack
   Derek Sedlack
   1007 Wilderness Path
   Round Rock, TX 78664
   US
   Phone:
   Fax..:
   Email: dom-admin@OZNIC.COM

Administrative Info:
   sedlack.com
   Derek Sedlack
   1007 Wilderness Path
   Roundrock, TX 78664-2505
   US
   Phone: 512-244-2331
   Fax..: 512-244-2331
   Email: derek@sedlack.com

Technical Info:
   Domainhost Intl.
   Michael Philopulous
   1139 S. Sunnyslope Dr. Suite 202
   Racine, WI 53406
   US
   Phone: 262-886-3121
   Fax..: 262-886-3121
   Email: support@domainhost.com
Billing Info:
   sedlack.com
   Derek Sedlack
   1007 Wilderness Path
   Roundrock, TX 78664-2505
   US
   Phone: 512-244-2331
   Fax..: 512-244-2331
   Email: derek@sedlack.com

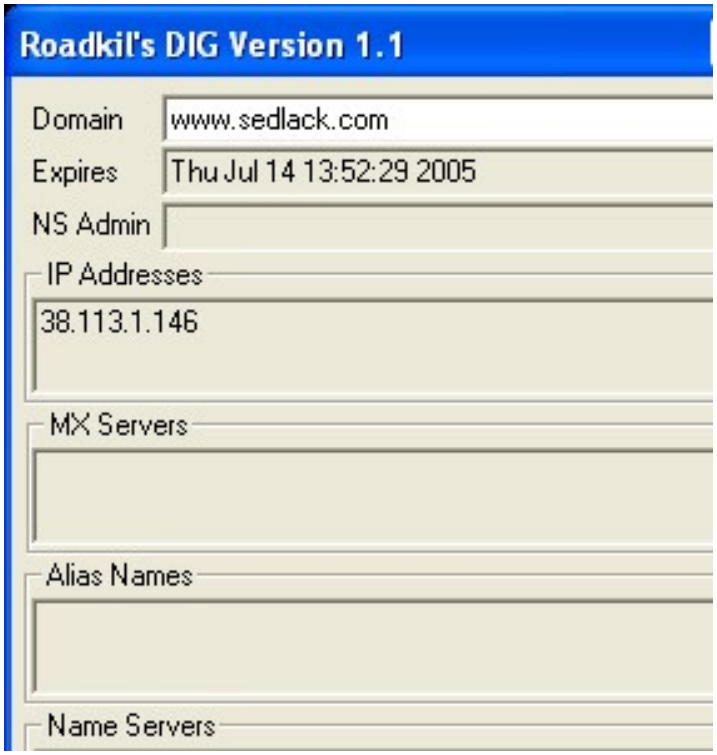
Status: Locked

Domain servers in listed order:

    ns1.domainhost.com.
    ns2.domainhost.com.

```
C:\Documents and Settings\SARDIS>nslookup www.sedlack.com
Server:  ns1.nunet.nova.edu
Address:  137.52.128.11

Non-authoritative answer:
Name:    www.sedlack.com
Address:  38.113.1.146
```

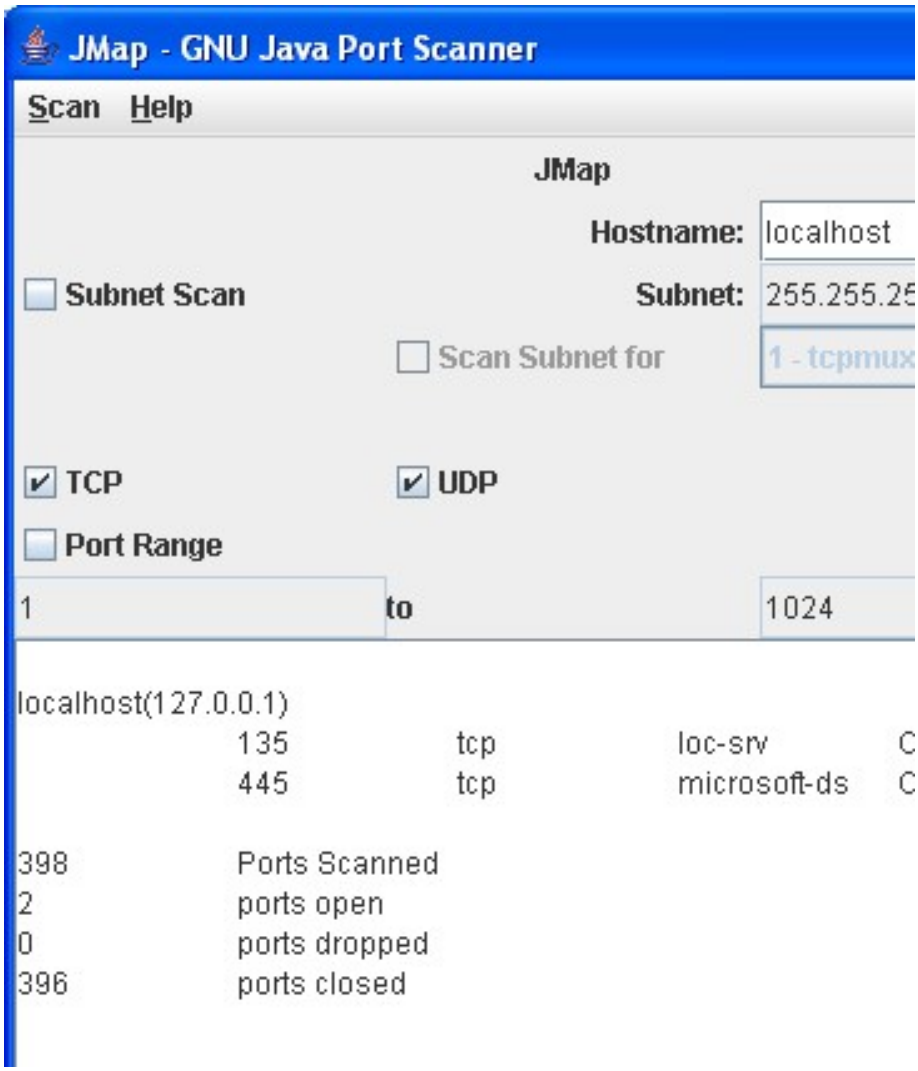
```
C:\Documents and Settings\SARDIS>tracert www.sedlack.com

Tracing route to www.sedlack.com [38.113.1.146]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  ssr-55.scis.nova.edu [137.52.55.1]
  2     1 ms    <1 ms    <1 ms  mh-core-b.nunet.nova.edu [10.207.0.1]
  3     5 ms     4 ms     4 ms  orl-flrcore-7609-1-te31-1834.net.flrnet.org [198.32.155.153]
  4     9 ms     9 ms     9 ms  florida_lambdarail_llc.demarc.cogentco.com [38.112.31.66]
  5    10 ms     9 ms     9 ms  g0-5.na21.b006657-0.mia01.atlas.cogentco.com [38.112.31.65]
  6     9 ms     9 ms     9 ms  g4-1-101.core01.mia01.atlas.cogentco.com [38.112.37.53]
  7    24 ms    23 ms    23 ms  p5-0.core01.atl01.atlas.cogentco.com [66.28.4.138]
  8    35 ms    35 ms    35 ms  p5-0.core02.dca01.atlas.cogentco.com [66.28.4.162]
  9    41 ms    41 ms    40 ms  p6-0.core01.jfk02.atlas.cogentco.com [66.28.4.82]
 10    46 ms    45 ms    45 ms  p5-0.core01.bos01.atlas.cogentco.com [66.28.4.117]
 11    47 ms    46 ms    46 ms  g7.ba21.b006523-1.bos01.atlas.cogentco.com [66.28.65.70]
 12    46 ms    46 ms    46 ms
EnduranceInternationalGroup.demarc.cogentco.com[38.112.14.62]
 13    47 ms    47 ms    46 ms  ip38-113-1-146.yourhostingaccount.com [38.113.1.146]

Trace complete.

C:\Documents and Settings\SARDIS>
```


Roadkil's DIG Version 1.1
Domain
www.sedlack.com
Expires
Thu Jul 14 13:52:29 2005
NS Admin
IP Addresses
38.113.1.146
MX Servers
Alias Names
Name Servers

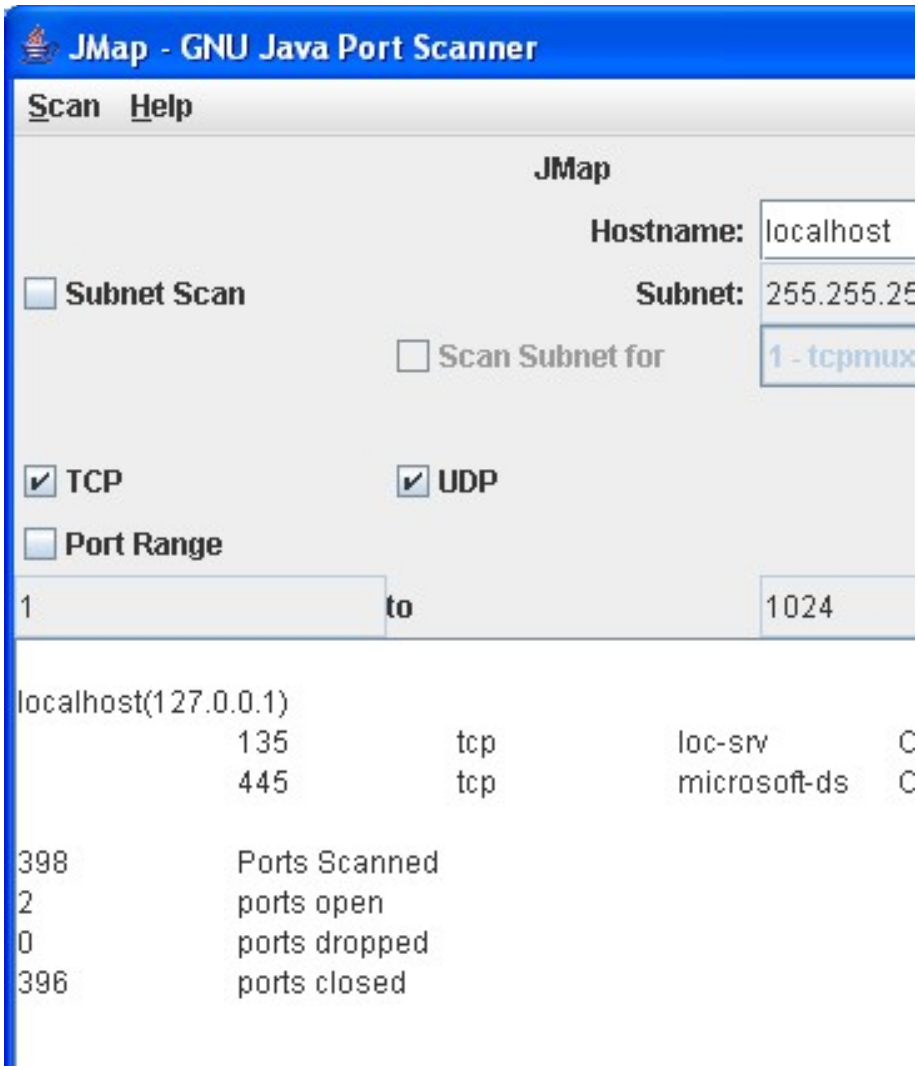
**Tool 3 – Port/Service/Operating System Discovery**
NMAP (Network Mapper)
You need the WinPcap Utility and the NMAP Tool for this to work
http://download.insecure.org/nmap/dist/nmap-3.81-win32.zip
http://www.winpcap.org/install/bin/WinPcap_3_1_beta4.exe
Run a stealth scan and operating system scan to guess OS of localhost (nmap –sS –O XXX.XXX.XXX.XXX)
Do this with and without XP SP2 Firewall (disable in Control Panel), capture screen shot of with and without Firewall, note the differences.

http://slashtom.org/Software/index.php?package=jmap

**Firewall On**




**Firewall On**

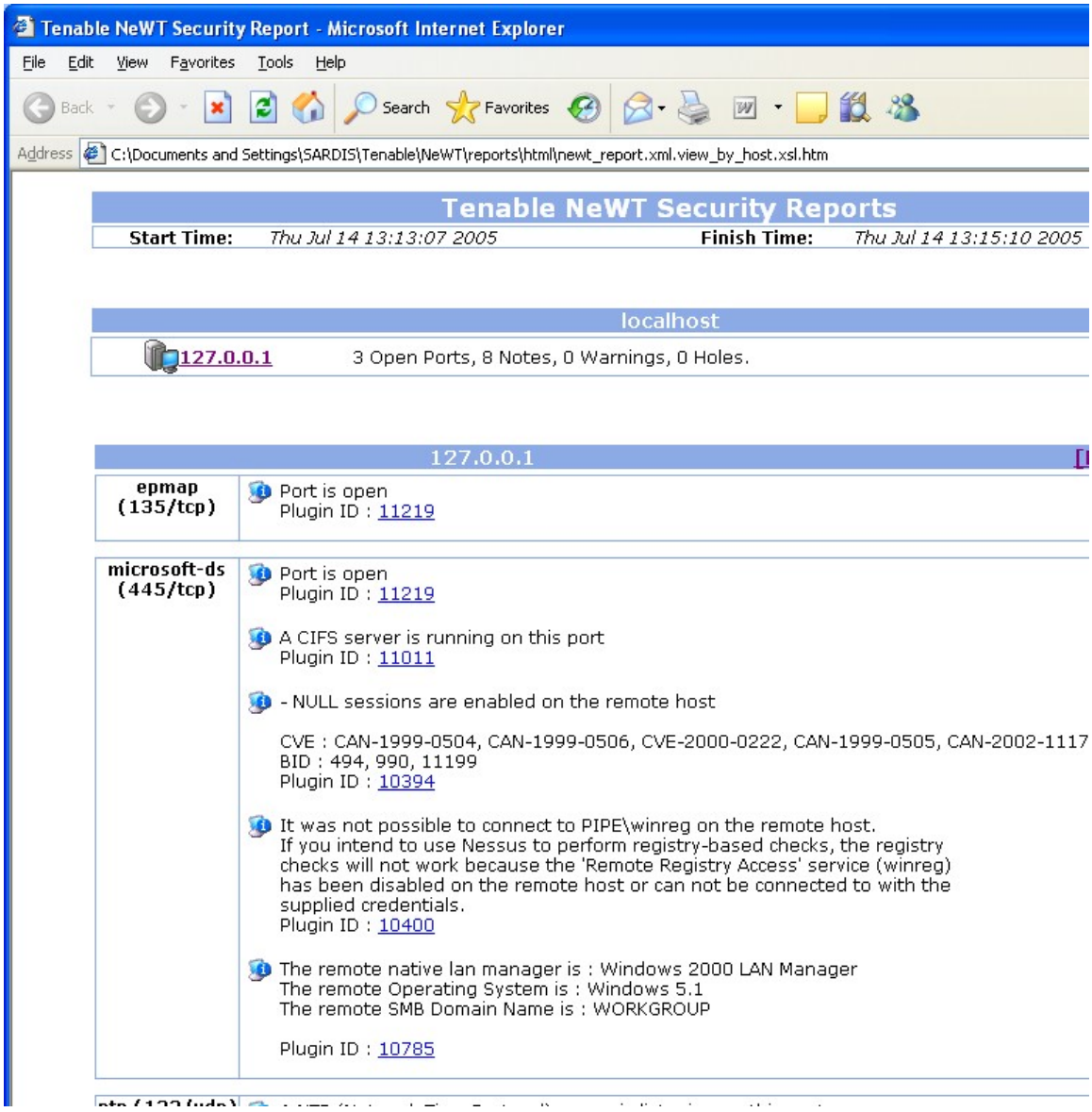

JMap - GNU Java Port Scanner
Scan Help
JMap
Hostname: localhost
Subnet Scan
Subnet: 255.255.25
Scan Subnet for
1 - tcpmux
TCP
UDP
Port Range
1
to
1024
localhost(127.0.0.1)
135 tcp loc-srv C
445 tcp microsoft-ds C
398 Ports Scanned
2 ports open
0 ports dropped
396 ports closed

**Tool 4 – Vulnerability Assessment Tool**
NeWT (Nessus Windows Technology)
http://cgi.tenablesecurity.com/tenable/dl.php?p=TenableNeWT-2.2-Setup.exe&x=f23e442d
You may have to register and download your own tool
Here is your plugin activation code: E32B-1174-C4FD-89C0-753F
The above code will be needed to update plugins.
Run a scan with all but dangerous plug-ins of the localhost
Do this with and without XP SP2 Firewall (disable in Control Panel), capture screen shot of with and without Firewall, note the differences.

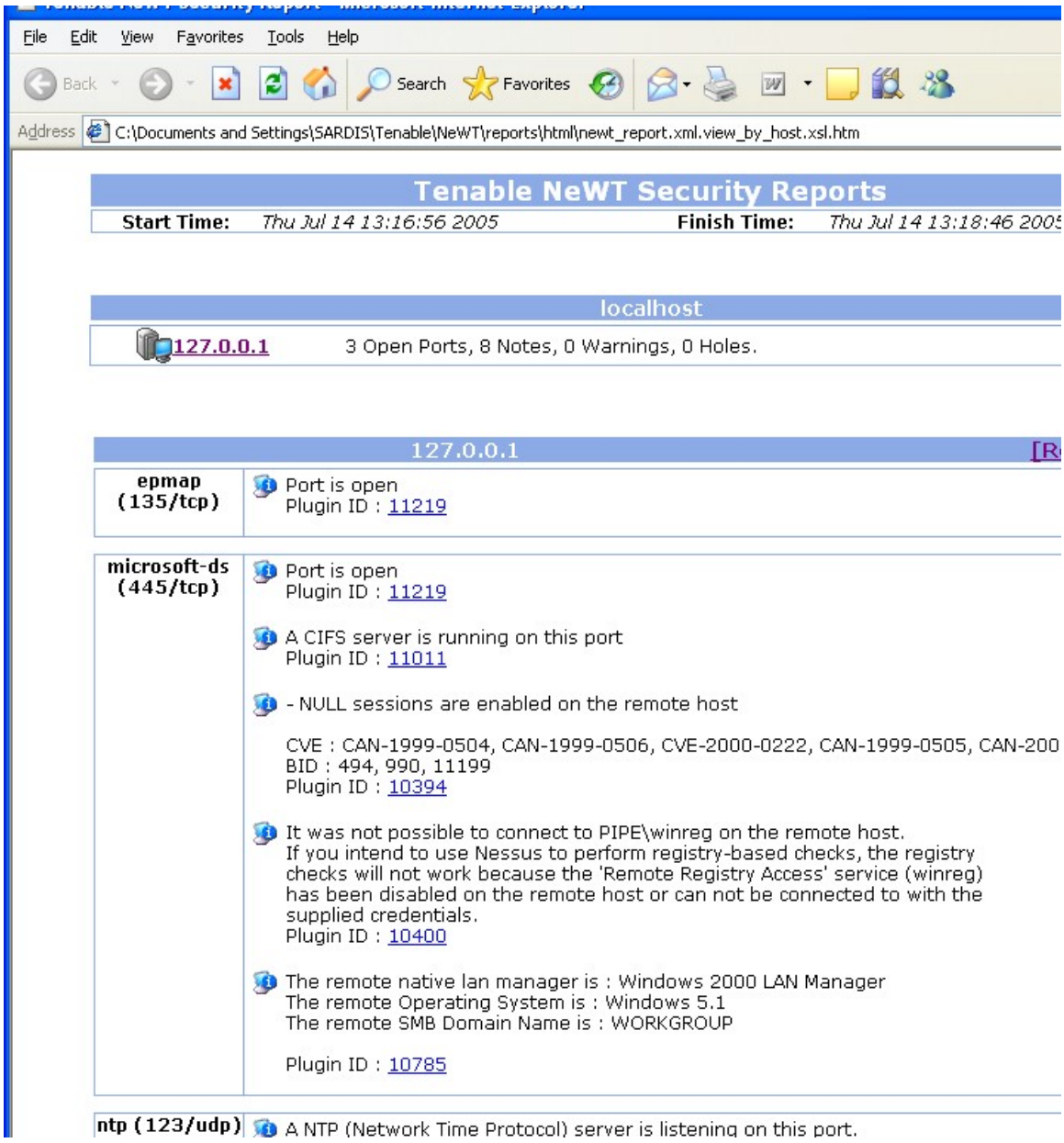
**Using IP Saved on Disk**

**Using localhost for address**

**Firewall On**



## Firewall Off



**Tool 5 – Network Protocol Analyzer (Sniffer)**
Ethereal 0.10.11
http://www.ethereal.com/distribution/win32/
Requires WinPcap 3.1 beta4 to work (also at the same link above)
Capture about a hundred packets, do a save as to a **file name of your choice** and look at it later on your own system. (Later practice sorting and filtering on same kind of protocols).
At you leisure after you leave the campus, monitor an Ethereal session where you access one of you web mail accounts via SSL and without SSL – note that the payload in SSL is not readable due to encryption).

**Saved to Disk**

**Tool 6 – Hashing Tool – (Basic Component of File Integrity Tools (like Tripwire & AIDE); also supports forensic examination** MD5 Deep v1.7
http://md5deep.sourceforge.net/
Perform a recursive hashing using the MD5 utility of the ZIP file with an easily modifiable file Word, Excel, do a screen capture
Modify a file, do a screen capture and note the difference

**Before Modify**

```
C:\Documents and Settings\SARDIS\Desktop\SCIS Tools\MD5>md5deep -r files
d05ab88927849df74cf4f1c303daeb4f  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\adptif.dll
1c4f086dc41818d79d16413ea1db5705  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\adsldp.dll
d41d8cd98f00b204e9800998ecf8427e  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\AUTOEXEC.BAT
6ec547186032cefa696bfe80b1d01672  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\DISS799.doc

C:\Documents and Settings\SARDIS\Desktop\SCIS Tools\MD5>
```

**After Modify Autoexec and DISS799**

```
C:\Documents and Settings\SARDIS\Desktop\SCIS Tools\MD5>md5deep -r files
d05ab88927849df74cf4f1c303daeb4f  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\adptif.dll
1c4f086dc41818d79d16413ea1db5705  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\adsldp.dll
2e6b1609a55a57fe4a75eff6cba3b8d7  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\AUTOEXEC.BAT
b6d5ecada1b0061090b6dd747e7cc5c3  C:\Documents and Settings\SARDIS\Desktop\SCIS
Tools\MD5\files\DISS799.doc

C:\Documents and Settings\SARDIS\Desktop\SCIS Tools\MD5>
```

**Tool 7 – Operating System Baselining**
MBSA Benchmark Security Tools for Windows Assessment (MBSA) & Microsoft Management Console (MMC)
MBSA – http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx
MM Cis native to Windows
Complete the scan and email yourself a copy of the file (*.MBSA file) , i.e. C:\Documents and Settings\jcarroll\SecurityScans\ -> review at a later date with another system with MBSA later
MMC is opened from a DOS window using the command MMC, Add Snap-ins for Security Configuration & Analysis AND Security Templates, Right Click Security Configuration & Analysis and Select Open, Right Click Open Databases and create a file of your naming and select "securews.inf" as the reference *.INF -> Do an "Analyze Computer Now", do a File Save As to "Console13JUL05.msc" to the **desktop** and email to yourself for later review (approx. 40K file). Analyze the delta at a later date and see what is different?

C:\Documents and Settings\SARDIS\SecurityScans

| | |
|---|---|
| Computer name: | WORKGROUP\SARDISLAB01 |
| IP address: | 137.52.55.30 |
| Security report name: | WORKGROUP - SARDISLAB01 (7-14-2005 1-33 PM) |
| Scan date: | 7/14/2005 1:33 PM |
| Catalog synchronization date: | |
| Security update catalog: | Microsoft Update |
| Security assessment: | Potential Risk |

Security Updates

| Score | Issue | Result |
|---|---|---|
|  | Windows Security Updates | 1 service packs or update rollups are missing. |

**Update Rollups and Service Packs**

| Score | ID | Description |
|---|---|---|
| Missing | 890830 | Windows Malicious Software Removal Tool - July 2005 (KB890830) |

**Current Update Compliance**

| Score | ID | Description | Maximum Severity |
|---|---|---|---|
| Installed | MS04-043 | Security Update for Windows | Important |

| | | | |
|---|---|---|---|
| | | XP (KB873339) | |
| Installed | MS04-041 | Security Update for Windows XP (KB885836) | Important |
| Installed | MS05-001 | Security Update for Windows XP (KB890175) | Critical |
| Installed | MS05-007 | Security Update for Windows XP (KB888302) | Important |
| Installed | MS05-009 | Security Update for Windows Messenger (KB887472) | Moderate |
| Installed | MS05-013 | Security Update for Windows XP (KB891781) | Important |
| Installed | MS05-015 | Security Update for Windows XP (KB888113) | Important |
| Installed | MS05-012 | Security Update for Windows XP (KB873333) | Important |
| Installed | MS05-016 | Security Update for Windows XP (KB893086) | Important |
| Installed | MS05-018 | Security Update for Windows XP (KB890859) | Important |
| Installed | MS04-044 | Security Update for Windows XP (KB885835) | Important |
| Installed | MS05-011 | Security Update for Windows XP (KB885250) | Critical |
| Installed | MS05-026 | Security Update for Windows XP (KB896358) | Critical |
| Installed | MS05-032 | Security Update for Windows XP (KB890046) | Moderate |
| Installed | MS05-027 | Security Update for Windows XP (KB896422) | Critical |
| Installed | MS05-033 | Security Update for Windows XP (KB896428) | Moderate |
| Installed | MS05-025 | Cumulative Security Update for Internet Explorer for Windows XP Service Pack 2 (KB883939) | Important |
| Installed | MS05-019 | Security Update for Windows XP (KB893066) | Critical |
| Installed | 890830 | Windows Malicious Software Removal Tool - June 2005 (KB890830) | |

| | | | | |
|---|---|---|---|---|
| | | Installed | MS05-037 | Security Update for JView Profiler (KB903235) | Critical |
| | | Installed | MS05-036 | Security Update for Windows XP (KB901214) | Critical |
| ✔ | Office Security Updates | No security updates are missing. | | | |
| | | **Current Update Compliance** | | | |
| | | Score | ID | Description | Maximum Severity |
| | | Installed | 842532 | Office 2003 Service Pack 1 | |
| | | Installed | MS05-023 | Security Update for Word 2003 (KB887979) | Critical |

Windows Scan Results

Administrative Vulnerabilities

| Score | Issue | Result |
|---|---|---|
| ✱ | Windows Firewall | Windows Firewall is enabled and has exceptions configured.<br>Windows Firewall is enabled on all network connections. |
| | | Connection Name: All Connections — Firewall: On — Exceptions: Programs |
| | | Connection Name: Local Area Connection — Firewall: On — Exceptions: Programs* |
| ✱ | Incomplete Updates | No incomplete software update installations were found. |
| ✔ | Local Account Password Test | No user accounts have simple passwords. |
| | | User: Guest — Weak Password: - — Locked Out: - — Disabled |
| | | User: HelpAssistant — Weak Password: - — Locked Out: - — Disabled |
| | | User: SUPPORT_388945a0 — Weak Password: - — Locked Out: - — Disabled |
| | | User: Administrator — Weak Password: - — Locked Out: - — Disabled: - |
| | | User: SARDIS — Weak Password: - — Locked Out: - — Disabled: - |

| | | |
|---|---|---|
| ✔ | File System | All hard drives (1) are using the NTFS file system.<br>Drive Letter: C:<br>File System: NTFS |
| ✔ | Guest Account | The Guest account is disabled on this computer. |
| ✔ | Restrict Anonymous | Computer is properly restricting anonymous access. |
| ✔ | Administrators | No more than 2 Administrators were found on this computer.<br>User<br>Administrator<br>SARDIS |
| ✔ | Automatic Updates | Updates are automatically downloaded and installed on this computer. |
| | Password Expiration | This check was skipped because the computer is not joined to a domain. |
| | Autologon | This check was skipped because the computer is not joined to a domain. |

Additional System Information

| Score | Issue | Result |
|---|---|---|
| ℹ | Windows Version | Computer is running Windows 2000 or greater. |
| ✱ | Auditing | This check was skipped because the computer is not joined to a domain. |
| ℹ | Shares | 2 share(s) are present on your computer.<br>Share: Directory: Share ACL: Directory ACL |

| | | | | |
|---|---|---|---|---|
| | ADMIN$ | C:\WINDOWS | Admin Share | BUILTIN\Users - RX, BUILTIN\Power Users - RWXD, BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F |
| | C$ | C:\ | Admin Share | BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, BUILTIN\Users - RX, Everyone - RX |

Services — Some potentially unnecessary services are installed.

| Service | State |
|---|---|
| Telnet | Stopped |

Internet Information Services (IIS) Scan Results

| Score | Issue | Result |
|---|---|---|
| | IIS Status | IIS is not running on this computer. |

SQL Server Scan Results

| Score | Issue | Result |
|---|---|---|
| | SQL Server/MSDE Status | SQL Server and/or MSDE is not installed on this computer. |

Desktop Application Scan Results

Administrative Vulnerabilities

| Score | Issue | Result |
|---|---|---|
| ✓ | IE Zones | Internet Explorer zones have secure settings for all users. |
| ✓ | Macro Security | 4 Microsoft Office product(s) are installed. No issues were found. |

| Issue | User | Advice |
|---|---|---|

| | | | |
|---|---|---|---|
| | Microsoft Office Excel 2003 | All Users | No security issues were found. |
| | Microsoft Office Outlook 2003 | All Users | No security issues were found. |
| | Microsoft Office PowerPoint 2003 | All Users | No security issues were found. |
| | Microsoft Office Word 2003 | All Users | No security issues were found. |

**Tool 8 – NetBIOS over TCP Vulnerability Assessment**
Essential Net Tools
Download the **Essential NetTools 4.0** Build 158 Tool and Use the "NetAudit Feature"
http://www.tamos.com/download/main/
Do a Save As to HTML, look at at a later date

**Saved to Disk**

**Tool 9 – User Rights/Privilege Assessment**
Somersoft DumpSec (formerly DumpACL)
Do a **Dump Users to Table**, create a screenshot like what is shown on the slides, do a Save As to DumpSec13JUL05 in DumpSec native format for later viewing
Do a **Dump Rights**, create a screenshot like what is shown on the slides, do a Save As to DumpSec13JUL05 in DumpSec native format for later viewing

**Saved to Disk**