

Limited Security Assessment of

Secure Hospital

Security Testing and Reporting done by
Jason Ellison <jason.ellison@jasonellison.net>

<http://www.jasonellison.net/>

Executive Summary

Secure Hospital requested a limited security assessment to evaluate their current security posture. The client requested the security assessment be limited to on site wireless access points and one publicly accessible network range. Due to the limitation requested by the client, this security assessment can only indicate the security posture of the devices tested. This document should not be referenced as a complete security assessment of internal/external system security beyond the scope specified by the client. The findings only represent the current security posture as of December 30, 2003.

Assessing the security of the publicly accessible network and publicly accessible wireless access points provide information of probable targets, or possible entry points, for an outside attacker. The data contained in this report could be later analyzed and used in a risk assessment. Network services and the risk they impose on network security should be compared to the value the service provides. Results of this assessment should also be compared against expected results. Compliance discrepancies between internal policy, governing regulations, and actual practice should be noted and addressed.

Scope

Per the client's request, this assessment was limited to the following publicly accessible targets:

- xxx.xxx.80.184/29 IP range publicly accessible
- 802.11 b/g wireless access points (WAP's) accessible external to the hospital

In an effort to reduce network impact and reduce interference with daily business, no denial of service (DOS) type attacks were tested. Tests took place between November 16, 2003 and December 30, 2003. Tests were performed using standard network testing tools as covered in the "The Open Source Security Testing Methodology Manual" (OSSTMM 2.1).

Wireless network testing was limited to networks accessible from outside the building using standard 802.11b/g equipment. High gain antennas were used in long distance data collection. Due to previous knowledge 802.11a was not tested. WEP key cracking of WEP encrypted 802.11 networks is considered outside the scope of this assessment.

Publicly addressable addresses xxx.xxx.80.184 - xxx.xxx.80.191 were tested using Firewalk, Nessus, Netcat and NMAP. In order to not impact the quality of service (QOS) of the remote network, these addresses were scanned and assessed using minimal bandwidth by using conservative setting when possible by limiting network bandwidth usage.

Detailed Reporting/Risk Assessment

Whois data on domain Securehospital.com

Whois data disclosed sensitive information that could be used in social engineering attacks. While the disclosure of this information is normal, it should be noted that this information is publicly available. All employees should be aware of what information is publicly available, so that the disclosure of this publicly available data to employees by an attacker does not gain unwarranted trust.

Registrant:

Secure Hospital
xxx xxxxx Ave
City, ST xxxxx
US

Registrar: XXXXXXXX
Domain Name: SECUREHOSPITAL.COM
Created on: 13-JUN-XX
Expires on: 13-JUN-XX
Last Updated on: 23-OCT-XX

Administrative Contact:

Lastname, Joseph jLastname@Securehospital.com
Secure Hospital
xxxx xxxxxxx Ave
City, ST xxxxx
US
xxx.xxx.xxxx
xxx.xxx.xxxx

Technical Contact:

xxxxx, xxxxx xxxx.xxxx@xxxx.com
XXXX
xxxx xxxxx St.
City, ST xxxxx
US
xxx.xxx.xxxx
xxx.xxx.xxxx

DNS data on domain Securehospital.com

The DNS Servers were queried for zone transfers. Both AXFR and IXFR transfers were attempted on all authoritative servers. All servers were found to be configured correctly. All servers denied AXFR and IXFR zone transfers.

```
# dig Securehospital.com NS

; <<>> DiG 9.2.0 <<>> Securehospital.com NS
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62320
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;Securehospital.com.          IN      NS

;; ANSWER SECTION:
Securehospital.com.         172800  IN      NS      xxx.xxx.net.
Securehospital.com.         172800  IN      NS      xxx.xxx.net.
Securehospital.com.         172800  IN      NS      xxx.xxx.net.

;; ADDITIONAL SECTION:
xxx.xxx.net.                172800  IN      A       xxx.xxx.xxx.xxx
xxx.xxx.net.                148415  IN      A       xxx.xxx.xxx.xxx
xxx.xxx.net.                148415  IN      A       xxx.xxx.xxx.xxx

;; Query time: 99 msec
;; SERVER: 10.0.0.1#53(x.x.0.1)
;; WHEN: Sun Jan 18 02:53:08 2004
;; MSG SIZE rcvd: 169
```

Target: xxx.xxx.80.185 (External Router)

This device was identifiable as a Cisco router via both: NMAP and its telnet banner. The Cisco device uses predictable IPID's. Predictable IPID's allow for the device to be used as a zombie to complete blind port scans. The telnet banner contains more information than is needed according to standard security practices.

ICMP

This device did respond to ICMP Echo (Type 8) and Timestamp (Type 13). The latter can be useful in breaking time based authentication methods.

TCP/23 - TELNET

The telnet banner discloses more information than needed. From this banner the following details are readily available:

- I. The router is likely owned by Securehospital.com
- II. Patty Xxxxxx is the likely administrator of the router
- III. Patty Xxxxxx's email exposes the format of mailboxes used by Securehospital.com
- IV. The phone number xxx-xxx-2375 gives a target exchange for wardialing.

Please read <http://www.cisco.com/warp/public/707/21.html#warning>

TCP/500 - ISAKMP

ISAKMP was detected on the device indicating that VPN services are available on the device. This should be checked against the public policies.

Target: xxx.xxx.80.186 (PIX External Address)

This device type was not detectable from external networks via standard scan types.

ICMP

This device's presence was detectable via ICMP Echo (Type 8).

Target: xxx.xxx.80.187 (Software Link Server)

This device fingerprints as a Windows 2000 Server running various services that have a history of bad security. Fingerprints were obtained via TCP fingerprints and verified via banner grabbing. This host is a prime target for network penetration. Regular updates and subscribing to all relevant mailing lists is highly advisable. The most recent remote arbitrary code execution was MS03-051. MS03-051 was released on November 11, 2003 and discusses a bug that allows complete remote control of the system.

TCP/21 - FTP

Port is filtered via the FTP server configuration apparently based on the source IP address. This does not protect the server from TCP fingerprinting attacks. If source IP address's are known this should be done at the router.

TCP/80 - HTTP

IIS 5.0 Webserver, banner unobfuscated. Information leakage of the following pieces of data was confirmed:

- anonymous user "webuser"
- internalip address "10.0.21.27"

Frontpage Extensions were detected. Frontpage extensions have been known to have security issues in the past. Two services, ".printer" and WebDAV, also appear to be active. Both of the afore mentioned services have been found to have remotely exploitable buffer overruns in the past. These services should be updated regularly.

TCP/443 - HTTP/SSL

SSL IIS Server port. This service has the same problems as the HTTP service.

TCP/1723 - PPTP

PPP Point to Point tunneling service. Service allows remote computers or networks to be connected to the internal network as if they were attached locally. It may be possible to brute force username/password combinations.

TCP/3389 - RDP

Remote Desktop Protocol allows for users or administrators to remote control a Windows operating system. These Services should be well protected due to the ability to brute force username password.

Target: xxx.xxx.80.188

This device type was not detectable from external networks via standard scan types.

ICMP:

This device's presence was detectable via ICMP Echo (Type 8).

Target: xxx.xxx.80.189

No device responded.

Target: xxx.xxx.80.190

No device responded.

802.11/b WAP "101" BSSID: "00:05:5D:XX:XX:6B"

Device was identified via broadcast beacon packets and unencrypted traffic. No security was detected. This device provides unauthenticated unencrypted access to the internal LAN.

802.11/b WAP "default" BSSID: "00:05:5D:XX:XX:84"

Device was identified via broadcast beacon packets and unencrypted traffic. No security was detected. This device provides unauthenticated unencrypted access to the internal LAN.

Conclusions and Recommendations

Basic security practices dictate that each service offered publicly should be reviewed to verify the service is in-line with the entities information technology plan. Services that are not in line with the information technology plan, services that have not provided enough value, and/or services that are not necessary should be justified carefully.

In review of the current security posture of devices within the scope of this test I offer the following suggestions in order of importance:

Remove or encrypt wireless connections

Large concentrations of wireless access points (WAP's) were detected around or near the Secure Hospital. Two WAP's found to be attached to Secure Hospitals internal network lacked encryption allowing for unauthenticated and unencrypted two way communications to the internal network from the parking lot. From an extended distance traffic could be sniffed revealing important information such as: the internal network layout, passive systems identification, workstation names and usernames, passwords, hardware platforms and software platforms deployed on the network. Periodic scanning of the local premises to discover unauthorized wireless access points should be considered.

Verify secure remote connections, re-certifying periodically

During assessing the targets within scope, several methods of remote connectivity were noticed. Allowing a remote network and or a user the ability to connect into your internal network carries with it inherent dangers. If an attacker manages to compromise the remote workstation or network, the attacker would then have all the privileges that were granted to that workstation and or network. For this reason written procedures and guidelines for securely attaching remote workstations and/or networks should be used. Occasionally the remote sites should be audited to verify they maintain compliance. This should include, but not be limited to, requiring remote sites to maintain antivirus software on all workstations and or workstations on remote networks, require remote sites implement certain security measures to maintain reasonable physical and network security on their location, require remote site and/or user to have read and sign written policies concerning network/computer usage.

Reduce unnecessary information leakage

A few information leaks discovered during the assessment could be used by an intruder to increase the chances of a successful computer attack and/or social engineering attack. When ever possible information should be restricted to anonymous users. For instance, the telnet banner on the Cisco router at xxx.xxx.80.185 provides information that could be used in a wardialing attack, and or a social engineering attack. Telnet banners are viewed by anonymous users before being prompted for a username and password. Telnet banners on devices that are publicly accessible should have generic messages containing only the information necessary to warn unauthorized users of the laws covering the use/misuse of the device. The N.S.A.'s discuss the purpose and format of a login banner in their publication titled "Router Security Configuration Guide"

"A login banner, which includes a legal notice, should be set up on each operational router. (A legal notice usually includes a 'no trespassing' warning, a statement that all use of the router must be authorized by the owning organization, and perhaps a statement about the router being subject to monitoring. A proper legal notice protects the ability of the owning organization to pursue legal remedies against an attacker. Consult your organization's legal staff or general counsel for suitable language to use in your legal notice.)" [1]

Current login banners for Internal policies that are currently shown on the telnet banner to anonymous users should be moved to motd banners so that only authorized users receive the sensitive information. The motd banners are only shown to users after they have provided valid authentication information. Examples of standard login banners are provided in the appendices. [2]

The IIS server at xxx.xxx.80.187 was found to disclose both the anonymous IIS account and the machines internal IP address. Restricting the HTTP methods available to users via URLSCAN can prevent this. [3] This information is valuable to an attacker for reconnaissance. Knowing the anonymous webuser gives the attacker a valid account to bruteforce. Disclosing the machines internal IP address allows for the attacker to understand the internal IP addressing schemes. Microsoft published an excellent tool to assist in locking down IIS called "IIS Lockdown Tool ".[4]

ICMP discovery revealed device layout on the on the public network. The ICMP egress responses can be restricted at the external router. This should be considered to avoid mapping the public devices. Detection of the IPID's was also significant when trying to defeat encrypted services that rely on time. Detection of sequential IPID's could also be avoided via filtering the packets at the egress router.

Rigorously maintain remotely accessible Windows machines

The Windows server found at xxx.xxx.80.187 is a prime target for entry into the network. Windows servers have been studied for weaknesses by the hacking community due to the high prevalence of them in the wild. The high number and high frequency of remote and local exploits written for the Windows platform highlight this fact. With this in mind, selected staff members should be assigned the task of following Microsoft's and CERT security mailing lists. These individuals should also maintain or verify patches on the operating system and services. Any service not being used should be closed to avoid increased chance of intrusion.

Technical Annexes and Appendices

[1] "Router Security Configuration Guide" Report Number: C4-040R-02 (<http://www.nsa.gov/snac/cisco/download.htm>).

[2]

login banner Sample 1:

"This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity or policy violation, system personnel may provide the evidence of such monitoring to law enforcement or other officials."

login banner Sample 2:

*** UNAUTHORIZED ACCESS PROHIBITED BY LAW - TITLE 18 U.S. CODE SECTION 1030 ***

[3]

URLScan Security Tool

<http://www.microsoft.com/technet/security/URLScan.asp>

[4]

IIS Lockdown Tool

<http://www.microsoft.com/technet/security/tools/locktool.asp>

[5]
802.11 kismet wireless scan

