Castle or Cardboard: They know your system, do you know your enemy?
Chad Butler
December 10, 2001

Introduction:

Imagine for a moment that you get a call for an interview, go in, and get a new information technology job fresh out of college. One of the conditions for employment is that you will be part of a team whose new project is to do a corporate wide deployment of Windows 2000. You gladly accept this spot knowing that you've performed about 5 installations of Windows 2000 on your home network and since it's such a breeze to do at home you figure that this wouldn't be that much different. The deployment goes great and your team just happens to have the whole migration complete within two months. You go home for the weekend only to find out when you come in on Monday that you have a defaced corporate website and about half of the company's machines are being used in a Denial of Service attack on a government web server. As the fear for your new job sets in, you fall into the chair at your desk and wonder what you missed. This scenario might sound familiar if you happen to have heard the symptoms of some of the new viruses out in the wild. Situations like this can often come down to one simple question: Do you know exactly what's going on when you decide to put a CD into a company machine and click the setup button? Knowing what is being put on and running on a machine is important from an operational standpoint but it becomes even more important when security awareness becomes involved. In fact, many popular operating systems include many default installation options that open enormous security holes if not properly patched. With the evolution of attack trends and the sophistication of new exploits made publicly available, it is imperative that the information community know every inch of their systems and the enemies knocking on their doors.

Attack Patterns:

A common misconception in the business world is that when you install a software package on a company computer system, the system is secure. In a world where one vendor team developing the piece of software knew every hacker's methodology, every virus threat, and every social engineering tactic to be used against every organization in the near and distant future, this assumption would be a safe one. However, this world does not exist and without proper user training and proper security practices, any network connected to the internet has potential to both attract attackers and provide them a way in. There is a series of steps to a system or network compromise according to the "Hacking Exposed Methodology" which can provide a framework for helping the information world understand how a methodical attacker gets in and does what he wants. According to this methodology, these steps are: "footprinting, scanning, enumerating, penetrating, escalating, getting interactive, pillaging, expanding influence, and cleaning up." (Scambray and McClure, XXVI). Let's say, for instance, that after cleaning up the problem with the Windows 2000 incident, your company decides that they're going to do a little more work on their web site but the person in charge of the Internet Information Services web server running on your new Windows 2000 environment forgets to apply the latest service packs or hot fixes. Let's expand the popularity of this scenario by saying that the company you work for provides an internet bill payment service for financial institutions which moves large sums of money each day. Naturally, if your company had a website URL that told outsiders your company deals with money, an attacker could easily spot the company's website from a search engine and be enticed. Following this he would begin footprinting the organization by using whois requests, name server lookups, and other techniques to gain information about the structure of your network.

Figure 1: A whois request for Microsoft.com

```
Registrant:
Microsoft Corporation (MICROSOFT-DOM)
     1 Microsoft way
     Redmond, WA 98052
     US

     Domain Name: MICROSOFT.COM

     Administrative Contact:
          Microsoft Hostmaster (MH37-ORG) msnhst@MICROSOFT.COM
          Microsoft Corp
          One Microsoft Way
          Redmond, WA 98052
          US
          425 882 8080
          Fax- - - .: 206 703 2641
     Technical Contact:
          MSN NOC (MN5-ORG) msnnoc@MICROSOFT.COM
          Microsoft Corp
          One Microsoft Way
          Redmond, WA 98052
          US
          425 882 8080
          Fax- PATH
     Billing Contact:
          idNames, Accounting (IA90-ORG) accounting@IDNAMES.COM
          idNames from Network Solutions, Inc
          440 Benmar
          Suite #3325
          Houston, TX 77060
          US
          703-742-4777
          Fax- - 281-447-1160

     Record last updated on 08-Jun-2001.
     Record expires on 03-May-2010.
     Record created on 02-May-1991.
     Database last updated on 10-Dec-2001 11:00:00 EST.

     Domain servers in listed order:

     DNS4.CP.MSFT.NET 207.46.138.11
     DNS5.CP.MSFT.NET 207.46.138.12
     DNS2.TK.MSFT.NET 207.46.232.38
     DNS1.TK.MSFT.NET 207.46.232.37
     DNS3.UK.MSFT.NET 213.199.144.151
```

Since the attacker realizes that your company is running a web service that deals with money, he decides to focus his efforts there. The attacker then begins the scanning process by using a port scanner to see if there are any other interesting ports to attend to later. Next, the attacker uses a vulnerability scanner for web servers called whisker. Whisker tells the attacker that the web server hasn't been patched since before the Code Red worm attacks, so he tries malformed URLs against the web server. This allows him to traverse directories on the web server eventually allowing him to get a command prompt. The attacker realizes that he could perform a web page defacement but decides that this attack should carry more weight so pwdump is used to dump the system password files and then l0phtcrack, a familiar password cracking program used to test system password accounts for strength, to harvest system user passwords. The attacker logs onto the web server with one of the harvested administrator profiles. The network is probed using tools like Legion which "can detect unprotected or poorly protected shares." (Cole, 1.25) Tools like this allow the attacker to gain information about the network from the inside. The attacker realizes that all of the subscriber profiles that are using your company's service are stored in an SQL server on the local network and that the System Administrator password for this server was left blank (default). He then pillages this server harvesting all of the information about the subscribers including Social Security Numbers, user names, passwords, bank accounts, etc. While the attacker was probing the network, he saw that no other machines were logging communications so he clears the log files on the SQL server, defaces the web site, cleans up the log files on the web server, and exits without a trace.

This example was a shortened description of what an attack might consist of. I've often heard it said before that attackers begin their homework on potential targets months in advance. Adrian Lamo, a "clean-cut 20 year-old-hacker" ("Security Focus: Lamo's Adventures in WorldCom"), is one of these dutiful attackers who "gained national attention" for executing attacks against major corporations. The following quote from the Security Focus news clip illustrates what early-level footprinting goes into an attack.

> **The hacker makes his discoveries during marathon all-night sessions in front of his laptop. He scans Internet address ranges for undocumented Web servers, or uses well- known software bugs to find the names of private files on otherwise-public servers. Sometimes, he just guesses. At any given moment, Lamo has a long list of "interesting" Web sites he may or may-not look into further, depending on the vagaries of his ever-shifting curiosity.**

-("Lamo's Adventures in WorldCom")

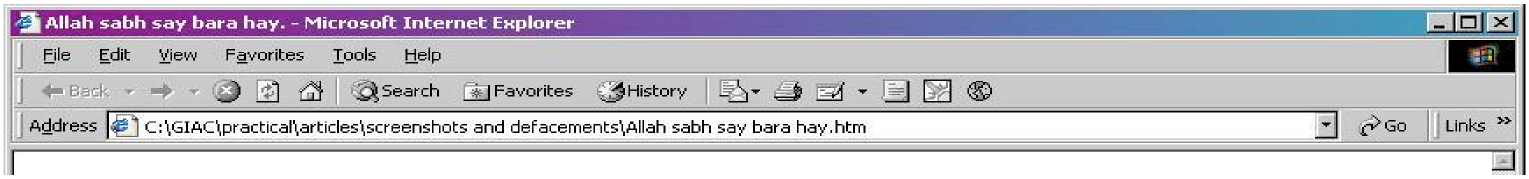
This message might make it seem that this "guessing" he does in order to find hidden web servers or other hidden machines is a difficult task. However, there are many tools that make jobs like his easier. For instance, nmap has a command line switch that allows an attacker to get an estimate at what operating system is running on the remote machine and how easy it would be to predict the sequence numbers of individual packets. This could be very handy if the attacker was looking for operating system specific exploits. The article states that Lamo uses a program called “proxy hunter” to locate proxy servers that he hopes would be configured improperly, allowing him access to the private network. If a proxy server is found and it is, in fact, configured improperly then all an attacker would have to do is configure a web browser to use the server and the inside network would be completely visible to him.

Evolving Trends:

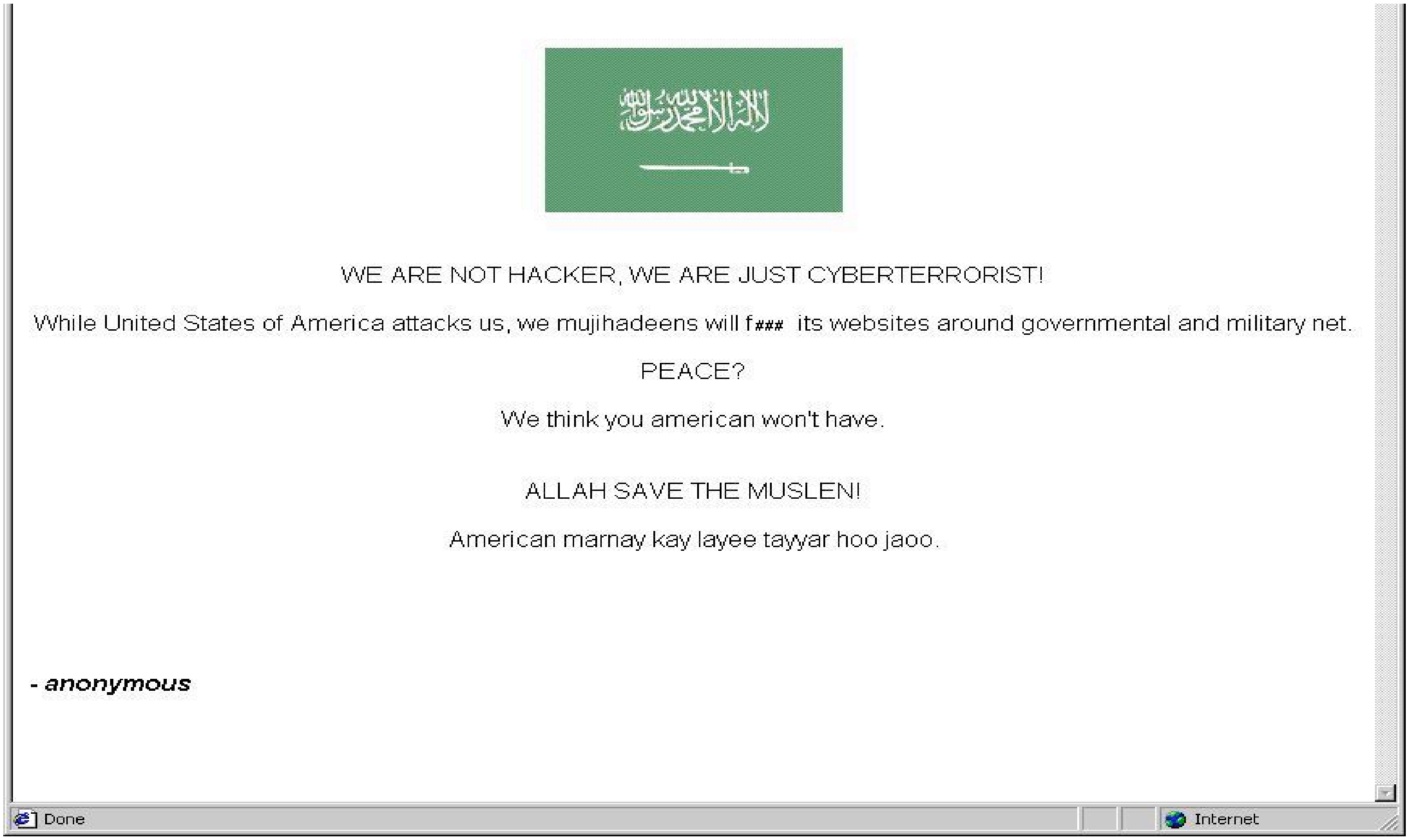
With the advent of newer operating systems, precautions are being taken and new strategies developed to try and neutralize some of the threats that have evolved from the past. One such strategy on the operating system level was to make sequence number prediction more difficult by randomizing the sequence numbers traded on a packet by packet and connection by connection basis, thus decreasing the probability of attacks like session hijacking. Another example might involve developing a product with a plug-in architecture so that customers might be able to download secure updates in a packaged form and easily install them into the product making it more secure in an emergency situation. Encryption has become a hot topic effectively making it hard for attackers to even make sense of your data if they were effectively able to get into your network. As data gets more sensitive, the encryption algorithms have begun to get stronger and the keys more complex. On the perimeter security side, Internet Service Providers have begun to provide ingress filtering services so that packets perceived to be of a malicious nature are dropped before even reaching a network. Routers and firewalls can perform stateful filtering and application layer analysis. This prevents data hidden on a higher level of the TCP/IP stack from reaching inside to more sensitive systems.

However, as new technologies are developed to thwart attackers, their methodology is becoming stealthier and more malicious. For instance, the old style of manually dialing phone numbers to locate a modem to dial into is quickly evolving into a world of automated reconnaissance and more widespread damage. Web server defacements and Denial of Service attacks are becoming more widely observed. Attackers have also began using a new type of attack in which they can take control of a large number of systems in different geographical locations and use all of them to push large amounts of traffic at a server trying to make it shut down. This is known as a Distributed Denial of Service attack and is now being employed by a number of recent worms. Within the last few years, the security world has seen the appearance of automated network scanning programs like nmap or nessus. Nmap and a host of other port scanning programs can be used to scan a machine over all TCP and UDP ports for listening services while guessing the operating system, using decoys, and many other features. Nessus is a popular freeware program that can be used to scan a host to identify holes against a long list of vulnerabilities. Nessus can then prepare a report giving the attacker a good idea of where to start their attack. Even more dangerous and revealing are the mass mailing worms and viruses that install Trojans or upload password files from infected machines to a site or email address of the attacker’s choice. The recent Badtrans worm was an example of such a worm. It was able to install a key logging Trojan on an infected machine, allowing it to capture network passwords as well as a host of other private data that was then mailed back to one of several addresses.

The evolution of operating systems and tools against systems is not where the fun stops. The trend of curious browsing is changing rapidly into one of malicious abuse and information warfare. The government believed after the September 11, 2001 attacks on the United States, that one of the next targets would be our nation’s computer and telecommunication systems. Most, if not all, organizations in the United States have data that is vital to their organization from the inside and could be abrasive if it was to fall into the wrong hands. Adrian Lamo, through his adventures within company networks, has gained access to documents and websites considered highly classified that could possibly bring these companies to their knees. At WorldCom, he was able to obtain a classified network diagram that showed a large amount of internet backbones as well as specific configuration details on many critical links like the one connecting an AOL Mexico office and its Virginia offices. Even more alarming was the fact that he could use the human resources machine to get employee names and social security numbers for most, if not all of WorldCom’s 86,000 employees. If he could obtain the employee’s birthday, he could get into their personnel account containing salaries, direct deposit instructions, and bank accounts. Now, what if this information was obtained by a foreign attacker working for a non-ally nation’s government and the information weren’t salary details, but nuclear weapon schematics or the President’s personal agenda? Two government organizations of national interest may have recently disclosed some of this type of information. In an article on the Symantec Security Response website explained the abuse of a group that broke into the “NOAA Office of High Performance Computing and Communications, as well a Web server operated by the National Institute of Health's National Human Genome Research Institute.” The defaced websites displayed a similar banner message at the bottom of the page that read “Americans be prepared to die” and the attackers threatened “the greatest cyber attack against American government” on one of the sites. When a U.S. Army Research site was attacked, the defaced website had a greetings section that listed a hacker group responsible for October attacks on Department of Defense sites.("'Mujihadeen' Hackers Take Out U.S. Government Sites")


Allah sabh say bara hay. - Microsoft Internet Explorer

Address C:\GIAC\practical\articles\screenshots and defacements\Allah sabh say bara hay.htm



WE ARE NOT HACKER, WE ARE JUST CYBERTERRORIST!

While United States of America attacks us, we mujihadeens will f### its websites around governmental and military net.

PEACE?

We think you american won't have.

ALLAH SAVE THE MUSLEN!

American marnay kay layee tayyar hoo jaoo.

- anonymous

Figure 2: Defacement of NIH site by Mujihadeen

With this kind of attack activity looming on the horizon, what is our nation doing for defense? According to an article on Symantec Enterprise Security's website, the Bush administration has come to a decision for a $218 million "Advance Technology Program" to increase security measures against cyber-crime, child pornography, and intellectual theft issues such as software piracy starting in 2002. In comparison, another article stated that the Computer Emergency Response Team Coordination Center also predicts that in the coming year we can expect the amount of cyber-attacks to double what they were last year. This estimate would push the attack count to over 40,000, all with the potential to "bloom into serious threats similar to the Code Red or Nimda worms." ("Record-breaking Year for Computer Security Incidents Expected") It is also stated that the vulnerabilities exploited by worms like code red and nimda were common to about 80% of all organizations, and the "Internet worm attacks have cost companies more than $10 billion in repairs and lost productivity." ("Record-breaking Year for Computer Incidents Expected") As these figures detailing compromised organizations and the number of outbreaks of extremely malicious viruses continue to grow, it can quickly be seen that the unaware user or organization becomes a mere bystander in the war for the web that is fought daily by the white hat and black hat communities.

Defensive Maneuvering:

According to the SANS Institute, there are 3 keys to "defense in depth" which is the ability to be intrusion tolerant. Intrusion tolerance is achieved if an organization's resources are confidential, available, and remain unchanged in their integrity. An attacker's goal is to disrupt these characteristics in order to reflect the compromise of an organization. **Confidentiality** is the ability of data to stay safe regardless of the circumstances. If an attacker was able to intercept network traffic, would the data gathered be in a form that would allow him to read the deepest and darkest secrets of your organization? The second key, **integrity**, refers to the ability of data to remain unchanged without your permission. If an attacker were to break into your network and install a rootkit in your file system, would you notice? And last is the **availability** key which is the ability of data and other network resources to be ready for use by individuals on your network. Defense against the growing internet threat can be complex and must be as methodical and well thought out as the attacks themselves.

In order to understand how to best defend against attackers, it is necessary to understand what information an organization is trying to protect. A pictorial representation of the SAN'S Institute's "defense in depth" concept which shows the layers surrounding an organization's core (or critical) data is the "onion model."(Security Essentials II, 1.35)

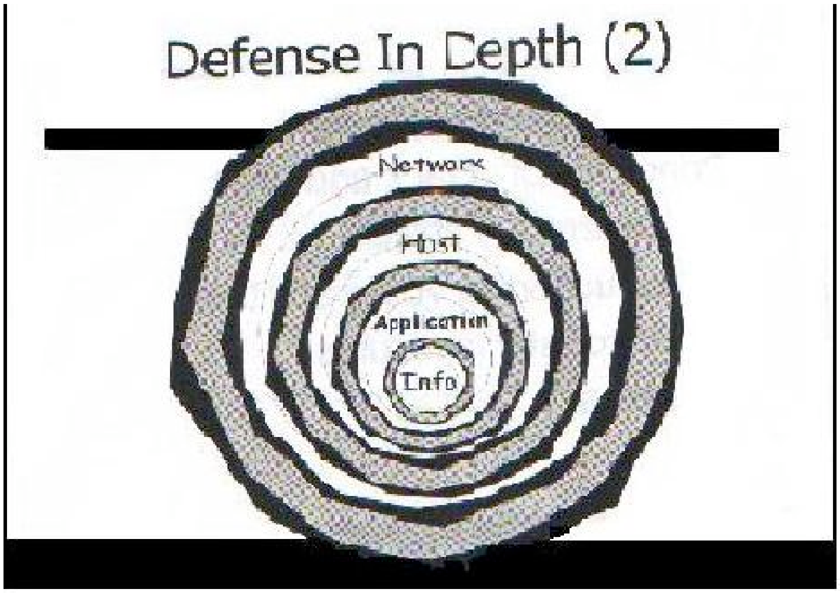


Figure 3: The Onion Model

It can be seen that the “info” that is at the center of the onion is the assets the organization is trying to protect. The application layer exists outside the information layer. This layer interacts with the information and is the interface for the systems on the network. The next layer is the host layer and finally the network layer. The attacker would have to penetrate all of these layers in order to perform a full compromise and retrieve the vital information.

At the heart of any well thought out defense strategy resides a plan, or more specifically a security policy. Good security policies are made of many different aspects which can include things like Purpose, Related documents, Cancellation, Background, Scope, Policy Statement, Action, and Responsibility. (Kessler, 2-5) Policies exist at many different layers of an organization. This is important in decisions about the scope of the policy that is being written. The most important thing to remember, however, is that a policy is a focused document that must be consistently reviewed on a regular basis and must be as dynamic as the corporation it’s being written for. Policies must cover things like responsibilities of individuals, actions to be taken, emergency situations, etc. as they relate to the organization. Many good resources exist on the internet for writing good security policies. http://www.sans.org/newlook/resources/policies/policies.htm provides model security policies by the SANS Institute.

Once a good plan is put into place, the actual design and implementation of the layers of the defense can begin. Due to the high amount of attacks from the internet and the harsh numbers expected in the future, many options are being explored by service providers, such as the ingress filtering mentioned above, as a way to hopefully prevent attacks from reaching the customers' networks. However, when thinking about security, an organization or individual must always count on the attacker reaching their front door. The first layer of defense exists at the perimeter of the network and can be a device like a filtering router, a firewall, or a proxy server. Many configuration options are provided on these devices to do actions such as address translation which permits users on the inside to only see an internal address and attackers from the outside to only see an external address. This helps an organization by making it appear that all traffic is coming from one host. In addition, some firewalls can be configured to only allow packets into the network that have a proper reverse DNS record (that is, the IP address and the domain name the user appears to be coming from match up). The next layer of defense could possibly be a network intrusion detection system (NIDS). Many NIDS exist that allow intrusion analysts and individuals to analyze packets and the data contained in them for attack signatures coming to the network. One way to analyze these signatures would be to place one monitoring interface from the NIDS on the external line coming into the network and then another monitoring interface on the line going to each of the core resources as defined in an organization’s security policy. This allows an organization or individual to ensure that the proper patches are applied to their network and can help tune the defenses further.

Honeypots are another helpful way to learn about attackers. A honeypot is a computer that is fashioned in such a way that it encourages attackers to attack it. These systems can be set up with logging mechanisms and change-monitoring applications designed to record the attacker’s tracks throughout the attack. These can be used as distractions for the attacker while at the same time gathering information to help you better tune your defenses. Caution must be exercised if using honeypots because attackers view the presence of these as offensive and may decide to attack your network harder or get their buddies to do so if they discover you’re using them.

At the next layer of defense lies the host. By the time an attacker gets to the host, he would be able to perform many more devious and damaging tasks. If the host was a server, the attacker would not only be a “paper-thin” line close to possible “core” data but he would also be able to enslave the host and use it to attack other systems on the organization’s network or as an availability attack on another network. A proper thing to do at the host level would be to run services and programs that will monitor things like the windows registry, password files, the file system, etc. A popular host-based program that can monitor these aspects of a system is a Host-based Intrusion Detection System (HIDS). Many NIDS and HIDS exist for administrators to use. One popular freeware NIDS is Snort and some famous HIDS are Tripwire for Windows and UNIX variants as well as TCP Wrappers and Psionic Port Sentry. Psionic Port Sentry and TCP Wrappers run on UNIX variants and monitor incoming connections. If set to certain modes these programs can automatically respond to the requests by blocking the route back to the attacker and drop the address into deny files effectively "black holing" the offensive machine. At the application and info levels, there are also many options in the encryption field that can make data retrieved by an attacker very difficult to decipher. This may hopefully deter the attacker by making them think reading an organization's "core" data is going to be more trouble than it's worth. Encryption can be seen almost everywhere, even in common channels used on the internet. For example, any time eCommerce is taking place with a "noteworthy" organization on the internet, encryption is used to protect the data during the transaction (i.e. a credit card number or order form). Some common protocols like telnet and pop3 transfer user names and passwords in plain text. Reasons like this make the need for strongly encrypted cyphertext and channels in an organization's communication essential. A popular freeware encryption product for encrypting files and folders is PGP or Pretty Good Privacy. PGP uses what's called a public/private key pair architecture which means data that is encrypted is done so using the sender's key as well as the public keys of the recipients chosen. When the encrypted cyphertext is received, the receiver must have the private key in order to match up the public and private keys and decrypt the message. The keys used in this program are 2048-bit keys which provide strong encryption which at this point has not been broken. An important point to remember about encryption is that the strength of the cryptography used is not determined by the strength of the algorithm but by the strength of the key. Encryption can be a complex "process" to implement and it is recommended that proprietary methods are avoided and that the cryptosystem is thoroughly tested and understood before using it as a permanent solution.

Some other suggestions to keeping an organization's network and systems secure are to keep obtaining log files on servers and workstations and regularly auditing the network using the tools the attacker might use. Security vulnerabilities can be found on a day-to-day basis and having these open will lead to a greater risk of compromise. If an attack is successful on an organization's network, log files may be the only convincing evidence pointing an organization toward the real attacker. Using tools like host-based and network vulnerability scanners such as **nmap** and **nessus**, password cracking programs like **LC3** (or l0phtcrack v.3) and **crack** for UNIX variants, and a host of other tools may ensure that no new vulnerabilities show up that you are not made aware of. Keeping these tools up-to-date ensures that the network is being tested with the latest developments in the security industry and can ensure that the security policy of the corporation is being followed and not taken advantage of. I've been told that if a password can be obtained from a password file using a cracking program in less than two weeks; the password is not strong enough.

I mentioned above that many resources concerning security policies exist on the internet, however, there are many resources that can help an organization plan their defense and keep up-to-date with the latest vulnerabilities and fixes in the security world. "Hacking Windows 2000 Exposed" offers some tips to developing a good strategy for defense that can apply to any environment. Their "Basic Security Practices" include:

- Block everything that is not explicitly allowed.
- Always set a password, make it complex, and change it often.
- Keep up with vendor patches-Religiously!
- Authorize all access using least privilege.
- Limit trust.
- Be particularly paranoid with external interfaces (Dial-up, too!)
- Monitoring, Logging, Auditing, and Detection should be enabled.
- Plan an incident response capability, Business continuity
- Technology will not protect you from social attacks.
- Develop a security policy, get management buy-in, and distribute widely.
- Perform Real-World risk assessment.
- Learn your platforms and applications better than the enemy.

(Scambray and McClure, 4)

It seems that some of these may seem like they're being driven into the ground by repetition, but they must be stressed and must be continuous over many different security circles. This is to prevent confusion in planning, implementation, and maintenance and facilitates the sharing of information and distributed defense. One last thing that must be remembered is that many organizations still do not know or care about security of their networks and probably will not until they are attacked and taken advantage of. Standard security practices will hopefully turn the tables and place security officers finally ahead of the attackers. Until that day arrives, the most important thing to remember is that there is no such thing as a completely secure network, only a hardened one, and that we must always stay as up-to-date as we can and share our findings to put the "white hats" back in the battle and defend our territory.

References:

Cole, Eric, et al. *Sans Security Essentials I: Internet Threat Brief*. v.1.6. (c)Sans.org. Aug. 10, 2001.

Cole, Eric, et al. *Sans Security Essentials IV: Encryption and Exploits*. v.1.4. (c)Sans.org. Aug. 10, 2001.

Ferrie, Peter. "W32.badtrans.b@mm." Dec. 10, 2001. http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html, Dec. 20, 2001.

Kessler, Gary, et al. *Sans Security Essentials II: Network Security*. v.1.3. (c)Sans.org. Aug. 10, 2001.

Krebs, Brian. "Bush Signs Spending Bill with Cyber-Security Funding." Newsbytes. Article ID: 961. Nov. 29, 2001. http://enterprisesecurity.symantec.com/content.cfm?articleid=961&PID=9637730&EID=0. Dec. 22, 2001.

McWilliams, Brian. "'Mujihadeen' Hackers Take Out U.S. Government Sites." Newsbytes. Article ID: 962. Nov. 30, 2001. http://enterprisesecurity.symantec.com/content.cfm?articleid=962&PID=9637730&EID=0. Dec. 22, 2001.

Poulsen, Kevin. "Lamo's Adventures in WorldCom." Dec. 5, 2001. http://www.securityfocus.com/news/296. Dec. 22, 2001

Scambray, Joel and Stuart McClure. *Hacking Windows 2000 Exposed*. Berkeley: Osborne/McGraw-Hill, 2001. XXVI, 4, 5, 6.

Verton, Dan. "Record-Breaking Year for Security Incidents Expected." Computer World. Article ID: 954. Nov. 26, 2001. http://enterprisesecurity.symantec.com/content.cfm?articleid=954&PID=9637730&EID=0. Dec. 22, 2001.