GIAC Enterprise

Vulnerability Assessment

Fritschie Security Services

January 1, 2001

Table of Contents

Executive Summary

For the scope of this review two servers in GIAC's network were examined. The scope of this assessment was to examine the unix portion of GIAC's network. GIAC is primarily a Windows NT based network, however, they are considering implementing additional unix based servers. The two servers selected to be examined were a domain name server (DNS) running Red Hat 6.1 and an application/web server running Solaris 2.6. Vulnerability assessment tools were run against the two servers from an internal perspective to gain an understanding of the vulnerabilities that exist. It is suggested that an additional vulnerability assessment is conducted from an external perspective to see what vulnerabilities might exist and be seen by an attacker without internal access to the servers.

The running of the vulnerability assessment tools and the interviews with the network staff of GIAC Enterprise took place on December 27th and December 28th. After analyzing the results from the scans it is apparent that both of the servers that were examined are vulnerable to attacks that could lead to a total and complete compromise of the network. Once these machines had been compromised it is possible that the entire GIAC network could also be compromised.

Both of the servers had unnecessary services and applications running on them. In addition the recommended patches and hot-fixes had not been applied. Lastly, there were no backup procedures in place, no documented disaster recovery plan or procedure in place in the event of a suspected network compromise, and the password policy was not adequate. Complete details of vulnerabilities can be found in the section entitled "Detailed Vulnerability Assessment".

It is recommended that both of these servers are hardened and the correct patches applied to eliminate the vulnerabilities that were found. It is also suggested that other servers in GIAC's network are examined to determine if similar vulnerabilities exist. In addition there should be documented disaster recovery plans, password policy, backup procedures, etc… Complete details of specific recommendations can be found in the section entitled "Recommendations".

Detailed Vulnerability Assessment

Solaris 2.6 Application Server 209.xxx.xxx.1 Vulnerabilties

- Configuration/Operating system vulnerabilities

To determine if any configuration and/or operating system vulnerabilities were present two different open-source vulnerability scanners were used. The two scanners that were used were Nessus 1.06, which was developed by Renaud Deraison and SARA which is based on Dan Farmer's SATAN scanner. In addition any high level vulnerabilities that were discovered by the scanners were then manually checked to insure that they were not false positives.

Both of the scanners discovered several high level vulnerabilities that could lead to the system being compromised. Several of these vulnerabilities centered around dangerous Remote Procedure Call services that were running. RPC is a mechanism used to simplify development of networked applications. The Remote Procedure Call (RPC) Tool Talk service was found to be running. Tool Talk is a desktop manager support program. Rpc.ttdbserverd can be exploited through a buffer overflow attack. Possibly, some patched versions are also exploitable. A remote intruder can execute commands as root if the buffer overflow attack is successful. This vulnerability was checked using an exploit that was downloaded from the Internet and was used successfully to gain root access. This particular vulnerability is well known and used in the "hacker" community. The SANS Institute has this exploit on their top ten vulnerability list. For additional information on this vulnerability see CVE-1999-0003.

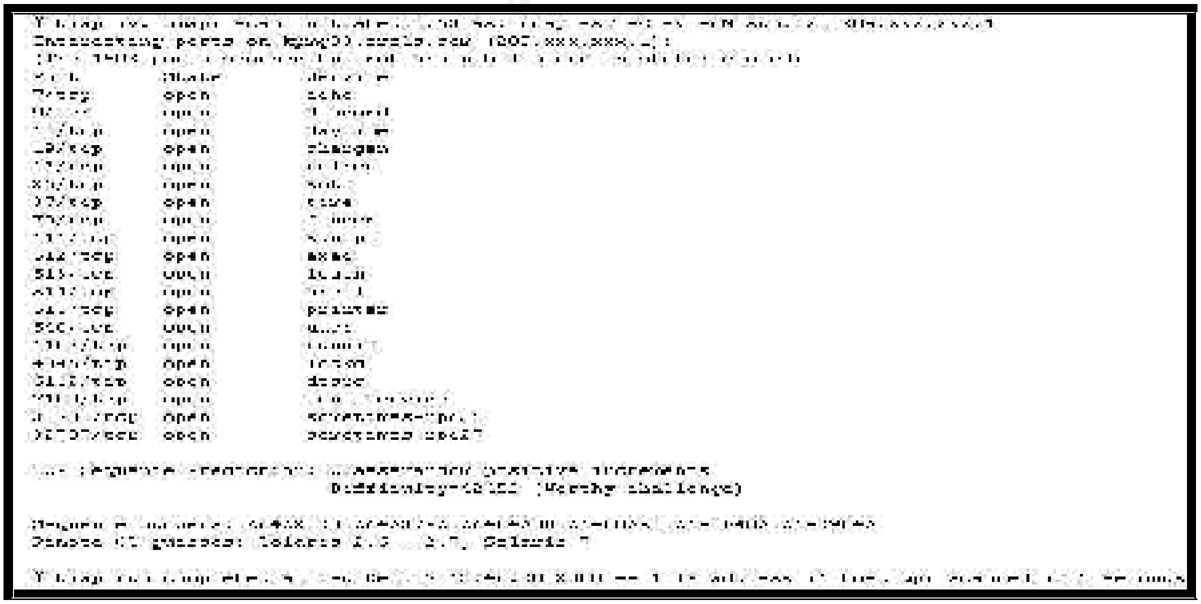
Another dangerous RPC service was discovered to be running. The CMSD RPC service, which is a desktop calendar manager program. RPC.CMSD can be exploited through a buffer overflow attack. A remote intruder can execute commands as root if the buffer overflow attack is successful. This exploit is also well known and is on SANS top ten vulnerability list. This vulnerability was checked manually using an exploit that can be downloaded from the Internet. The exploit was executed successfully and remote commands could be executed on the server as root. For additional information on this vulnerability see CVE-1999-0696 and CVE-1999-0320.

A third potentially compromising RPC service was found to be running on the server. The sadmind RPC service is running. Sadmind is a Solstice administrator support program that can be exploited through a buffer overflow attack. The sadmind program (especially Solaris 2.4, 2.5.x and 2.6) is exploitable for remote root access. Versions are vulnerable to a buffer overflow attack where a well crafted pattern could execute arbitrary commands as the root user. This vulnerability has also made it to SANS to ten vulnerability list and is well known in the "hacking community". This vulnerability was also checked manually using code that was downloaded from the Internet. The code was executed and commands could be issued on the server remotely as root. For additional information on this vulnerability see CVE-1999-0977.

The last dangerous RPC service that was discovered to be running was the Stad RPC service. The rpc.statd program is a support program to NFS which supports file locking when requested. Older versions of statd are vulnerable to a buffer overflow attack where a well crafted pattern could execute arbitrary commands as the root user. This vulnerability was checked manually using code that downloaded from the Internet. The exploit was executed, but it did not appear to be successful. This could indicate that the service is patched or that the exploit code was not written correctly. In any event if NFS is not used by this server the statd service should be removed because additional vulnerabilities could be discovered in the future. For additional information on this vulnerability see CVE-2000-0666, CVE-1999-0493, CVE-1999-0019, and CVE-1999-0018.

A vulnerability was discovered in the netpr program. A buffer overrun exists in the netpr program, part of the SUNWpcu (LP) package included with Solaris, from Sun Microsystems. Versions of netpr on Solaris 2.6 and 7 are potentially vulnerable to this problem. By specifying a long buffer containing machine executable code, it is possible to execute arbitrary commands as root. On Sparc, the exploits provided will spawn a root shell, whereas on x86 it will create a setuid root shell in /tmp. For additional information on this vulnerability see

By running Nmap, an open-source port scanner, several ports were found to be open that could potentially lead to an attacker compromising the system:



```
# Nmap [illegible]
Interesting ports on [illegible] (207.xxx.xxx.[illegible]):
([illegible])
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
540/tcp    open        uucp
[illegible]/tcp   open        [illegible]
4045/tcp   open        lockd
6112/tcp   open        dtspc
7100/tcp   open        font-service
[illegible]/tcp  open        sometimes-rpc[illegible]
[illegible]/tcp  open        sometimes-rpc[illegible]

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=[illegible] (Worthy challenge)

Sequence numbers: [illegible]
Remote OS guesses: Solaris 2.6 - 2.7, Solaris 7

# Nmap run completed [illegible]
```

Several of the ports that are open are not necessarily dangerous, but they are not necessary and are rarely used. Those ports are port 7 echo, port 9 discard, port 13 daytime, port 19 chargen, and port 37 time. Some of the ports that were found to be open that are potentially dangerous are port 23 telnet and the r-service ports 512, 513, and 514. Telnet, rlogin, and rshell are considered dangerous in the sense that they are not encrypted. That means anybody can setup a sniffer, such as dsniff, and can sniff the data that passes between the client and the server. This includes logins and passwords. The rexecd service is open. Because rexecd does not provide any good means of authentication, it can be used by a remote user to scan a third party host, giving you troubles or bypassing your firewall. Also if an attacker can take advantage of another vulnerability and can edit the rhost file he can then connect using rlogin or rshell without any authentication.

In addition port 79 finger was found to be open by Nmap. Certain finger servers, when queried, will release excess data about accounts on the system including who is currently logged on. This excess information could be used as clues for guessing user passwords, determining when the system is idle, and providing indicators when to best attack the system. Many finger servers provide excessive information on users of the system. It may provide a list of users and associated personal information. It also indicates who is logged on. This information can provide the hacker with valuable data to (1) guess poor passwords and (2) determine the optimum time to hack.

- Recommendations on configuration/operating system vulnerabilities

The first step to dealing with RPC services is to determine if the service is necessary, if it is not necessary then it should be disabled. Certain RPC services may not be needed, such as statd if the network is not using NFS. This is a decision that must be made by GIAC's network staff. If the network staff determines that a dangerous RPC service, such as Tool Talk, is necessary then they must be certain to apply the appropriate patches and keep up with future patches and warnings. Other good security strategies involving RPC services are to block port 111 at the external firewall, block spoofed IP addresses, and consider using rpcbind as a replacement. To fix the netpr program removal of the setuid bit on the /usr/lib/lp/bin/netpr program will eliminate this vulnerability.

To fix the ports that were found to be open by Nmap the first step, similar to the RPC services, is to determine if the service is needed. Any services that are not needed should be commented out of the /etc/inetd.conf file. Instead of using the r-services and telnet consider using Secure Shell (SSH) to connect to the server. This will insure that information passed between the client and the server is encrypted, including login names and passwords.

- Risks from installed third-party software

The version of sendmail that was found to be running was 8.6 which is old and has some known vulnerabilities. The SMTP server is configured to allow mail relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth. In addition the EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account. Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

The web server that was running was Apache 1.2.6. Apache is the most popular web server on the Internet according to www.netcraft.com. It is also one of the most secure when installed with the default settings. Apache does not appear to have as many vulnerabilities as the second most popular web server Information Internet Server (IIS). Many vulnerabilities found on Apache web servers are cause by third-party Common Gateway Interface (CGI) scripts. The version of Apache that is currently running on the server has several vulnerabilities that can lead to Denial of Service (DOS) attacks. In addition the web server is running as root instead of as a non-privileged user. This means that if the web service can be compromised the attacker will have root access instead of access as a non-privileged user.

❖ Recommendations on risks from installed third-party software

The version of sendmail should be upgraded to the newest version. To insure that you install the latest version of sendmail see www.sendmail.org. In addition you should configure the smtp server not to accept mail relays. You can list machines which can send email to other domains in the /etc/mail/relay_domains file. This will insure that spammers can not use your smtp server and that email can not be forged. Also the network staff should configure the smtp server to respond to expn and vrfy commands. These commands give an attacker additional information that can be used to attack the network. Consider using an alternative to sendmail, such as qmail, which is more secure,

The web server that is currently running has know vulnerabilities. Upgrade to the newest version of Apache, see www.apache.org for the latest version. Also have the web server running as a non-privileged user not as root. Consider running it in a chrooted environment, this allows the web service to run in a captive environment so that security holes in the web service can not be exploited against the entire machine. Lastly, review all CGI scripts to insure that they are secure.

❖ Security patches up to date

To determine if the appropriate security patches had been applied Axent's Enterprise Security Manager (ESM) was utilized. To run ESM root access to the server was granted by GIAC's network staff. The scan discovered that ten vendor recommended patches had not been applied. Those patches are:
105216-03
105395-03
105401-15
105407-01
105518-01
105667-01
105736-01
105755-06
106049-01
106271-04

These patches can be found at www.sun.com. It is important that the appropriate patches have been applied, as they correct security problems that could lead to the system being compromised.

- Recommendations on bringing security patches up to date

Part of essential network security is staying up to date on the latest patches. It is suggested to apply all patches that have not already been applied. In addition it is important to stay aware of future service patch releases, not only from the operating system vendor, but also from third-party vendors. Consider joining or monitoring security mailing lists that point out the latest security patches.

- Is sensitive data encrypted

Currently sensitive data is not being encrypted on the server. It is suggested that any data that GIAC Enterprise feels is sensitive is encrypted. Consider using a third-party application such as PGP, or some other vendor to insure that sensitive data is encrypted. In the event that the server is compromised the companie's data will be encrypted making it more difficult for an attacker to steal the data.

- Is data sent over Internet encrypted

Currently data that is sent over the Internet is not encrypted. It is recommended that GIAC Enterprises begins to start encrypting data that is moving across the internet. For employees and business partners accessing the corporate network oven the internet a VPN should be implemented to insure that data is encrypted while passing over the internet. For customers using the companies web site to place orders SSL should be implemented using a trusted certificate authority such as a Verisign. This will insure that customer's information is passed encrypted over the Internet, including credit card numbers, and they will not be able to be sniffed.

- Access is granted to those that need it

GIAC's network staff is currently small, however, as it grows stricter access control will have to be enforced. Currently anybody on the network staff has root access to the server and several accounts have not be used to login for a significant amount of time. ESM discovered that three accounts had not been used to login within the last 90 days. From discussions with the network staff it was discovered that there is no password policy.

- Recommendations on how access is granted to those that need it

It is recommended that GIAC begins enforcing a strict password and access control policy. Passwords should expire every 90 days, should have a ten time history, should be greater then eight characters, should be a alpha-numeric mix, and users should be forced to chose a strong password at change time. The use of one time passwords could also be used for greater security. In addition insure that the passwords are stored in /etc/shadow instead of /etc/passwd.

- Backup policies, disaster preparedness, etc.

GIAC Enterprises does not have a disaster recovery plan. A disaster is defined as an event that considerably interrupts or stops the IT infrastructure of the company. This can include the loss of a system, loss of power, natural disaster, or any other event that may result in a diminished IT infrastructure. The presence of a disaster recovery plan will lend structure to the overall IT infrastructure and provide steps that should be taken in the event of a disaster.

GIAC Enterprises does not have an incident response plan. An incident is defined as a breach in security, whether the breach occurs externally or from within the organization. The presence of an incident response plan will assist in the identification and containment of an incident. Without a plan in place containment may occur slowly and evidence may be lost or corrupted prior to areas of authority being properly assigned.

GIAC Enterprises does not have a backup policy. A backup policy is designed to assist system administrators on what to backup, how often to backup, and how backups are handled and stored. Having a backup policy in place will assist in ensuring that all necessary data is backed up in an accurate and timely fashion, are retained for a sufficient amount of time, and are accessible in a timely manner. Backups are occurring at GIAC Enterprises, however there is no policy in place to define the procedures on how backups are to be handled.

- Recommendations on Backup policies, disaster preparedness, etc.

Create a disaster recovery plan for GIAC Enterprises. In the even of a disaster steps and procedures will be available to the recovery team members. This plan will assist in defining disaster criticality, assigning areas of responsibility to recovery team members, and reducing down time in the event of a disaster.

The disaster recovery plan should include areas of responsibility for disaster recovery team members, how usable hardware can be redistributed, the priority of services that must be re-established, a time-line of recovery events, and how to deal with the public.

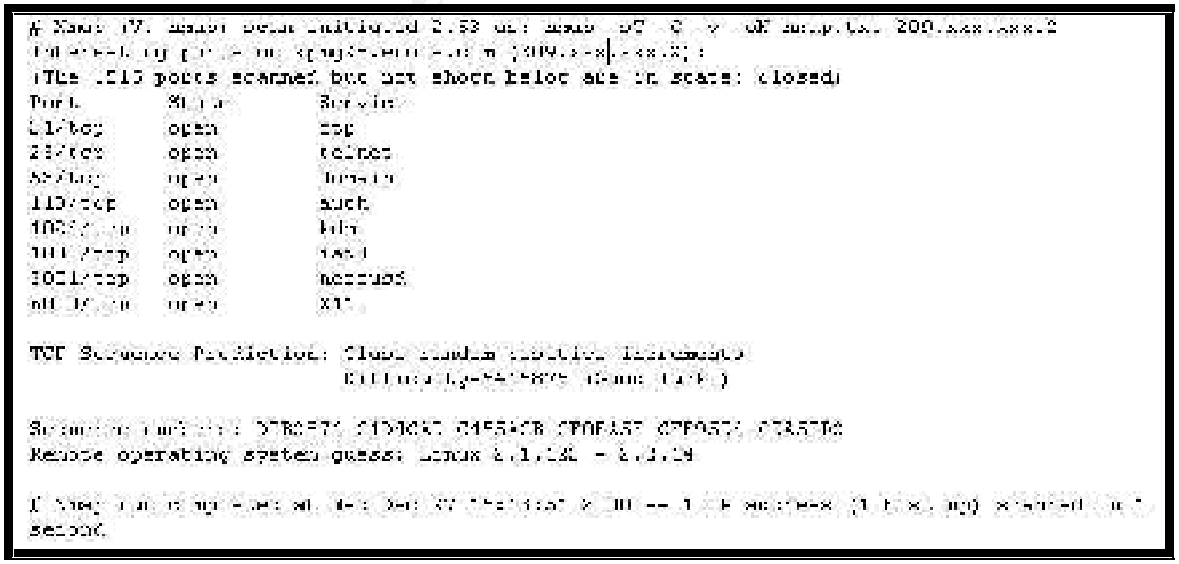
Create an incident response plan for GIAC Enterprises. Should an incident occur steps and procedures will be available to an assigned incident response team. This will assist with the proper handling of data, containment procedures, recovery procedures, and how best to proceed with possible prosecution.

Create an effective backup policy for GIAC Enterprises. Having accurate backups is a critical factor for every IT department.

Red Hat Linux 6.1 DNS Server 209.xxx.xxx.2

- <u>Operating system/Configuration vulnerabilities</u>

Several vulnerabilities exist in the Linux Red Hat operating system. Several of these vulnerabilities have been fixed in service patches. Like the Solaris server that was examined Nmap discovered that several potentially dangerous ports were found to be open:



```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sT -O -v -oN nmap.txt 209.xxx.xxx.2
Interesting ports on [illegible] (209.xxx.xxx.2):
(The 1513 ports scanned but not shown below are in state: closed)
Port        State       Service
21/tcp      open        ftp
23/tcp      open        telnet
53/tcp      open        domain
113/tcp     open        auth
1024/tcp    open        kdm
1011/tcp    open        [illegible]
3001/tcp    open        nessusd
6000/tcp    open        X11

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=[illegible] (Good luck!)

Sequence numbers: 7TBC5F71 [illegible]
Remote operating system guess: Linux 2.1.122 - 2.2.14

# Nmap run completed at [illegible] -- 1 IP address (1 host up) scanned in [illegible]
seconds
```

Port 21 ftp, port 23 telnet, and port 6000 xwindows. These ports can be potentially dangerous if not configured correctly.

- Recommendations on operating system/Configuration vulnerabilities

Instead of using telnet consider using Secure Shell (SSH) to connect to the server. This will insure that information passed between the client and the server are encrypted, including login names and passwords. Review the need for using FTP, if not needed remove it. For information on securing FTP see the next section. Xwindows is potentially dangerous to run on a production server, if not need remove it. If needed insure that xhost file is setup to only allow connections from the local machine, block port 6000 at the firewall, use SSH to tunnel remote xhost events, and use kerberos authentication.

- Risks from installed third-party software

Two major vulnerabilities were found involving third-party software. Older versions of wu-ftp and BIND were found to be running. The version of wu-ftp that is currently running is 2.5.0. There is a general class of vulnerabilities that exist in the version of wu-ftp that is currently running. Due to insufficient bounds checking, it is possible to subvert an ftp server by corrupting its internal stack space. By supplying carefully designed commands to the ftp server, intruders can force the server to execute arbitrary commands with root privilege. On most vulnerable systems, the ftpd software is installed and enabled by default. This vulnerability is well known in the hacker community. An exploit was downloaded from the Internet and run successfully against the server, which would allow an attacker to issue commands as root. For additional information on this vulnerability see CVE-2000-0573.

The version of BIND that is currently running is 8.2.1. The version of BIND that is currently running does not properly bounds check a memory copy when responding to an inverse query request. An improperly or maliciously formatted inverse query on a TCP stream can crash the server or allow an attacker to gain root privileges. Also the version of BIND that is running does not properly bounds check many memory references in the server and the resolver. An improperly or maliciously formatted DNS message can cause the server to read from invalid memory locations, yielding garbage record data or crashing the server. Also the BIND service was running as root. For additional information on this vulnerability see CVE-1999-0833

- Recommendation on risks from installed third-party software

To fix the vulnerabilities that were found in the ftp service upgrade to the newest version of wu-ftp, see www.wu-ftp.org to insure that you have the latest version. Remove anonymous ftp access by removing guest access in /etc/ftpaccess and remove the anonftp home directory. Utilize TCP wrappers to control access to the ftp server.

To fix the vulnerabilities that were found in the version of BIND that was running upgrade to the newest version of BIND, which currently is 8.2.2P3. Consider running BIND in a chrooted environment without superuser privileges. Implement a split-horizon DNS. This is where one set of information is available to the outside world and another set is available to the internal organization.

- <u>Security patches up to date</u>

From reviewing the system and interviewing the network staff it was apparent that the appropriate security patches had not been applied.

- <u>Recommendations on bringing security patches up to date</u>

Part of essential network security is staying up to date on the latest patches. It is suggested to apply all patches that have not already been applied. In addition it is important to stay aware of future service patch releases, not only from the operating system vendor, but also from third-party vendors. Consider joining or monitoring security mailing lists that point out the latest security patches.

- <u>Is sensitive data encrypted</u>

See the Solaris section for information.

- <u>Is data sent over Internet encrypted</u>

See the Solaris section for information.

- <u>Access is granted to those that need it</u>

See the Solaris section for information.

- <u>Backup policies, disaster preparedness, etc.</u>

See the Solaris section for information.

Prioritized Vulnerabilities/Issues

Solaris 2.6 Application Server 209.xxx.xxx.1

1. **Dangerous/Vulnerable RPC services**
2. **Older version of Sendmail**
3. **The r-services are running**
4. **Telnet running.**
5. **Finger running**
6. **No documented procedures.**
7. **Appropriate patches have not been applied.**

Red Hat Linux 6.1 DNS Server 209.xxx.xxx.2

1. **Older version of BIND running.**
2. **Old version of wu-ftp running.**
3. **Telnet service is running.**
4. **No documented procedures.**
5. **Appropriate patches have not been applied.**

Appendix A
Scan Results

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 2
 - Number of security warnings found : 3
 - Number of security notes found : 3



TESTED HOSTS

 209.122.157.60 (Security holes found)



DETAILS

+ 209.122.157.60 :
 . List of open ports :
   o domain (53/tcp) (Security hole found)
   o telnet (23/tcp) (Security warnings found)
   o ftp (21/tcp) (Security hole found)
   o auth (113/tcp) (Security warnings found)
   o unknown (3001/tcp) (Security warnings found)
```

edited because of length……….

SARA Scan Summary

Host Name	IP Address	Host Type	Green	Red	Yellow	Brown
kpmg28.erols.com	209.xxx.xxx.2	Red Hat	1	2	0	0

Table 1 Hosts on Sub-net 209.xxx.xxx

Host: xxxx.erols.com

General host information:

- Host type: Red Hat
- Subnet 209.xxx.xxx
- Telnet server (GREEN)

Vulnerability information:

- WU-FTPD vulnerabilities(RED)
- DNS is vulnerable(RED)

Edited due to length………

References

www.apache.org
www.securityfocus.com
www.sendmail.org
www.wu-ftp.org
www.netcraft.com
www.sun.com
www.redhat.com
www.sans.org