Global Information Assurance Certification Paper

What's the Frequency, Kenneth? Protecting from the dangers of corporate users accessing WiFi hotspots.

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Ed Fisher
Location: Challenge

Table of Contents

List of Figures

Abstract/Summary

Ubiquitous computing: Our users want it. Our employers expect us to support it. The commercials, posters, and coffee cups tell them that they can have it through the wonders of Wi-Fi. Free or low cost Internet access using 802.11b is becoming widely available through the deployment of Wi-Fi hot spots. Hotspots are now in airports, coffee shops, bookstores, and restaurants. "Free high-speed Internet" is replacing "Free HBO and continental breakfast" on hotel signs. We, as information security professionals, must be prepared to address the risks, and to provide our users with a secure way of using this access. The threats are numerous, and run the gamut from network exploits to corporate espionage. The challenge of securing a machine using such a potentially hostile network may seem insurmountable. I say "seem," because in reality it is not. A proper balance may be achieved between security and functionality that will satisfy the needs of information security, while accommodating the wants of the "road warrior."

This paper will discuss the exploitation of a laptop user accessing the Internet through a hotel's free Wi-Fi network. The improper configuration of corporate portals will then be highlighted to show the risks of users accessing corporate resources from open networks. Although the scenario is fictional, the exploits and the repercussions are real. One hundred systems attached to the Internet, and discovered through a simple search using Google, were analyzed. The percentage of Internet systems poorly configured and easily exploited is alarming, and it is hoped that this paper may raise an awareness of this, and help convince those systems' administrators of the need to better secure their systems.

Introduction

The purpose of this paper is to highlight the dangers of accessing confidential data while using an open wireless network, and to present the reader with a guide on how best to remediate those dangers.

An increasing number of knowledge workers are being equipped with laptop computers and sent beyond the boundaries of the corporate network to perform their jobs. These users travel continuously, and may only be in the office once a quarter or even more infrequently. They either have local administrator accounts on the laptop, or are given the administrator password by a well-intentioned Helpdesk employee when they are having problems. They are outside of our protections. Worse, they will at some point connect to the internal network over a vpn, or physically when they do visit the office. If they have "picked something up" they may bring the compromise within the boundaries of the internal network.

In the defense of our traditional user base, we rely upon certain mainstays of our trade. Although your actual mileage may vary, the following statements are generally considered true, or at the very least desirable.

- Users' workstations live on the corporate internal network, behind our firewalls.
- We use NAT for their connectivity, and filter it with access control lists.
- Security updates can be deployed to them when needed, either by automated processes or in the good old fashioned way.
- Internet access is controlled by the proxy so that no 'inappropriate' sites are visited.
- The users are not local administrators of the machines, so there is little that they can do.
- And, should something slip past these precautions, we can always touch the machines when needed.
- Data is stored on network shares that are backed up regularly, and access to that data is controlled.
- Physical security prevents unauthorized users from accessing removable media, and
- IDS systems are in place to detect anything that somehow manages to bypass everything else.

There are also a number of common assumptions that administrators make about their Internet attached networks, and the safety of their external systems. This paper should help to convince systems administrators of the importance of properly setting up and securing systems.

Wireless Networking and "Hotspots"

Wireless networking uses FM radio signals, commonly in either the

2.4GHz or the 5.8GHz bands. There are three common wireless network specifications;

802.11b	the most common type, using DSSS signaling in the 2.4GHz ISM band. Speeds of up to 11Mbps are possible, and many newer laptops have client hardware built-in.
802.11g	Compatible with 802.11b, but offering speeds of up to 54Mbps.
802.11a	Uses the 5.8GHz UNII bands and offering speeds up to 54Mbps, 802.11a is not as common because of a number of reasons, including higher cost, and shorter range.

No matter which standard is chosen, the common implementation is to use Infrastructure mode, where a central access point acts as a bridge between the wireless clients and the wired network. For Internet access, the access point may be a combination device, offering a number of services including DHCP, NAT, and firewalling, and facilitates the connection between the wireless clients and the Internet.

Hotspots are locations offering inexpensive or free Internet access, usually to attract customers to their core business. Hotels offer wireless access to the Internet as a cost effective alternative to deploying a wired infrastructure. Coffee shops, bookstores, and restaurants may deploy a simple wireless infrastructure to attract customers and encourage them to remain in place for longer periods of time, which should lead to more sales. Airports are beginning to deploy hotspots as either a free or pay service to attract business travelers.

In all cases, there is typically no advanced technical support in place, so the more readily available means for protecting users from malicious activity are not deployed. Layer 2 encryption methods are available to protect confidentiality, but cannot be used with most hotspots. WEP encryption requires an understanding of how to set the client up, which is not something that the hotspot operators can count upon the users posessing. WPA, TKIP, and 802.1x mechanisms all require compatible clients and prior knowledge of the user. The transient nature of the typical hotspot client rules this out. To attract the users, the network must be made as easy to use as possible. Accessibility trumps security once again.

Wireless networking transmissions propagate indiscriminately, and the wireless network can be readily compared to a “shared-access” medium like Ethernet using a hub. Anyone within range of a wireless network can intercept these transmissions with any compatible client and protocol analyzer. Without transport or application layer data encryption, anyone in range can view the data transmissions of any user on the network. Worse yet, the authentication and association methods used by open wireless hotspots means that a malicious user can easily mount a “man in the middle” attack for encrypted traffic.

When combined with poor remote access policies, the potential for a compromise is very high. Two common remote access applications have been identified and researched to further illustrate the problem.

Protocols/Services/Applications

The Open Wireless Network User exploit takes advantage of the open nature of 802.11b hotspot networks. A user's credentials can be compromised through the use of common clear text based network services. With compromised credentials, a malicious user can gain access to corporate web portals, websites, personal email accounts, and more. A malicious user can also use compromised credentials to exploit a user's workstation.

802.11b networks use Direct Sequencing Spread Spectrum radio transmissions in the 2.4 GHz ISM band. The spectrum is divided into eleven channels (in the United States) of 800 MHz each. All clients of the same access point will use the same channel, and share half duplex access to the network by using either CSMA/CA or Polling. The natural propagation of radio frequencies means that anyone in range of both an access point and a client can use a frequency analyzer to view the client's traffic. There are various layer 2 encryption methods meant to protect against this eavesdropping, but they cannot be easily deployed to clients of a hotspot network.

- Static Wired Equivalent Privacy (WEP): Static WEP is built into all 802.11b access points, and uses an implementation of the RC4 encryption algorithm to provide encryption of layer 2 data. Unfortunately, there are a number of problems with this for hotspots. Static WEP is not configured in the same way across all operating systems or clients, and can present challenges to experienced technical support staff. All users of the same access point must use the same WEP key, and could therefore decrypt one another's traffic. Finally, the implementation of RC4 is flawed, and can be broken by a determined user with time enough to intercept enough packets to perform a collision attack on the encryption key.
- Dynamic Wired Equivalent Privacy (WEP): Dynamic WEP addresses some of Static WEP's shortcomings by providing for automatic key distribution, unique keys for each client, and regular rekeying. Unfortunately, not all operating systems or clients are supported.
- Temporal Key Integrity Protocol (TKIP): TKIP uses a much larger initialization vector than WEP, and combines it with the MAC address of the client to establish unique keys for each client. Unfortunately, there must still be a pre-shared value between clients and access point, which prevents this from being a useful solution on an open wireless network.
- WPA: Wi-Fi Protected Access is a new security mechanism that will provide for AES encryption with a key exchange mechanism. When this standard is fully implemented and supported by access points and clients, it will effectively close the Open Wireless Network vulnerability. However, today's implementation is known as WPA-PSK. That acronym means PreShared Key, and again makes it unmanageable for a hot spot to use.

As all of these require more infrastructure or technical support than a hotel or coffee shop can provide, or will only support a limited range of clients, a hotspot provider has no choice other than to operate the hotspot in open mode.

Clear text protocols transmit all data in the clear, including user credentials. Using a protocol analyzer, anyone within range of the radio transmissions will be

able to view the data, including the credentials. Some of the protocols that can be exploited are detailed as follows.

- Hypertext Transfer Protocol (HTTP): HTTP is the most often used protocol on the internet for the transfer of information from a server to a client, for rendering in a web browser. In addition to web pages of text and graphics, applications can be delivered using application plug-ins, ActiveX components, or even well designed forms. HTTP supports a number of methods, but most often uses get requests from the client to request information, or post requests from the client when submitting information to the server. Graphics and most other files are transferred as binary information, but gets and posts are transmitted as clear text. Application portals including Outlook Web Access and Citrix Nfuse by default use HTTP to provide clients access using only a web browser.

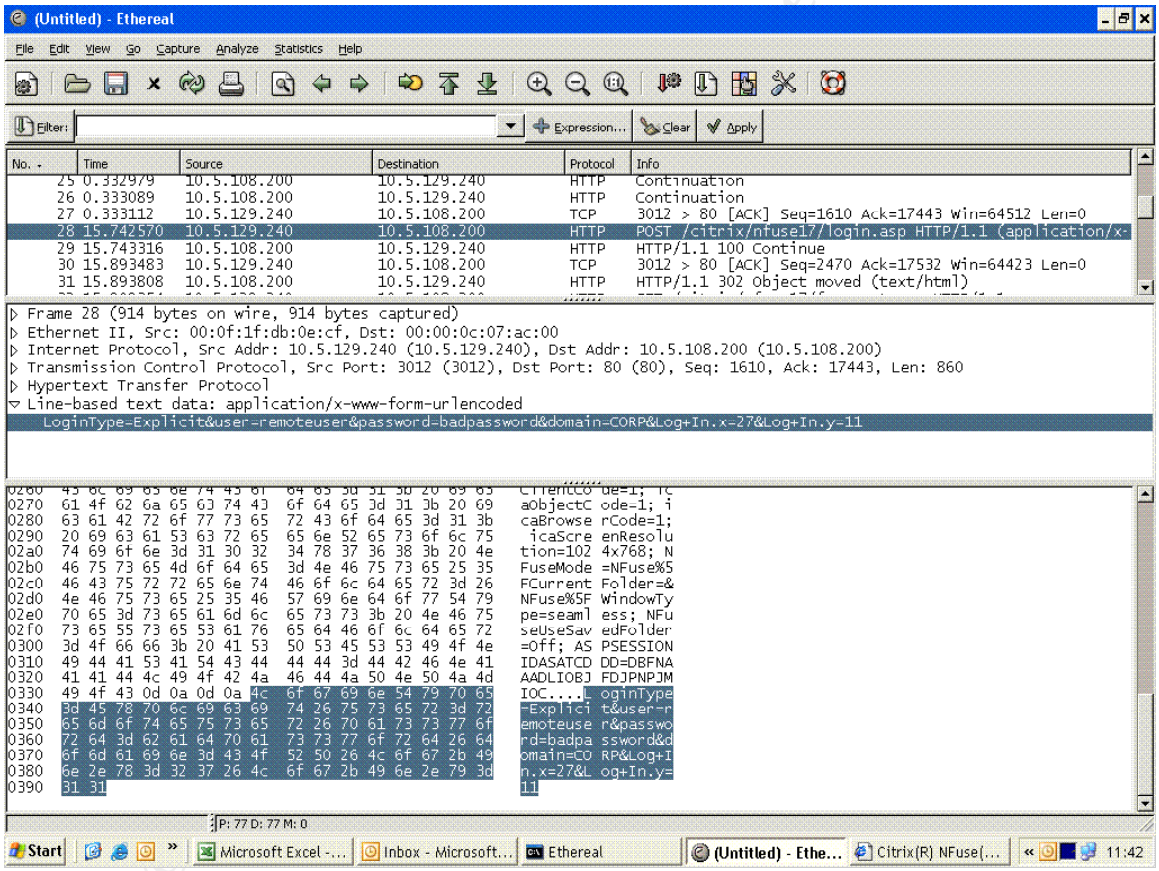


Figure 1-Packet Trace of HTTP traffic

- Post Office Protocol version 3 (POP3): POP3 is a protocol used by mail clients to retrieve emails from a POP3 server. POP3 transmits all information, including usernames and passwords, as clear text. Most ISP's providing email services use POP3. Authenticated POP (APOP) can be used to obscure user credentials, but is only implemented in a small percentage of clients and servers.

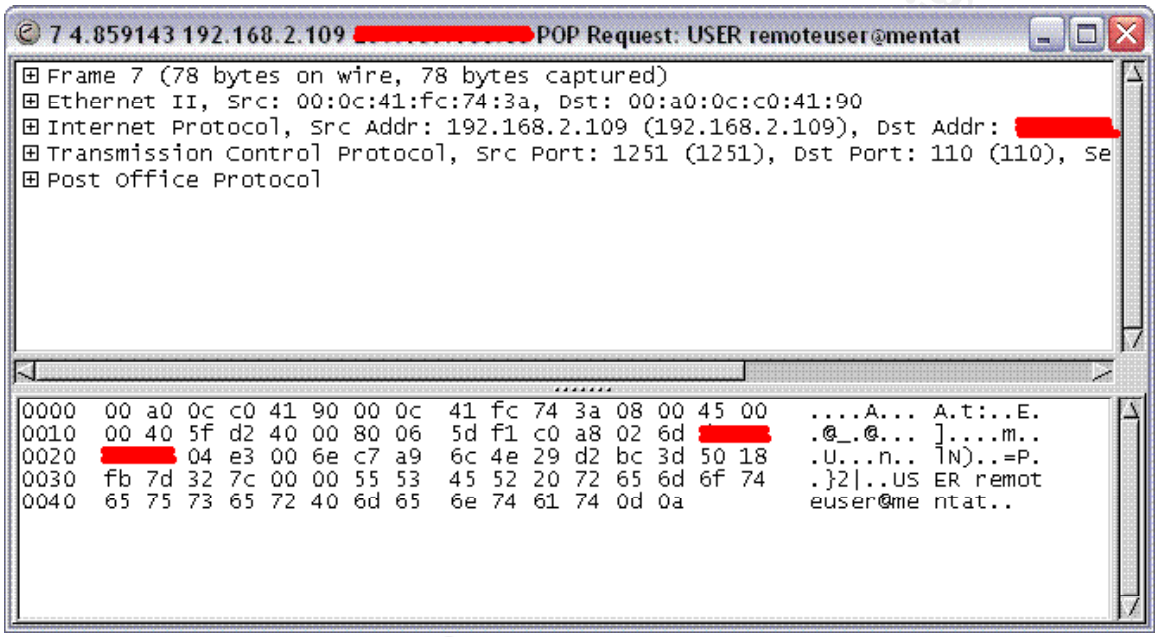


Figure 2-Packet Trace of POP3 username

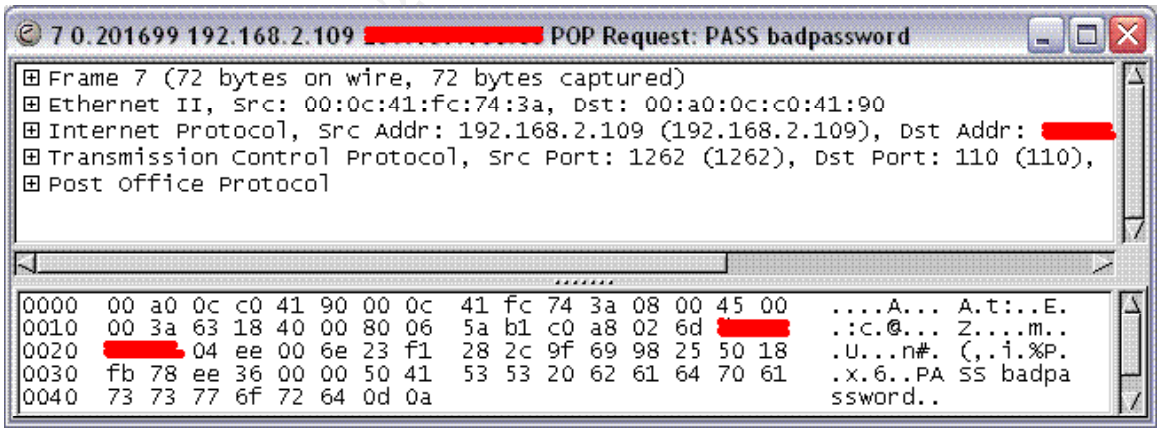


Figure 3-Packet Trace of POP3 password

- Simple Mail Transport Protocol (SMTP): SMTP is used by mail servers when sending mail to other mail servers, but is also used by mail clients when sending mail through a mail server. Like POP3, all information, including usernames and passwords, is sent as clear text. There are authentication extensions to SMTP to protect user credentials, but their use is extremely limited. Usually, client SMTP authentication is accomplished by limiting access to privileged ip addresses, or by first authenticating with POP3 credentials.

Both Citrix Nfuse and Outlook Web Access should only be considered as applications that rely upon the configuration of the webserver for their network communications. If the webserver is properly set up to use an encrypted transport, the user credentials will be protected by that encryption. At the application layer, HTTPS operates the same way as HTTP, however the data transmission is protected by session layer encryption established using a server certificate, or both a server and a client certificate.

Usually the certificate is issued to the server by a Certificate Authority (CA) that the client trusts, but some companies choose to implement their own CA to save money. When this is done, it is critical that the client have the CA root certificate installed. If that is not done, a warning will be presented to the user every time they access the site. If the user becomes accustomed to seeing warnings about certificates, they will not suspect a problem when there is a problem, such as when a site has been compromised, DNS has been poisoned, or a Man in the Middle attack such as webmitm has been launched to circumvent the protections offered by the use of HTTPS.

Section Two

Reconnaissance and exploitation:

A malicious user needs only a laptop computer with a Wi-Fi card and a protocol analyzer compatible with 802.11b networks. One could use almost any operating system and protocol analyzer, but this paper will first illustrate vulnerabilities by using Windows XP sp2 and Ethereal, a GNU/OSS protocol analyzer available on a number of platforms.

While sipping his coffee and reading a book, the malicious user could let Dsniff could run on a Linux or Unix-like operating system, listening for any "interesting" traffic containing login credentials. Dsniff runs on a promiscuous interface, and listens for any protocols that might carry authentication data. When it detects credentials, it displays them in a window, or can save them to a file for later examination.

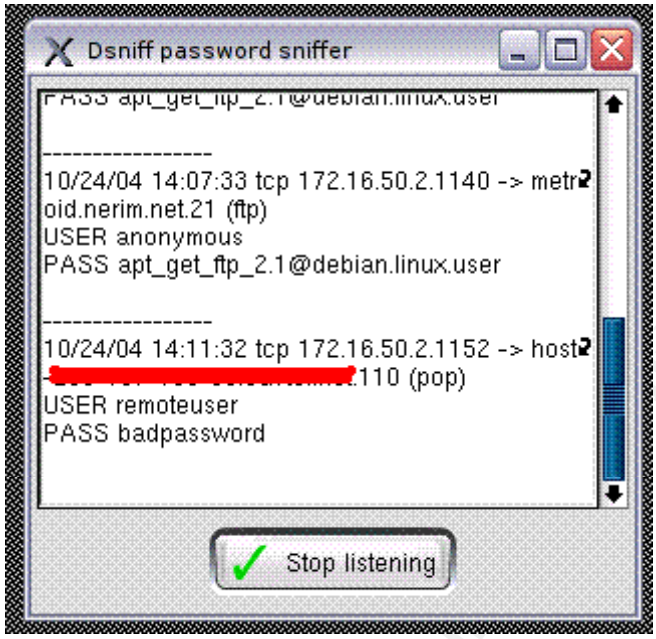
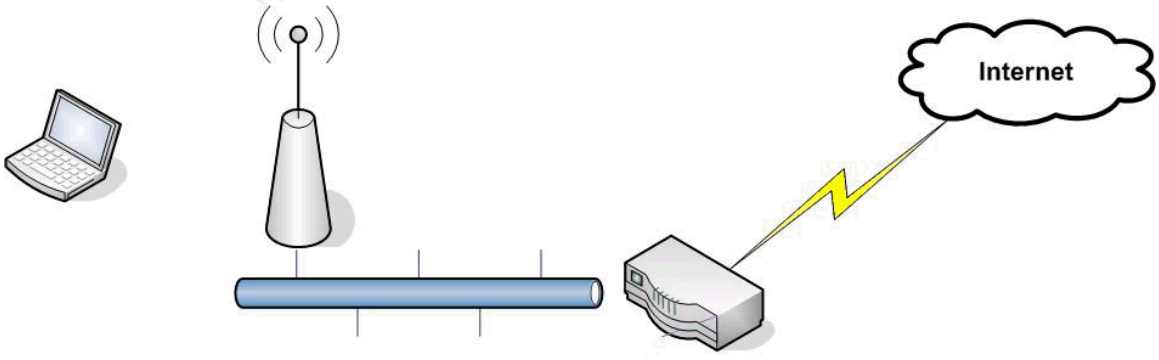


Figure 4-Dsniff displaying usernames and passwords

Typical Wireless Hotspot

The target network for the initial exploit is the wi-fi hotspot network itself. The typical open wireless hotspot network consists of one or more access points, configured to accept any SSID, and to use open authentication without WEP. The network provides DHCP and DNS services, and may have a simple proxy in place. Some "pay for use" networks may use a captive portal in order to prevent access by users who have not paid, but this does not affect the clear text data transmissions. In many cases, all of these services are offered by a single hardware device. Network Address Translation is used to provide the clients with Internet access, and the Internet connection is typically a DSL connection.



Simple Open Wireless Network

Figure 5-Wireless Hotspot

Exploiting a user

The victim must first become a user of the wireless hotspot. For the "Vic" to access the hotspot, he must configure his client operating system to access the network. Again, since this is a hotspot network, there is little to do in the way of security. Vic's client detects the presence of the wireless network, and prompts him to connect.

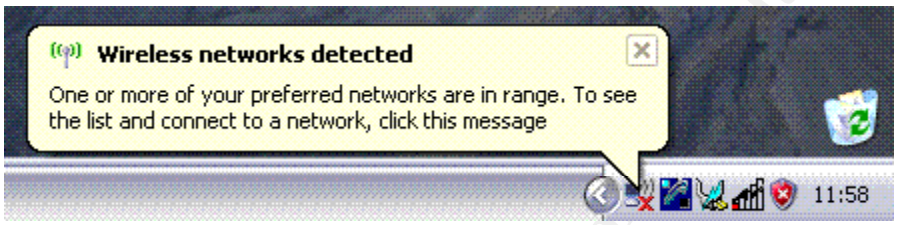


Figure 6-Windows XP wireless network detection notification

Microsoft Windows XP Service Pack 2 does inform the user that the network is open, and the information sent over the network may be visible to others. That probably won't mean anything to Vic though. He clicks the connect button, and is warned one more time.

Figure 7-Warning about open networks

Of course, we all know what Vic is going to do. He clicks Connect Anyway, and is on the network and able to access whatever Internet resources he desires.

Scanning

A malicious user starts by looking for an easy target. Low hanging fruit is the guiding principle here. "Mal" could "wardrive" until he finds an open network.

Wardriving is not a crime. It is the practice of equipping a vehicle with a laptop, wireless client, and a GPS to go out and find wireless networks. As an exercise in security, this is an informative way of surveying networks for their use of security, default ssids, broadcasting ssids, etc.

For a malicious user, it is a way to detect available wireless networks for

unauthorized access or for users to exploit.

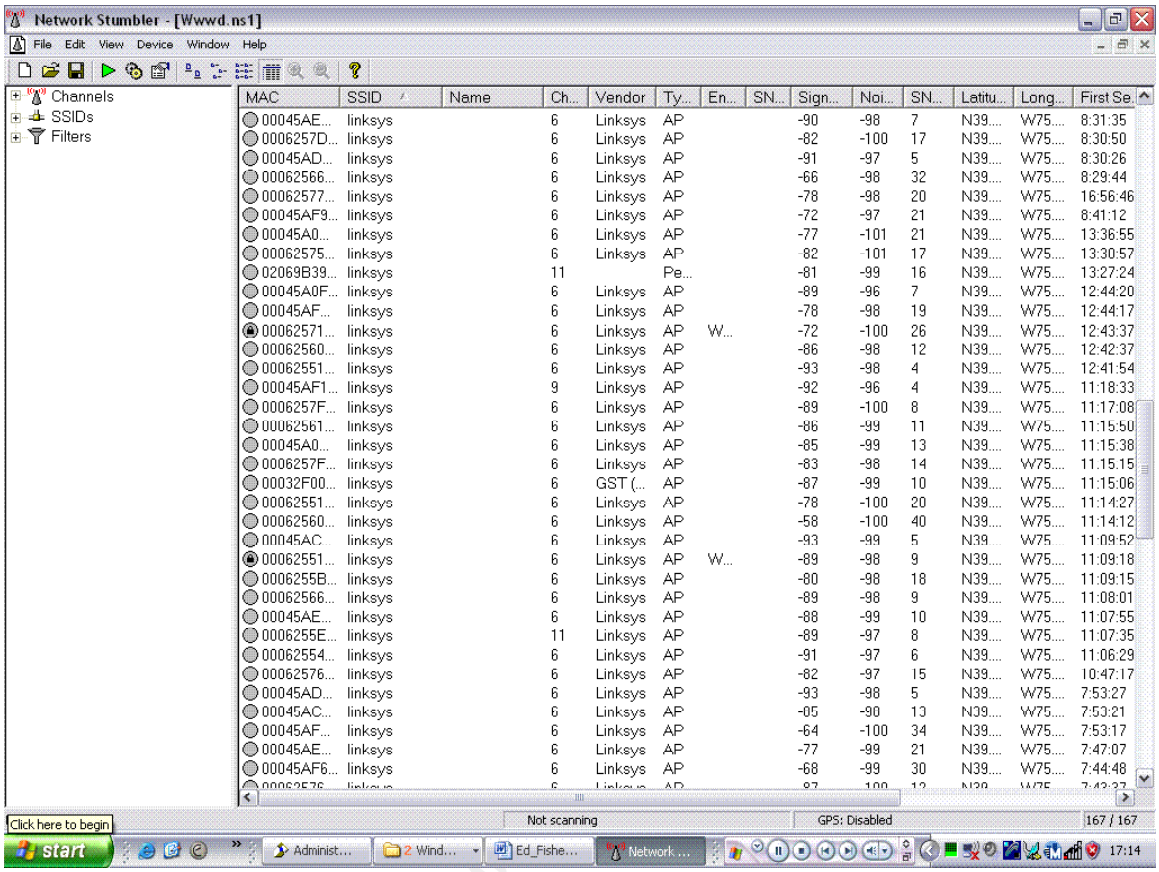


Figure 8-Netstumbler, popular wardriving application

Mal knows that the nearby coffee shop offers free wireless networking to its patrons. He finds a place to sit down, orders a triple latte, and passively scans the frequencies with a protocol analyzer until he finds the hotspot and the channel it uses.

Wireless network transmissions can propagate over large areas, and can be detected by anyone with in range. Using the open-source protocol analyzer Ethereal running on a laptop with a wireless network card, Mal sees a number of different users.

Vic's traffic stands out, however, because of the number of different websites that he visits, and the protocols that he uses. Mal can readily identify all the websites by examining the DNS queries and HTTP GETs. Mal also looks for protocols that require authentication, but transmit data in the clear, such as telnet, smtp, and pop3. Even if no other portals are accessed by Vic, if he checks his email, Mal may pick up mail account credentials that he can use later to send out spam.

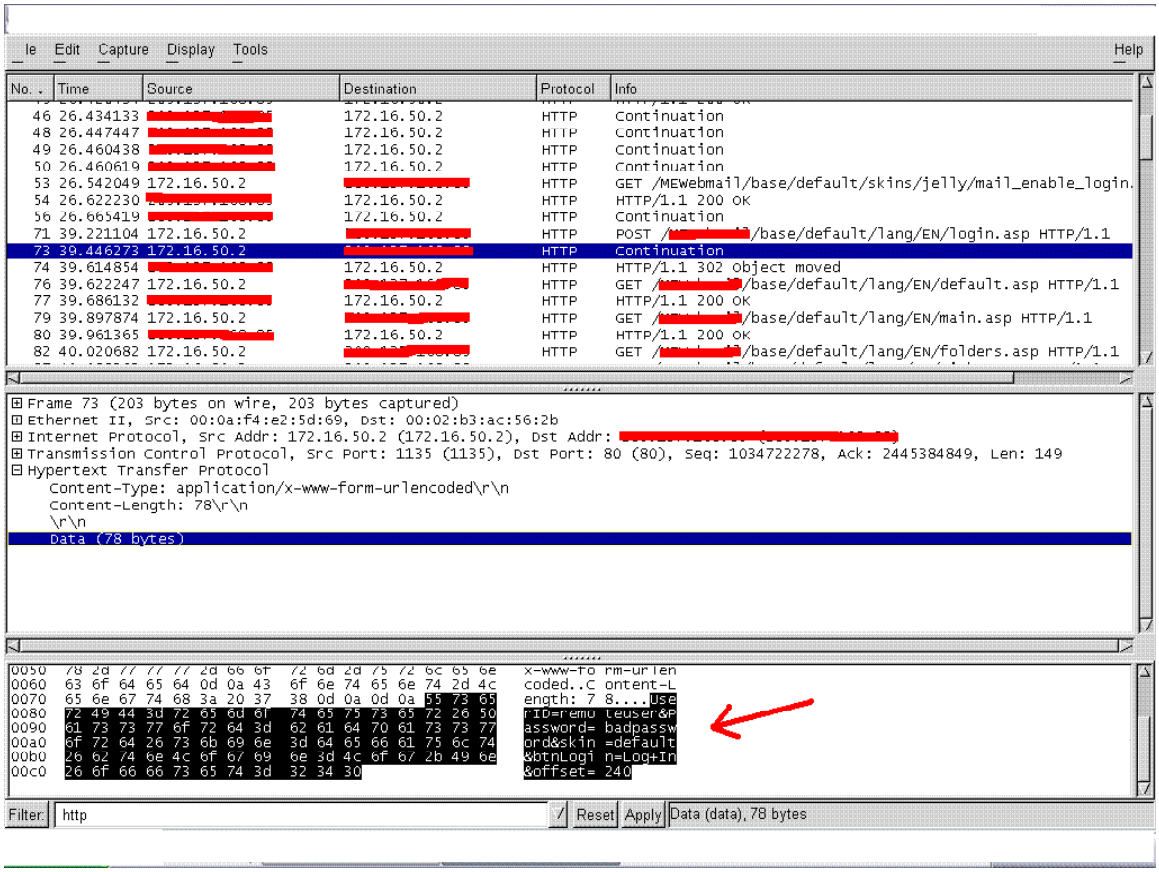


Figure 9-Ethereal displaying cleartext credentials for personal webmail

Vic does access his company's Citrix portal, which is exactly what Mal was hoping for. Vic's company is one of the over 90% of companies "surveyed" that does not use any form of protection for their web based resources, other than to protect access by requiring the user to enter a username and password.

These are submitted to the webserver as HTTP Posts. Mal can easily see those in his protocol analyzer display, and he is very pleased by what he sees.

```
      POST /citrix/nfuse17/login.asp HTTP/1.1
      Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/msword, application/vnd.ms-
powerpoint, application/x-shockwave-flash, */*
      Referer:
http://citrix.company.corp/citrix/nfuse17/login.asp?NFuse_loginErrorI
d=On
      <snip>
      NFuseLogin=NFuse%5FLogonMode=Explicit;
NFuseMode=NFuse%5FCurrentFolder=&NFuse%5FWindowType=seamless;
ASPSESSIONIDASBTCDCC=GNMAEKFALBIGAMEFOLHKIKGD

      LoginType=Explicit&user=remoteuser&password=badpassword&domain=
company&Log+In.x=0&Log+In.y=0
      HTTP/1.1 100 Continue
      Server: Microsoft-IIS/5.0
      Date: Sun, 24 Oct 2004 17:50:14 GMT
```

Now that Mal knows Vic's credentials, he is no longer limited to passive scanning of network traffic. Mal can log in to the Citrix portal the same as Vic, and access any application or data that Vic can access. Depending upon the nature and sensitivity of this information, Mal could do major damage to Vic and his corporation. If Vic is a salesperson, then he will have access to documents and email that could be of interest both to Vic's customers, and to his competition. If Vic is a manager, there could well be information of a sensitive nature, relating both to other employees, and to customers. Suppose Vic works in the financial or healthcare sectors, and has access to confidential information including medical records or financial information. This information, which Vic's company is legally required to protect, is now accessible to Mal.

Detection of this unauthorized access will be extremely difficult. As long as Mal only observes data, there will be very little to show in any logs unless Vic is questioned about every access time and action. Because both OWA and Nfuse permit multiple logins from the same user, there may be nothing that stands out to a security administrator's review of the logs. Because Mal's access will be using Vic's credentials, there will be no failed authentication attempts to either flag an event in the logs, or to cause an IDS system to alert.

Only if the timing is just right, and the administrator very diligent in their review of logs, will this be detectable. Should Mal use Vic's credentials from a different IP address than one that Vic users, at about the same time as Vic accesses the network, a sharp-eyed administrator might notice two entries in the Nfuse logs for the same user, coming from the different ip addresses. In the next graphic, notice the two consecutive entries for the account "remoteuser." In this case, they are from different IP addresses. If Mal used the same hotspot as Vic, and that hotspot used a single global NAT address, it would simply appear as a second login. By itself, that is not unusual.

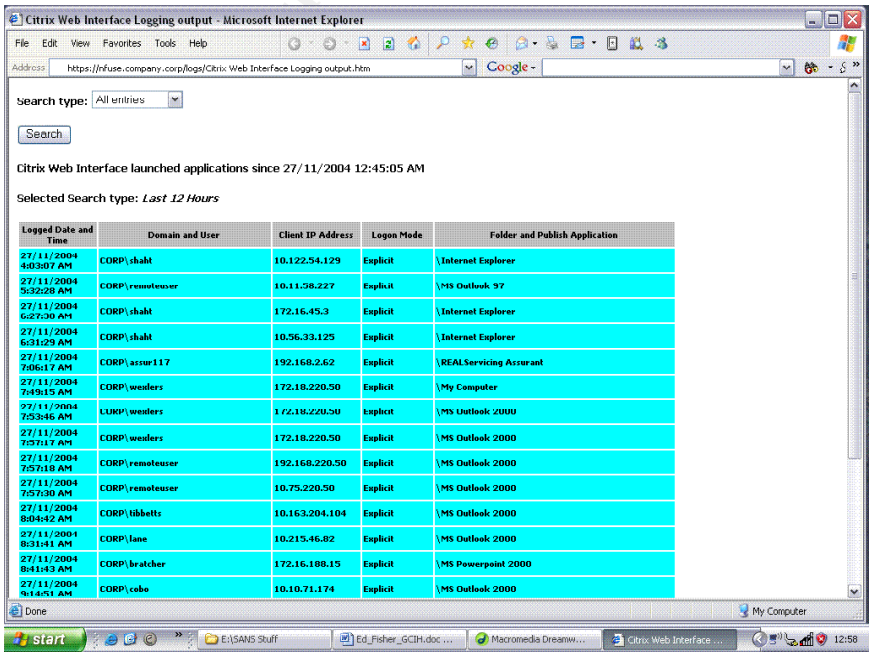


Figure 10-Citrix Web interface logging output

For OWA access, this will be even more difficult to detect as the Security logs in Windows do not log the source IP address of the user. Two differently logins for the same user will only appear as part of the overall listing of logins.

Since both logins will be successful, there will not be anything to flag this access. Only by performing a careful comparison of both the Security Event logs and the IIS logs could someone detect that the same user account was used to access the system from different source IP addresses.

Probing

Mal decides to run a port scan against Vic's computer to see if there is anything interesting. In this example, Vic has an ip address of 172.16.50.6. Mal's first order of business is to scan Vic's IP address to see if there are any ways in to the system. He uses his Linux laptop and Nmap to see if there are any open ports on the system.

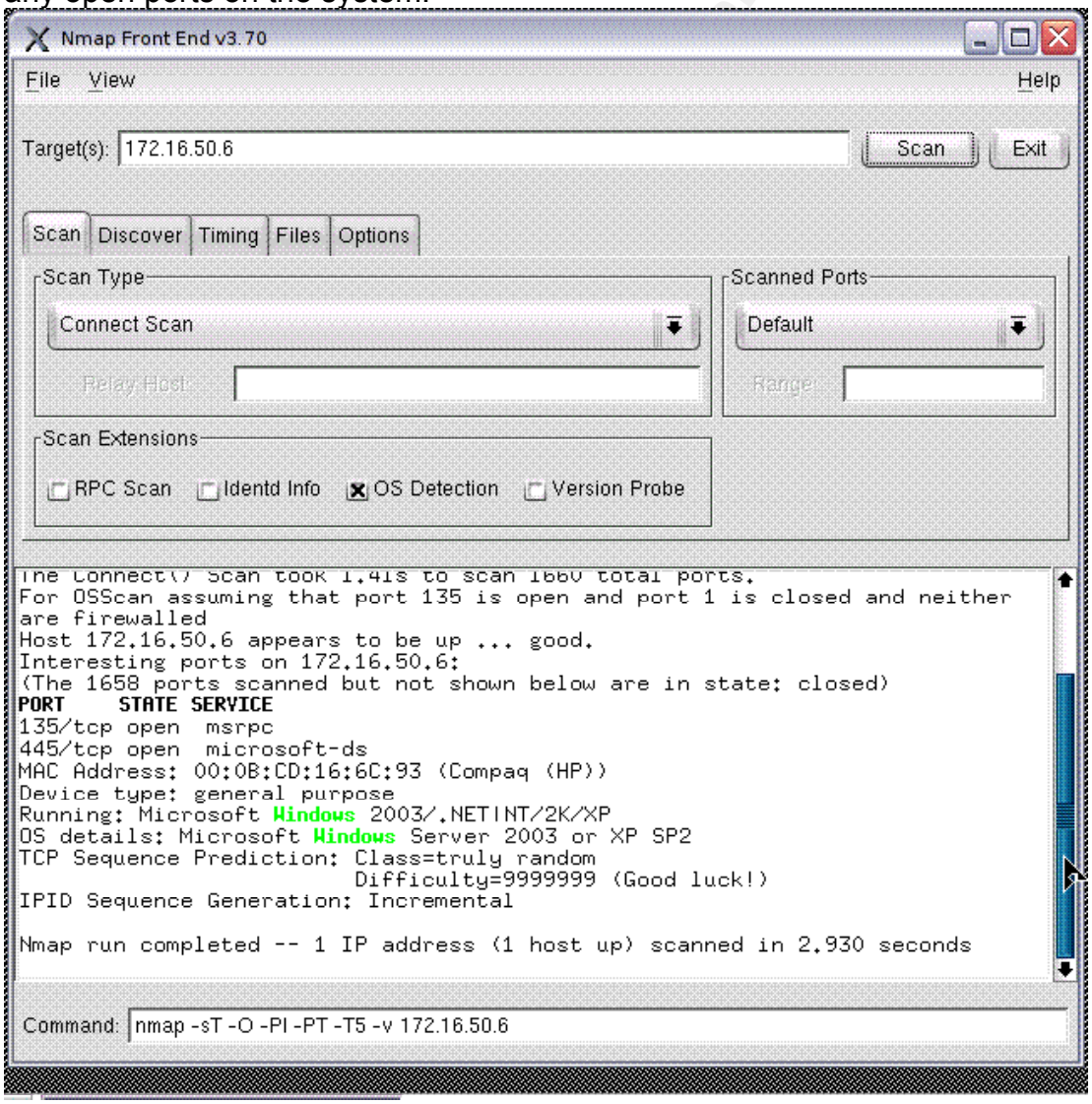


Figure 11-Nmap scan of Windows XP with no firewall

In this case, Mal sees that he can connect to Vic's computer by accessing the Microsoft File and Print Sharing service, which is enabled by default on all Windows XP machines. The output of Nmap wishes the user luck, as Windows XP does not offer a number of ways into the operating system itself. However, when you possess valid credentials, luck has nothing to do with it. The exploit of Vic's laptop can begin.

Since Mal has Vic's domain credentials which he learned from Vic's earlier access to the corporate sites, it is reasonable to assume that they can be used to access Vic's laptop. Mal uses his smbclient to remotely mount Vic's entire harddrive, as follows.

```
root@0[mal]# pwd
/home/mal
root@0[mal]# mkdirhier remote
root@0[mal]# smbmount //172.16.50.6/C$ /home/vic/remote/ -o
username=remoteuser,password=badpassword
root@0[mal]# cd remote
root@0[remote]# ls
AUTOEXEC.BAT            I386            Personal Folders.pst
BOOT.INI                imagestored     Platform.ini
BOOTSECT.DOS            IO.SYS          Program Files
COMLOG.txt              MSDOS.SYS       RECYCLER
CONFIG.SYS              MSOCache        System Volume
Information
DELL                    NTDETECT.COM    temp
DELL.SDR                NTLDR           WINDOWS
Documents and Settings  oracle          WUTemp
DRIVERS                 pagefile.sys    salesquote.xls
Customerinfo.doc        ras directions.txt
VLA keys.txt
root@0[remote]#
```

Mal is now able to access any file on Vic's computer. He can copy, modify, or delete information. Mal might first copy over the "Personal Folders.pst" file from Vic's machine. No doubt, there would be some emails in there that are interesting. Then Mal could check out Vic's "My Documents" for interesting bits of information, although some of the files at the root of C: look interesting too.

Mal might also remotely install files on Vic's machine, including software that will allow him to connect to Vic's machine later, when he is not on the same network as Vic.

For once, a patch can make up for poor configuration. Service Pack 2 for

Windows XP, by default, enables the Internet Connection Firewall on the client PC. If Vic was running the firewall in its default, the results of Mal's scan would be quite different.

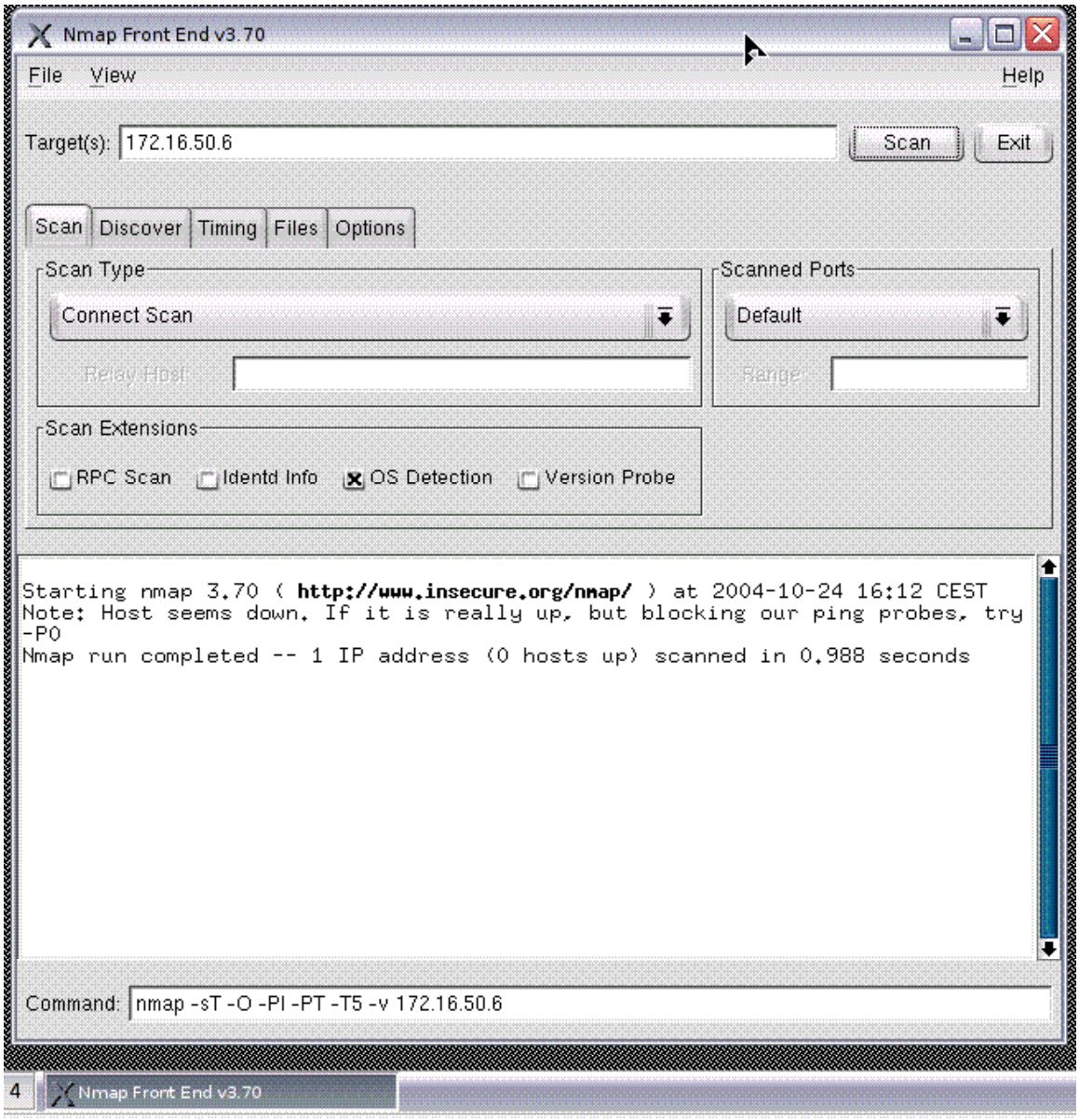


Figure 12-Nmap front end against XP firewall

The default in this case would serve Vic well. Of course, we would have to trust that Vic had not turned off the firewall in an attempt to troubleshoot some unrelated issue, but there would not be a way for Mal to exploit Vic's computer.

Many antivirus programs perform scans of all files written to the disk or read from the disk. If i/o scanning is in place, the antivirus program could prevent Mal from uploading to Vic's hard drive remote access programs or other programs recognizable by the a/v software as malicious. This is not a fool-proof method, as many remote access programs have fully legitimate uses and may

not be considered the a/v software as malicious.

Corporate Web Portals

Microsoft Exchange Outlook Web Access

Companies using Microsoft's Exchange can create a web portal, so that users can login using a web browser and access their email. This web portal uses Microsoft's IIS, and can run over http or https. Proper configuration of the IIS site is critical to ensure both that only authorized users can access the site, and that data confidentiality is maintained.

A default installation of Outlook Web Access only requires a compatible IIS installation, and connectivity between the web server and the Exchange server. Access is limited by requiring that users enter a name and a password that match a configured user of the system.

Secure communications can be setup by installing an SSL certificate for the OWA site on the webserver, but there is no facility to generate a default certificate, nor is there a requirement to explicitly permit insecure operation. It is regrettable that secure communications requires additional knowledge and effort.

Stronger authentication, including two factor, can be set up to work with OWA, but as with any two factor authentication scheme, this requires a compatible system, more hardware, and significantly more administrative work. A survey of one hundred OWA sites was performed. The sites were checked to see if they permitted http or https connections, and if https, whether the certificate was valid or invalid.

Search of www.google.com for websites containing the string "/exchange/logon.asp." The first 100 sites that were actual OWA sites were surveyed.

http	https with a valid* certificate	https with an invalid** certificate	total
84	8	8	100

*valid in this case means issued by a recognized CA, properly configured to match the name of the site, and with a valid date.

** invalid in this case means issued by an internal CA, issued by a valid CA but to a different name, expired, or some combination thereof. In other words, it would cause a web browser to display an error/warning about the certificate.

Table 1: Survey of OWA Sites

Citrix Nfuse Portal

Citrix offers an application portal accessible using a web browser and a downloadable client side component. Again, proper configuration of the website site is critical to ensure both that only authorized users can access the site, and that data confidentiality is maintained.

A default installation of Citrix Nfuse only requires a compatible webserver installation, and if a separate Citrix server or server farm is being used, connectivity between the web server and the Citrix server(s.) By default, access is limited by requiring that users enter a name and a password that match a configured user of the system.

Secure communications can be setup by installing an SSL certificate for the site on the webserver, or by implementing another component (licensed separately) called Citrix Secure Gateway. There is no facility to generate a default certificate, nor is there a requirement to explicitly permit insecure operation. It is regrettable that secure communications requires additional knowledge and effort.

Stronger authentication, including two factor, can be set up to work with Nfuse, but as with any two factor authentication scheme, this requires a compatible system, more hardware, and significantly more administrative work.

A survey of one hundred Nfuse sites was performed. The sites were checked to see if they permitted http or https connections, and if https, whether the certificate was valid or invalid.

Search of www.google.com for websites containing the string "/Nfuse17/logon.asp." The first 100 sites that were actual Nfuse sites were surveyed.

http	https with a valid* certificate	https with an invalid** certificate	total
94	4	2	100

* valid in this case means issued by a recognized CA, properly configured to match the name of the site, and with a valid date.

** invalid in this case means issued by an internal CA, issued by a valid CA but to a different name, expired, or some combination thereof. In other words, it would cause a web browser to display an error/warning about the certificate.

Table 2: Survey of Citrix Sites

For companies offering these services without proper configuration, there is a significant risk of compromise when remote users access these services over open wireless networks. Should that occur, unauthorized access will be easily gained, as will be shown in the following exploits. Recommendations for proper configuration that can mitigate these risks while still permitting access to these business critical services follow in the next section.

Recommendations

It will be tempting for security administrators to ban the use of wireless hotspots and assume that will take care of the problem. That is not the proper course of action. Instead, the insecure systems need to be configured so that clear text authentication is not permitted.

Then, remote users must be trained to access the systems securely. Wireless hotspots can greatly improve productivity, and when remote users have no other way to access the corporate network, there is little choice but to ensure that such access is done safely and securely.

The following recommendations may be helpful in establishing a more secure network that can still be accessible by remote users.

Policies

-Strong password policy
Although Mal compromised Vic's password, requiring regular changes can reduce the amount of time Mal has knowledge of legitimate credentials, and may help to identify that Mal had them if he continues to attempt using them once they have been changed.

-Regular application of patches to workstations and servers, including both operating systems and applications
Windows XP SP2 would have automatically turned on the client firewall, which would prevent Mal from accessing Vic's laptop hard drive.

-Mandatory use of antivirus software, with regular updates and weekly scans of all clients
This might prevent Mal from uploading remote access programs to Vic's computer, and/or logged Mal's access to data stored on the hard drive (depending upon the level of logging.)

-Regularly scheduled reviews of security logs
Diligent monitoring and observation of unusual access patterns might be able to detect the unauthorized access to the OWA and Citrix portals.

-Established company standards for server and workstation images, including a list of approved applications
Had the company standards specified HTTPS for all web based applications, and the use of VPN connectivity for all remote users, this incident would not have occurred.

-Regular inspection of all laptop computers to ensure that they remain in compliance with company standards
Much like requiring passwords to be changed regularly, this will at least reduce the amount of time a compromised system is running undetected.

-Baselines for all standard images, detailing file systems, running services, listening ports, and normal traffic patterns
Again, this is designed to make it easier to detect a compromised system should it exhibit unusual behaviors.

-Firewall policies that are based on "explicit permits" for both incoming and outgoing traffic, and that require investigation of all outbound violations
Compromised systems often attempt to "phone home" to the malicious user, in order to report that they are available for further exploit, to download more tools, or to receive instructions for the exploitation of other systems. If there is no reason for a system to use TFTP, and then it suddenly attempts to connect to an Internet site and download files, this is a sure sign that something is wrong. FTP, TFTP, HTTP, HTTPS, and IRC are all common protocols used by compromised systems to connect to external systems. DNS, ICMP, and other protocols, though less commonly used, can also be used. Companies should minimize what protocols can leave the network perimeter, and what systems are allowed to directly access the Internet. When violations occur, the offending systems should be carefully examined to determine whether the violation was caused by malicious code running on the system in question.

-The use of IDS systems both externally and internally
Even if firewall policies cannot be restricted, many remote access programs use recognizable protocols and strings of data. IDS systems can recognize and report on these.

-"Least privilege" access to all systems and data
No user should be given more access to any system or data then what they need to do their jobs. If Vic did not have administrative access to his laptop, Mal would find it very difficult to install software remotely to it. If Vic only had access to data required for his job, Mal would only have access to that data as well. However, if Vic was a domain admin with full access to all data on the network, Mal would also have that access.

Web based resources:

All web portals should be configured to use https communications. Https uses certificates to provide encryption of all data transmissions. Existing web sites can easily be setup to use https with minimum effort by obtaining a certificate, configuring the webserver, and changing any embedded links to use https instead of http. The reader is cautioned to consider carefully whether to deploy their own Certificate Authority or to purchase certificates from a commercial entity. For internal use, it is simple to use internally generated certificates, but unless you intend to install your CA as a trusted authority into every remote user's browser, you greatly increase the chances that your users may fall victim to a spoofing attack. WEBMITM (Web Monkey in the Middle) is

part of the Dsniff package, and can decrypt https traffic when acting as an intermediary between client and server. Of course, your user should be prompted that the certificate is not from a known authority, but if they are accustomed to seeing warning messages like this

Figure 13-Unrecognized Certificate Authority

every time they access the corporate portal they will not realize when their traffic is being intercepted.

Fifty percent of the OWA sites surveyed that used https were using self generated certificates. One third of the Nfuse sites surveyed were using self generated certificates. If Vic's company chose to use certificates generated by their own Certificate Server to secure both the webmail and Citrix portals, Mal would only need to set up a webmitm attack to gain Vic's credentials. In many cases, the resources may only be intended for employee use, and the cost of a commercial certificate is considered to be unnecessary. If a company's infrastructure supports the easy installation of an internal Certificate Authority as a Trusted Root, that is fine, but it may be less expensive in the long run to purchase commercial certificates for these services.

Two factor authentication:

Companies should also consider implementing two factor authentication for all remote access. Two factor authentication uses a combination of "something you know" such as a PIN, and "something you have" like a token or challenge/response card. By using two factor authentication, even when Mal captures Vic's credentials, they will not be exploitable because Mal will not have the second factor of Vic's credentials.

Figure 14-RSA SecurID for two factor authentication

VPN:

Companies should also consider whether corporate resources should even be accessible over the Internet. A VPN can provide encryption and a secure method to access the internal network, or a DMZ containing remote resources like OWA servers and Citrix servers. It is another step that the users need to perform before being able to access the resources, and may limit the accessibility of those systems, but VPN technology can provide secure network access even when using open networks. Depending on company policy, remote users may even be permitted to access personal resources, such as web browsing and personal email, while using the VPN, so as to extend that protection to them while on using a hotspot or other foreign network.

Portable system protection:

Companies should establish policies and procedures for the proper configuration of all portable computers. Unnecessary services should be disabled, and ports closed. Firewalls should be turned on and the users should not be permitted to disable them. Filesystem encryption should be used so that locally stored data is secure, even if the laptop is stolen from the user.

References

Open Citrix Nfuse sites www.google.com
http://www.google.com/search?hl=en&lr=&newwindow=1&q=%22%2FCitrix%2FNfuse17%2Flogin.asp%22

Open Outlook Web Access sites www.google.com
http://www.google.com/search?sourceid=navclient&ie=UTF-8&q=exchange%2Flogon%2Easp

DSniff FAQ monkey.org
http://www.monkey.org/~dugsong/dsniff/faq.html

OWA Deployment Guide www.microsoft.com
http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/depguide.mspx

Best Practices for Securing a Citrix Secure Gateway www.ccaheaven.com
http://ccaheaven.com/wps/Best%20Practices%20for%20Securing%20a%20Citrix%20Secure%20Gateway%20Deployment.pdf

Digital Certificate Facts www.thawte.com
http://www.thawte.com/ssl-encryption/digital-certificates.html

NIST Special Publication 800-48 www.nist.gov
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800.48.pdf

DD and Computer Forensics www.crazytrain.com
http://www.crazytrain.com/dd.html

Ghost Sector Copy www.symantec.com
http://service1.symantec.com/SUPPORT/ghost.nsf/docid/2001111413481325?Open&src=&docid=19

ICS ImageMASSter Solo 2 Forensic Unit www.ics-iq.com
http://www.ics-iq.com/show_item_186.cfm

Knoppix Security Tools Distribution www.knoppix-std.org
http://www.knoppix-std.org

Phlak Bootable Linux CD www.phlak.org
http://www.phlak.org/

Insert Bootable Linux CD www.inside-security.de
http://www.inside-security.de/insert_en.html