Network Management and Security

Network Management

The creation of new networks or the modification of an existing network is the every day work of networking professionals. Management will select the least expensive technology that will meet user needs. Networks are never static, they are continually changing to the needs and goals of the organization and personnel over time. Today, we are building much larger networks than can be easily managed. For example, even a midsized company can have 500 Ethernet switches and over 100 servers.

Cost and Decision Making

In networking, cost is a major constraint. User demand can never keep pace with corporate budgets. To aid in understanding how network changes can affect performance, management uses simulation tools like Riverbed Academic Modeler, which we are using in this class. There is never enough money to meet all user demands; management must make rational decisions and decide which product is best for the organization. To aid its decision making, management will use a Weighted Criteria Table. All products, under consideration are written at the top of the chart. Each product is measured by the same criteria. The latter are subjective elements that management wants to compare the products by: such as cost, ease of installation and ease of use.

		Product 1		**Product 2**	
Criteria	**Weight**	**Rating**	**Points**	**Rating**	**Points**
Price	5	10	50	8	40
Ease of Installation	4	7	28	5	20
Ease of Use	3	6	18	8	24
Total			96		84

Table 1: Weighted Criteria Table

In the table above, each criterion is given a weight from 1-5, 5 being the most important and 1 the least important factor to management. Then the products are rated by each criterion on a scale from 1-10. For example, product 1 has a price rating of 10 and product 2 has a rating of 8. This means that product 1 has a lower price than product 2, and thus a higher score. The rating for each criterion is multiplied by the weight to create a value. The total of all values will lead to the best product. We can see that product 1 has a higher value that product 2, so management should purchase product 1 because it has the lowest price, and is easier to install than product 2. The latter has a higher ease of use, but management ranked ease of use a lower priority than price and installation. Using this method of decision making, management can quantify a subjective choice.

Once a product has been selected, it is managements responsibility to provide a multi-year budget to meet the network plan. Network projects have large capital outlays in some years and small outlays in others. The network administrator must constantly monitor the network and select the projects to keep the network up to date over time.

Service Level Agreements (SLAs)

Users and consumers expect quality of service (QoS) today. The days of slow speeds, long delays and frequent power outages will no longer be tolerated. Consequently, when companies deal with service providers, such as cloud or web hosting services, they seek a written contract specifying the level of service expected. If the supplier is unable to meet the contractual minimum then a performance penalty will be paid to the company. Some firms are even beginning to require SLAs as a performance measure for internal network staff. The two most common SLAs are speed and latency. Networks SLAs will have a stated speed that must be met a specific period of time, such as 512 Mbps 99% of the time in one year. This means that the service provide can fail to meet this standard for approximately 31/2 days out of a year without triggering a penalty. Latency deals with delays which can be aggravated by congestion. Latency greater that 15 ms can prevent real world applications, like VoIP, from working correctly. Thus, companies will seek a SLA where latency can not exceed 15 ms, 99% of the time over a year.

In addition to maintaining the network infrastructure and SLAs, managements main responsibility today is security. Regardless, of the industry today, all companies are primarily concerned with "data processing". Protecting the collection, storage and retention of data on the network is necessary for management to make timely and relevant decisions.

Reasons for Network Security Failures

Reasons for network security failures are many, but the majority of all failures are the result of human beings. For example, a hacker sends a system alert email to all employees of a company at 4:50pm which looks like it came for the IT manager's email account: "System maintenance in progress. All servers will reboot in 2 minutes, please log in and reboot your computer to complete the process". This is an actual social engineering attack playing on the ignorance of users. An IT manager never needs users to login and reboot to complete system maintenance. Another example is "piggy-backing" where an intruder waits at a secure door (usually complaining that he/she has a job interview, but has lost the access code) waiting for someone to let him/her in or scoots in before the door closes and the user is unaware that an authorized person has entered the building. Again, training can prevent this by entering a special code into the door keypad to alert security that an authorized person is attempting to gain access.

The second major reason for security failures is poor assumptions. This is particularly true with programmers; they make assumptions about how the application will be used and the type of data to be entered by the user. Overly trusting the input can lead to SQL injection or buffer overflow attacks. Best practice is to create a "choke-point" in your application where all input, regardless of source, file, environment variable, library, is checked and validated before used. This can be done using simple regular expressions, stored procedures and string safe libraries.

A third reason for security failures is hardware and/or software misconfigurations; the latter are more likely to occur if the server is a multipurpose server with data and code running on the same machine, as a small local business. Modern network design uses a 3tier approach. The user enters data into an HTML front end server which communications via sockets to an application server and data base servers. Using sockets is more secure because unless the data entered is in the format and length expected by the stored procedure, on the application server, the function call will fail. Network administrations must be aware of known vulnerabilities in software and patch regularly to avoid network exploits.

Note: A vulnerability is a known weakness in the software that could be taken advantage by malicious individuals

An exploit is a tool designed to take advantage of a known vulnerability. A network break-in is also called an exploit.

Servers for example should only run the services necessary to get the job done. For example, the windows print spooler service, which runs with system privilege, is a primary target for hackers. Taking over this service gives them system privilege on the local machine. A server which mistakenly has this service running then has an "increased foot-print" for attack. Software applications must work with system software and the combination of applications and operating system versions can lead to configuration vulnerabilities, such as the PDF file vulnerability. The main vulnerability today is application software where the developer overly trusted that users will input data in the format and length expected.

Reasons for Security Failures
• Human Factors (love, greed, extortion, ignorance) • Poor Assumptions (overly trusting on data input) • Hardware\Software Misconfigurations (system\application software) • Poor Policy Guidelines

Table 2: Summary table of Security Failures

Lastly, security failures occur when management sees security as a "technology" problem and not a "management" problem. Management must take security seriously and provide a "top-down" approach to creating a security policy. The latter must be comprehensive, relevant and consistent. You can't have a little security; it must be comprehensive and include all aspects of company behaviours, from logging into the network, the storage of sensitive information, the use of company technology and how to respond to suspected exploits. Security is a management problem balancing the privacy needs of the user with the needs of the organization. While the media makes "big news" about a network break-in, these are relatively rare. Companies are more likely to be attacked by disgruntled employees, than by outsiders. For example, in a recent IT study, only 28% of Canadian companies do hardware/software updates on a regular basis. This means most Canadian businesses have PCs which can be exploited by malicious employees or hackers to steal trade secrets or create DoS (Denial of Server) attacks.

Moreover, CERT (Central Emergency Response Team) which is a clearing house of vulnerabilities has researched network exploits and discovered that 85% of all network break-ins are the result of poor passwords. Therefore, to improve network security all businesses should require changing passwords on a regular basis and employ password complexity rules, such as not using English words, combining upper case and lower case characters with numbers and meta characters. Every change in an alphanumeric password increases the complexity exponentially by about 70 times. As Table 3 below indicates the difference between an at character password with same case is 8^{26}; this is a weak password which can broken in about 5 seconds. However, an 8 character password with mixed case and meta characters is 8^{78};[1] this password would take approximately 9 hours to crack. Complexity rules need to be combined with a password history, which prevents users from using a previous password. The number of previous passwords can be set by the system administrator.

Password Type	Exponent	Permutations
4 numeric pin	4^{10}	10,000
8 character same case	8^{26}	302231454903657293676544
8 characters mixed case	8^{52}	9.1343852333181432387730302044768e+46
8 character mixed case and numbers	8^{62}	9.807971461541688693493420973762e+55
8 character mixed case, numbers and meta characters	8^{78}	2.7606985387162255149739023449108e+70

Table 3: Password strength based on type of characters

Management is responsible for setting policy guidelines and standards for everyone in the company to do their job in a secure manner. Guidelines are regulations that should be followed, but are not mandatory. Standards are regulations which must be followed and are usually paired with corresponding penalties for non-compliance. The enforcement of the policies is security management.

Security Management

With the increased use of the Internet, network security has become more important. Currently, network administrators often spend more effort protecting their networks than they spend on the actual setup. They must make the following determinations:

- Who will have access to data?
- What resources will users have access to?

[1] An excellent web site is https://howsecureismypassword.net/ which indicates the time it takes to crack a password.

- When will users access the resources?

These questions evolve around different levels of trust. Every network is divided into “trust” spheres. The most trusted are network resources in an organization such as internal servers, domain controllers, and storage devices. Only a limited number of well-known people should have access to these devices. Below the most trusted is the less trusted sphere. This category includes internal users and remote, authenticated users, and servers in a DMZ (A de-militarized zone is a separate subnet which contains only public servers). On a certain level, an organization must trust its users, internal or remote, in order for them to perform their jobs. Despite the trust granted to them**,** some people in an organization will abuse the trust and do malicious things. Statistically, you are more likely to be harmed by an internal user than an external hacker. Although most employees can be trusted, the actions of the minority, who abuses its privilege, places this group in the less trusted, not most trusted category**.** The least trusted (sometimes referred to as untrusted) resources and users are Internet servers and remote, unauthenticated users. You can never trust this group because you cannot sure of their intentions.

Plan Protect and Respond

Management of security involves three functions: Plan Protect and Respond. Management cannot protect a network unless it understands the “threat environment”, the types of attacks and attacker methodologies. Planning involves understanding the goals of the company and what assets need protection and developing a comprehensive security policy which includes all aspects of the company and network. Protection involves the ongoing protection of the network from firewalls, to account and access control; for highly sensitive data, it could involve cryptography as well. Even the best efforts to protect a network will result in breaches from time to time. Respond dictates how management handles the compromise, from detecting and stopping the attack to prosecuting the attacker. The threat environment feeds into the process and as it changes, management must make changes, completing the cycle.

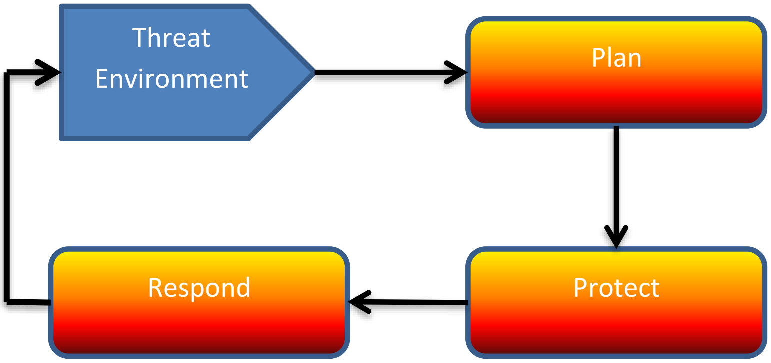


Figure 1: Plan Protect Respond of Security Management

Planning Protect Respond involves three interrelated factors:

- Planning: Risk Analysis
- Protect: Defense in Depth
- Respond: Comprehensive Security Policy

Planning: Risk Analysis

Risk analysis involves assessing the cost of an attack with the protection required. The goal is not to eliminate risk, but to lower it to manageable levels. Good management requires that if the cost of the counter measure is greater than the lost from an attack, then management should not implement the counter measure. Risk is the value of the assets lost X the probability of a loss.

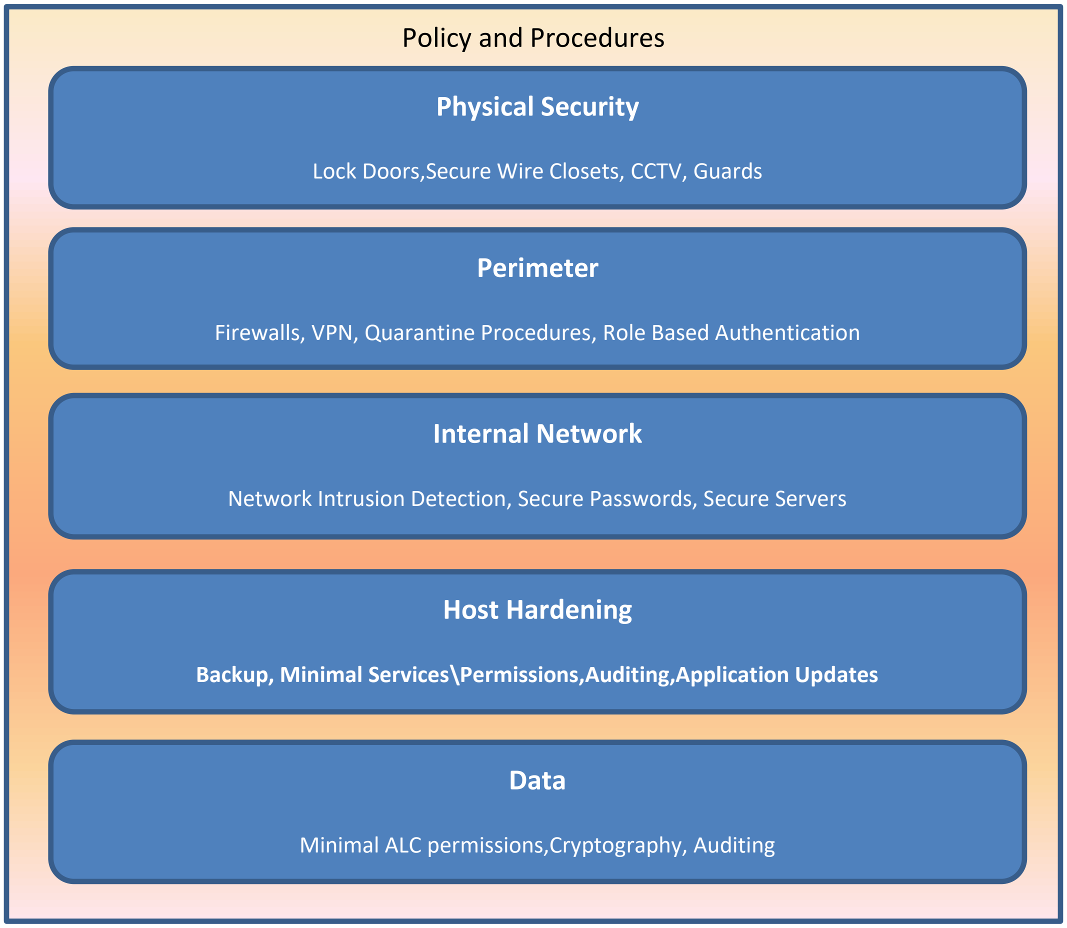
In the example below, the probability of a loss, 20% is equal for all three counter measures. The total cost to the company if an attack was successful was %500,00 for Counter Measure A and $1,000,000 for Counter Measures B and C. The annual probability of lost is the value of the loss multiplied by the frequency of the loss. This creates an annual probability of loss of $100,000 for Counter Measure A, and $200,000 for Counter Measure B and C respectively. Now management compares the cost of implementing a counter measure which is $25,000 for alternative A , $25000 for alternative B and $50,000 for alternative C. Subtracting the value of the counter measure from the Annualized probability of loss allows management to make a quantitative choice as to whether to implement the Counter Measure or accept the risk of not implementing the counter measure. From the table Counter Measure B should not be implemented because the cost is greater than the loss. On the other hand, Counter Measure B and A should be implemented immediately because of positive savings of $250,000 and $75, 000 respectively should a lost occur.

Description	**Counter Measure A**	**Counter Measure B**	**Counter Measure C**
Success Attack Damage	$500,000	$1,000,000	$1,000,000
Probability of an Attack	20%	20%	20%
Annual Probability of Loss	$100,000	$200,000	$200,000
Cost of Counter Measure	$25,000	$250,000	$50,000
Net Counter Measure Value	$75,000	-$50,000	$250,000
Implement Counter Measure	Yes	No	Yes

Table 4: Security Management Cost Comparison Table

Protect: Defense in Depth

Defense in depth means that there a multiple layers of network security so that even if an attacker breaches one level there is another level protecting the network and may prevent the attack from succeeding. Defence starts with physical security locked doors, secure cable closets, CCTV, guards, etc. Physical security is always the best form of security and the cheapest form when incorporated into the design of a network or building. If an attacker overcomes physical security, then the perimeter of the


Policy and Procedures
Physical Security
Lock Doors,Secure Wire Closets, CCTV, Guards
Perimeter
Firewalls, VPN, Quarantine Procedures, Role Based Authentication
Internal Network
Network Intrusion Detection, Secure Passwords, Secure Servers
Host Hardening
Backup, Minimal Services\Permissions,Auditing,Application Updates
Data
Minimal ALC permissions,Cryptography, Auditing

network is still protected by a firewall, quarantine procedures, or Virtual Private network (VPN). The next layer is the internal network which is protected by breaking the network into isolated segments and using network intrusion software to detect and attack. Inside the network, each host should be "hardened" by eliminating unneeded services to make the attack footprint as small as possible, installing anti-virus and spyware software, and auditing the frequency of key events such as the number of unsuccessful login attempts. Login servers should be physically secure and passwords should be complex and changed frequently. Inside the host, each running application should be hardened by making sure that all critical updates have been installed. Lastly, the date of each host should be backed up regularly and ACLs, should be set to the minimum required for each user to do his/her job. Policies should be based on role based authentication; this means that users are organized into groups based on their job responsibility, such as administrators, backup operators, or users. Members added to the group inherit the rights and privileges of the group. Users can also delegate responsibility to other users to the level of permission they have been assigned. These groups are mandatory and each user account must be associated with a functional group. User permissions are organized into Access Control Lists which are set to the minimal level of permissions for a user to do his/her job.

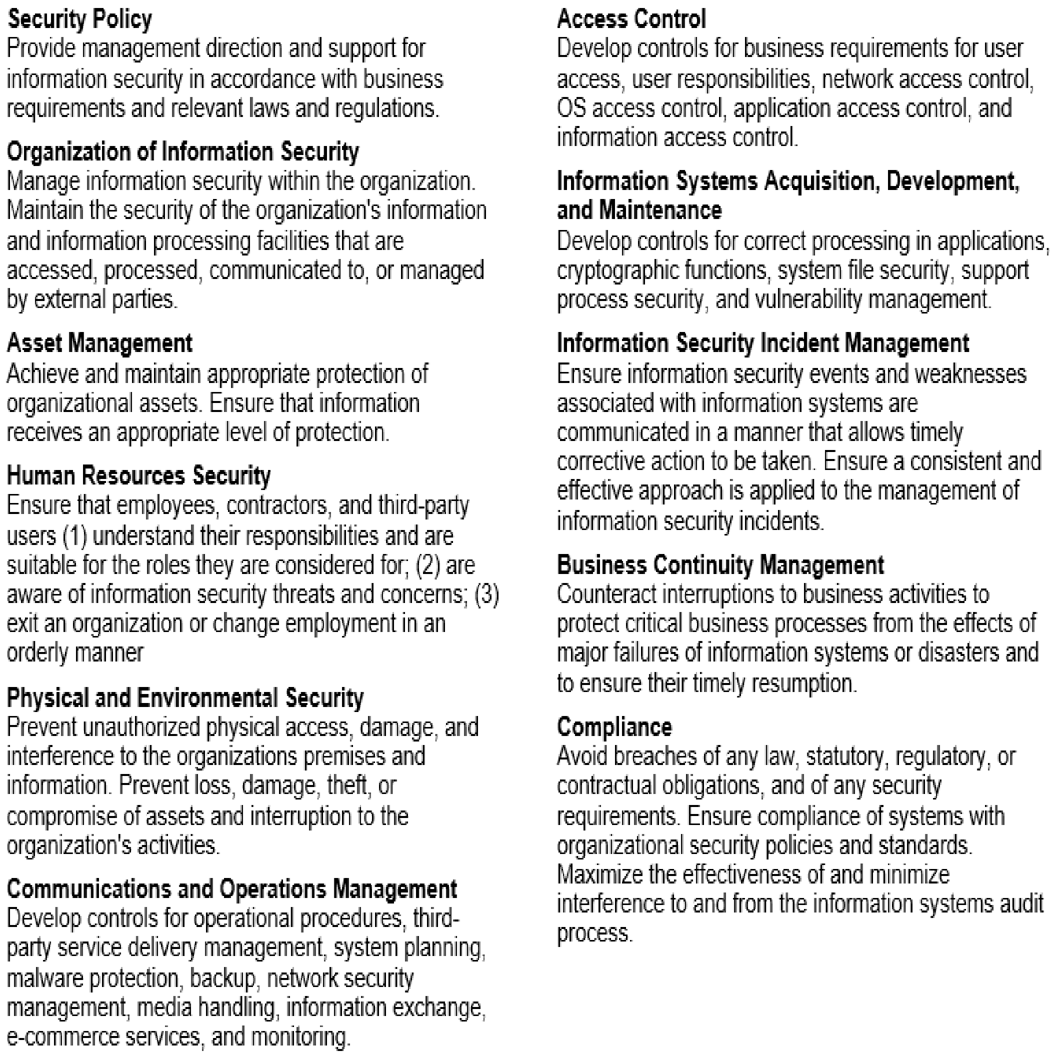
Note: Rights refer to what you can and cannot do on the network, such as the right to log in or shut down a PC

Permissions refer to what you can or cannot do with shared resources on the network, once you are authenticated on the network.

Lastly, sensitive data files should be audited to ensure only authorized changes. The defence in depth approach is outlined in policies and procedures to be followed by all employees daily.

Respond: Enforcement of Comprehensive Security Policy

A comprehensive security policy involves protecting the assets of the company by providing guidelines and standards for all employees to follow. An international standard for writing and implementing security policies is ISO 17799. Seneca College completed its ISO 17799 certification several years ago and it took 4 years to complete. Certification assures partners and government agencies that you have technical controls in place to protect data, to properly configure hardware and software, control how technology is used, how to respond to a break-in and recover from human or natural disasters. A review of the ISO topics, summaries the policies required for certification:



Security Policy
Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Organization of Information Security
Manage information security within the organization. Maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

Asset Management
Achieve and maintain appropriate protection of organizational assets. Ensure that information receives an appropriate level of protection.

Human Resources Security
Ensure that employees, contractors, and third-party users (1) understand their responsibilities and are suitable for the roles they are considered for; (2) are aware of information security threats and concerns; (3) exit an organization or change employment in an orderly manner

Physical and Environmental Security
Prevent unauthorized physical access, damage, and interference to the organizations premises and information. Prevent loss, damage, theft, or compromise of assets and interruption to the organization's activities.

Communications and Operations Management
Develop controls for operational procedures, third-party service delivery management, system planning, malware protection, backup, network security management, media handling, information exchange, e-commerce services, and monitoring.

Access Control
Develop controls for business requirements for user access, user responsibilities, network access control, OS access control, application access control, and information access control.

Information Systems Acquisition, Development, and Maintenance
Develop controls for correct processing in applications, cryptographic functions, system file security, support process security, and vulnerability management.

Information Security Incident Management
Ensure information security events and weaknesses associated with information systems are communicated in a manner that allows timely corrective action to be taken. Ensure a consistent and effective approach is applied to the management of information security incidents.

Business Continuity Management
Counteract interruptions to business activities to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Compliance
Avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements. Ensure compliance of systems with organizational security policies and standards. Maximize the effectiveness of and minimize interference to and from the information systems audit process.

Figure 2: ISO 17799 Policy Categories

Threat Environment

Employees are naturally against security procedures because it adds steps to the job and generally makes procedures more complex. This is the main reason why security policies must be implemented from the top down. The threat environment can be an insider or an outsider. You cannot adequately protect the network unless you have a thorough understand the hacker mind set and methodology. Hacking is **when a person intentionally uses a computer resource without authorization or in excess of his/her authorization**. Think of the following scenarios and ask is this hacking or not?

1. You work in the School of Computer Studies and you find the username and password of the secretary on his/her desk. You log in with the secretary's user name and password, just to browse around and you are careful not to change anything. Are you hacking?

   Yes, because finding the username and password did not give you authorization to use it. Most companies have an Acceptable use policy which strongly prevents a user from logging in to another users account for any purpose.

2. You log into your authorized account and discover you can accidentally see sensitive information in your manager's directory. You spend a few minutes browsing around, but you did not change anything. Are you hacking?

   Yes, because you did not have explicit authorization to read the information in another directory and therefore exceeded your level of authorization. This would be contrary to the company's Acceptable Use Policy.

3. Someone sends you an email with a link to a popular game site. When you click on the link, you find that you are logged into the i3 server. You log out immediately. Are you hacking?

   No, you did not use the resource without authorization; you were the victim of a malicious payload which you were not aware of and you did not intentional try to log into the server. You logged out as some as you knew. Most network security training would require you to inform the IT staff of the malicious email.

4. The company you are working for does not have an Acceptable Use Policy and strong security policies. You wish to show management security weaknesses by demonstrating how you can log into the company server without authorization. Are you hacking?

   Yes, you are hacking. Lack of a security policy did not mean that you had authorization to log into the server. Even if you did it to point out the company's weaknesses and had no malicious intent. You have created an illegal act and can be prosecuted by the company.

Hacker Motive and Methodology

Traditionally, hackers have been adolescents who break into networks or release malware. These individuals are driven by a desire for curiosity, power and peer "bragging" rights. The most dangerous group of hackers are "script-kiddies"; the latter are individuals who execute scripts written by others. They do not have a high level of technical knowledge, but their huge numbers make them very dangerous. According to the RCMP, most script kiddies work with a mentor, who is a member of a criminal organization, and uses script kiddies as unwitting pones in a criminal plan. One such plan is "pump and dumb" schemes. These are schemes which intentionally try to manipulate the price of stocks. For example, the criminal organization buys options on a stock, predicting that the stock price will fall in 3 months. The organization floods the social media and hacking sites with a GUI script which will create a denial of service attack on the victim company. Script kiddies launch the attack with the mentor and brag about how successful their denial of service attack was and how long they could maintain it. Customers of the company, however, finding it difficult to contact the company and receive updates, switched to a competitor. Consequently, the company's stock price falls and the criminal organization makes a wind-fall profit.

Traditional attackers have been external hackers motivated by bragging rights or disgruntled employees. Employees are dangerous because they are inside the network and are trusted; they also know the security policies making it easier to circumvent. Ex-employees have stolen money, trade secrets or sabotaged systems. These traditional attackers are now a small and shrinking minority. They are being replaced with a modern attacker who is part of a loosely organized criminal organization working solely for the profit motive, breaking into networks, stealing information, etc. Attackers today are showing increased sophistication using large and complex black markets for attack programs, conducting attacks-for-hire, renting bot services and money laundering.

Types of Attacks

There are two types of attacks in general use today: random criminal attacks on individuals and targeted criminal attacks on corporations.

Criminal Attacks on Individuals

Criminal attacks on individuals today are largely to steal personal information, such as credit card or banking information. In this case, the goal is steal a victim's credit card number so you can make purchases. Or, the goal could be to steal several pieces of a victim's identity to impersonate the victim and get a loan from a financial institution. The latter is more serious than the first, and can destroy a person's credit rating for many years. In corporate identity theft, the attacker impersonates an entire corporation's credit card and uses it in the company's name or commits other crimes in the name of the firm. Such action can seriously harm a company's reputation and product branding. In both cases, malware (evil software) is the tool used – viruses, worms or Trojan horses.

Viruses are pieces of code that attach themselves to other programs. A virus executes when the infected program runs. Viruses can be spread by email attachments, links on a web site or file sharing using USB flash drives.

The cost common malware today, however, is a worm. Worms are stand-alone programs that do not need to attach to other programs because they are written in a macro language like VB. They propagate the same way as viruses. Viruses and worms have payloads, which can erase hard disks, or send users to pornographic sites, steal personal information, or download another program such as a keystroke logger. Sometimes the payload is hidden in a Trojan Horse. The latter is a container which has a legitimate looking purpose, but contains an illegitimate payload.

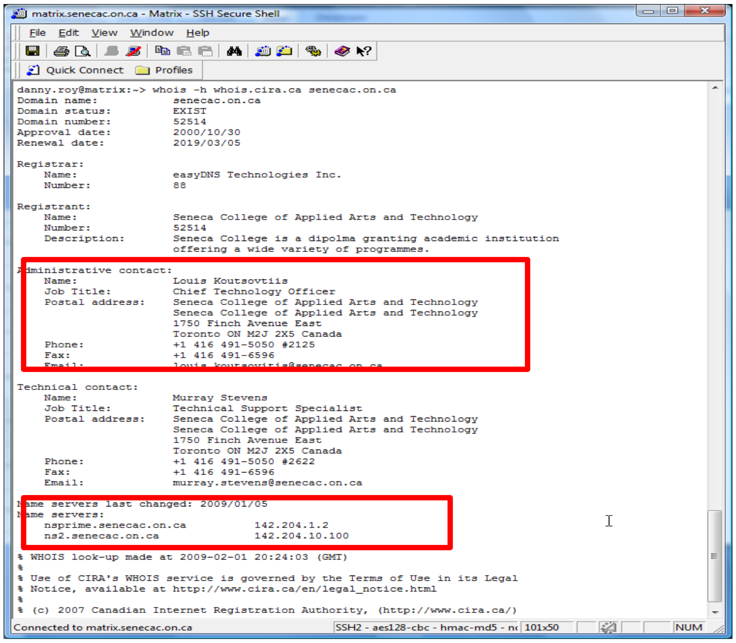
These types of attacks are rarely targeted; rather, the attacks are designed to be random and attack individuals in a specific region, or with an IP address in a specific range. Consequently, stopping these types of attacks requires installing anti-virus and anti-phishing software to scan applications and web sites for potential malicious use. Since criminals are always trying to find new methods, it is important to maintain regular software updates to catch the latest methods.

Criminal Attacks on Corporations

Attacks on corporate networks are usually targeted attacks to break in and if that is not possible, initiate a denial of service attack. The attacker typically has a 3 step plan.

Stage 1

The first step in planning a break-in is to scan the network and get as much public information about the network. A common tool used is the whois database with is built into the UNIX operating system. You can see that this database provides information that can be used in social engineering attacks, such as the name and phone number of the IT manager and the IP addresses of Seneca's DNS servers. Most attackers send 2 to 3 months gathering information and planning the attack. They use social engineering to steal information either remotely or by going on the premises. The PING command can be used to find active hosts and returns the host's IP address. Once an attacker knows that a host is active and available, the attacker will send another round of packets to see which ports are available. This tells the attacker which applications are running on the host.


matrix.senecac.on.ca - Matrix - SSH Secure Shell
File
Edit
View
Window
Help
Quick Connect
Profiles
Connected to matrix.senecac.on.ca
SSH2 - aes128-cbc - hmac-md5 - n
101x50
NUM

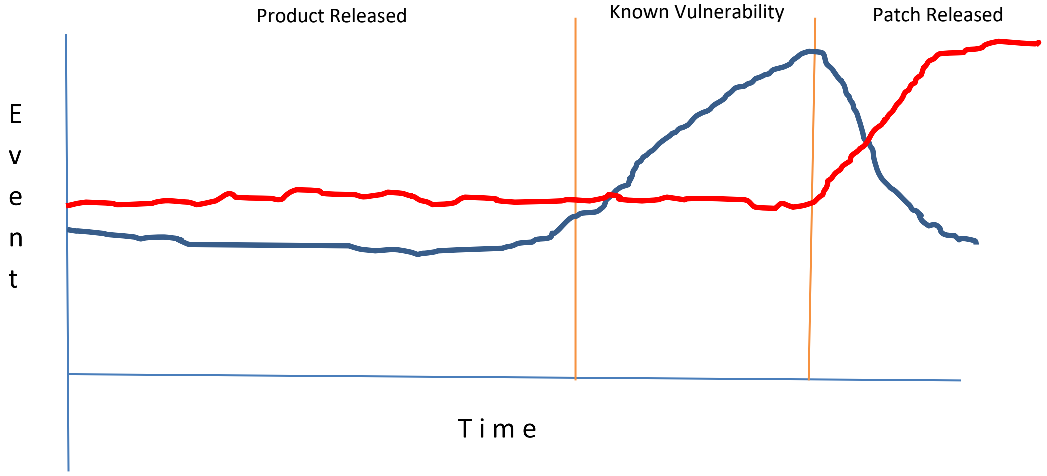
```
danny.roy@matrix:~> whois -h whois.cira.ca senecac.on.ca
Domain name:            senecac.on.ca
Domain status:          EXIST
Domain number:          52514
Approval date:          2000/10/30
Renewal date:           2019/03/05

Registrar:
    Name:               easyDNS Technologies Inc.
    Number:             88

Registrant:
    Name:               Seneca College of Applied Arts and Technology
    Number:             52514
    Description:        Seneca College is a dipolma granting academic institution
                        offering a wide variety of programmes.

Administrative contact:
    Name:               Louis Koutsovtiis
    Job Title:          Chief Technology Officer
    Postal address:     Seneca College of Applied Arts and Technology
                        Seneca College of Applied Arts and Technology
                        1750 Finch Avenue East
                        Toronto ON M2J 2X5 Canada
    Phone:              +1 416 491-5050 #2125
    Fax:                +1 416 491-6596
    Email:              louis.koutsovitis@senecac.on.ca

Technical contact:
    Name:               Murray Stevens
    Job Title:          Technical Support Specialist
    Postal address:     Seneca College of Applied Arts and Technology
                        Seneca College of Applied Arts and Technology
                        1750 Finch Avenue East
                        Toronto ON M2J 2X5 Canada
    Phone:              +1 416 491-5050 #2622
    Fax:                +1 416 491-6596
    Email:              murray.stevens@senecac.on.ca

Name servers last changed: 2009/01/05
Name servers:
    nsprime.senecac.on.ca         142.204.1.2
    ns2.senecac.on.ca             142.204.10.100

% WHOIS look-up made at 2009-02-01 20:24:03 (GMT)
%
% Use of CIRA's WHOIS service is governed by the Terms of Use in its Legal
% Notice, available at http://www.cira.ca/en/legal_notice.html
%
% (c) 2007 Canadian Internet Registration Authority, (http://www.cira.ca/)
```

Stage 2

Armed with this information the attacker can then research known vulnerabilities in system or application software that can be used to take over the host. The attacker than finds or designs an exploit that takes advantage of the vulnerability. A review of all attacks since 2002 has shown that there is a spike in attacks, after the patch for the vulnerability is released. This is counter initiative from what we think happens and we need to examine it. We think that once a vulnerability is known that attacks will increase until a patch is created and then as the patch is applied the number of attacks declines (represented by the blue line in the diagram below). This trend is not what happens. The spike in attacks does not occur until after the patch is released (represented by the red line). Why? Think like the attacker.

With the release of the patch the attacker can easily reverse engineer the patch to convert it to an exploit. Then the attacker can release the exploit and inflect PCs before the patch is applied. On a large network, the time delay between releasing a patch and applying it on network hosts can take 6 months to a year.

Figure 3: Chart showing when spike in attacks



Stage 2 is a Stage 2 is a process of trial and error. Try one exploit after another to find one that works. The attacker could also try and guess a user's password. However, this seldom works, if the network has good security, the attacker will be locked out after several attempts. The more fruitful attack is to use known vulnerabilities and convert the patch to an exploit or find an exploit on the web posted on hacking web sites. An open source tool used for this purpose is Metasploit (read about it at https://www.metasploit.com/). Originally designed as a tool for network administrators to test they own networks, it has become a tool to find vulnerabilities and break into networks.

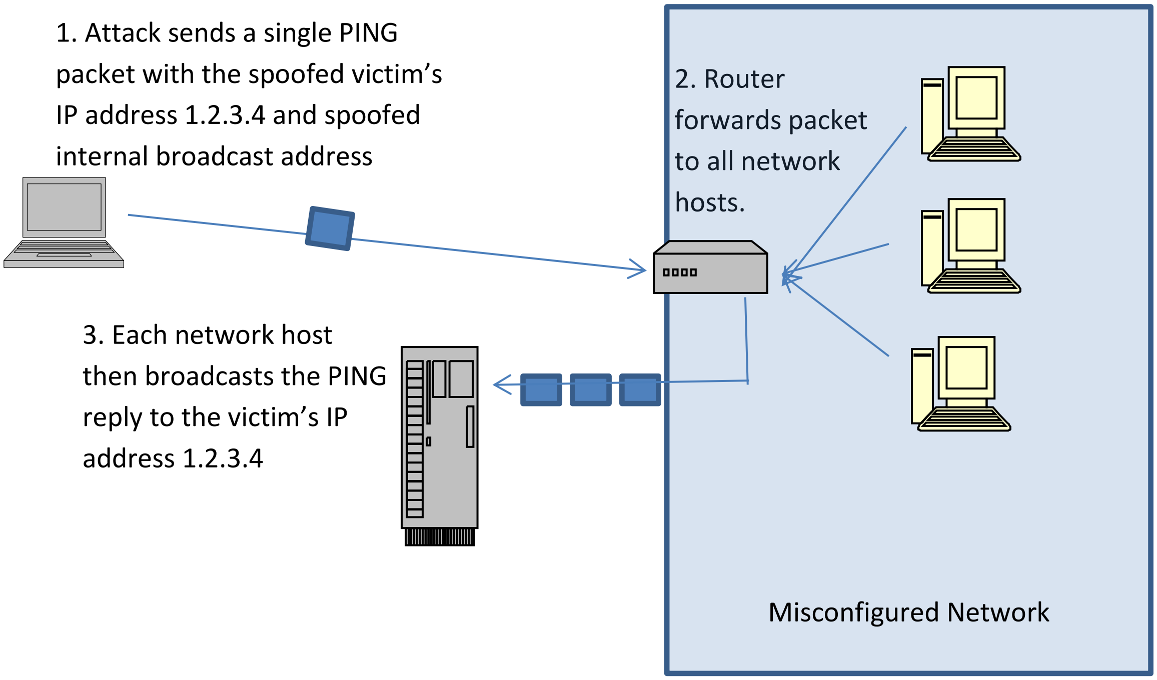
Stage 3

Once the hacker has successfully uses an exploit, he/she will download a hacker tool kit to automate the process by creating "a backdoor" (a way to get back into the computer with a known password and full privilege). The tool will also delete log files to cover the attack's tracks and/or download a keylogger program so the hacker can monitor company activity or steal passwords and account information.

DoS Attacks

If the attacker cannot break-in, he/she will initiate a denial of service attack (DoS). Or the goal is to disrupt the company operations, the hacker does not need to break in. He/she can disrupt company servers or switches\routers. A common DoS

Figure 4: Smurf attack


1. Attack sends a single PING packet with the spoofed victim's IP address 1.2.3.4 and spoofed internal broadcast address
2. Router forwards packet to all network hosts.
3. Each network host then broadcasts the PING reply to the victim's IP address 1.2.3.4
Misconfigured Network

In a Smurf attack, the attacker sends a single PING packet with spoofed source address of the victim's IP address, 1.2.3.4, and the spoofed internal broadcast address of an innocent network. The network router must be misconfigured because no router should forward an external packet arriving with the internal address of the network. This is a clear sign of a forged packet. However, if broadcasting is enabled, the router will forward the packet to all internal hosts. Each host then replies to the echo request and sends a packet to the victim's IP address. Using this attack an attacker can amplify one packet into a stream of packets to prevent the victim's server from responding to legitimate requests.