Identifying and Handling the Network Security Threats and the Security Mechanisms for Exploiting Vulnerabilities

Dr.R.S.Vetrivel
Assistant Professor, Department of Computer Science, Joseph Arts and Science College, Thirunavalur, Villupuram, TamilNadu, India

Abstract**--** Trojan horses, worms and DoS (Denial of Service) attacks are often maliciously used to consume and destroy the resources of network. With the advent of wireless Internet, more and more computer users are entering the world of cyber space. Yet, while these users are well aware of the importance of the protection of their computer when hooked up to regular internet providers, they are often oblivious to the fact that the same cyber dangers, and in fact even more, exist in the world of WiFi. Sometimes, misconfigured servers and hosts can serve as network security threats as they unnecessarily consume resources. In order to properly identify and deal with probable threats, one must be equipped with the right tools and security mechanisms. This paper will discuss some of the best practices for identifying and dealing with such threats.

Keywords**--** *Network security, Hackers, Malware, security management.*

I. INTRODUCTION AND TYPES OF NETWORK THREATS

Network security threats are classify in two major categories: Logic attacks and Resource attacks. Logic attacks are known to exploit existing software bugs and vulnerabilities with the intent of crashing a system. Some use this attack to purposely degrade network performance or grant an intruder access to a system. One such exploit is the Microsoft PnP MS05-039 overflow vulnerability. This attack involves an intruder exploiting a stack overflow in the Windows PnP (plug and play) service and can be executed on the Windows 2000 system without a valid user account. Another example of this network security threat is the infamous ping of death where an attacker sends ICMP packets to a system that exceeds the maximum capacity. Most of these attacks can be prevented by upgrading vulnerable software or filtering specific packet sequences. Resource attacks are the second category of network security threats. These types of attacks are intended to overwhelm critical system resources such as CPU and RAM. This is usually done by sending multiple IP packets or forged requests. An attacker can launch a more powerful attack by compromising numerous hosts and installing malicious software. The result of this kind of exploit is often referred to zombies or botnet. The attacker can then launch subsequent attacks from thousands of zombie machines to compromise a single victim. The malicious software normally contains code for sourcing numerous attacks and a standard communications infrastructure to enable remote control.

II. SEEK AND DESTROY

The first step is to identify network security threats of achieving network visibility. This level of network visibility can be achieved with existing features found in devices and can create strategic diagrams to fully illustrate packet flows and where exactly within the network might be able to implement security mechanisms to properly identify and mitigate potential threats. Establishing a baseline of normal network activity and patterns are in order to detect abnormal activity and potential network security threats. Mechanisms like NetFlow can be integrated within the infrastructure to help effectively identify and classify problems. The best defense against common network security threats involves devising a system that is adhered to by everyone in the network. With the advent of wireless Internet, more and more computer users are entering the world of cyber space. Yet, while these users are well aware of the importance of the protection of their computer when hooked up to regular internet providers, they are often oblivious to the fact that the same cyber dangers, and in fact even more, exist in the world of WiFi.

III. MALICIOUS INSIDERS

Rising Threat Employees with malicious intent have always been the biggest threat to their organizations. According to www.infosecurityanalysis.com, when a data security breach occurs as a result of a malicious insider, more records are compromised than any other breach source (including hackers). Several studies indicate that only a small percentage of data breaches are reported. Many companies still choose not to report them because it shows a systemic failure in hiring practices, policies, procedures, auditing, enforcement and technology safeguards. As economic times get worse, we will likely see desperate and malicious employee’s compromise security for a few extra dollars.

IV. MALWARE-STEADY THREAT

Malware means malicious software which can include viruses, worms, Trojan horse programs, etc. Web sites that host malware, when a vulnerable user accesses this web site, their system become infected. The system then falls under the control of the attacker. This is such an effective method to distribute malware and compromise systems that it has become the most prolific method.

V. EXPLOITED VULNERABILITIES WEAKENING THREAT

Exploiting a known vulnerability is the normal process when people talk about hacking. Hackers find a weakness and exploit it for their gain. There is nothing new here, except the location of the systems. In times past, it was external systems such as email servers, web servers, and firewalls that would be broken into. These attacks are moving inside the network. Systems on the inside of the network are not patched and updated as frequently. Networks have a hard outer edge and a gooey center from a security perspective. Organizations rely on Microsoft SUS (system update service) that patches to keep the systems up-to-date. The problem is that SUS only patches Microsoft which leaves all the non-Microsoft operating systems applications vulnerable. IT professionals make the mistake of thinking, “It was only the administrative assistant's machine that got compromised and it didn't have any sensitive information on it." If a system gets compromised, the attacker may have control of more than just that one system. From that system they could launch additional attacks to other systems. They can 'sniff' the credentials of anyone on that system to access other systems. Typically, the first system to be exploited is just the base camp to compromise more valuable assets. When an internal system is compromised, the bad guys now have ways of bypassing entire network and edge based security controls. They use encrypted tunnels over commonly used ports to make their deeds virtually invisible.

VI. SOCIAL ENGINEERING

Gartner states that the greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses. Why spend days trying to crack a username and password using sophisticated software and potentially get caught, when you can trick someone into just giving you theirs? With hacking, you are compromising a computer, and with social engineering you are compromising a human**.** Any method of communication can and will be used to perpetrate fraud including telephones, mobile phones, text messaging, instant messaging, and social networking sites. Many people will fall prey to their own natural curiosity.

VII. CARELESS EMPLOYEES

Careless employees are not a threat and have listed in the past. Not only have seen a trend that includes more mistakes made by careless or untrained employees that lead to a security compromise, but this will be fueled by the economic climate. With a recession, business will have to do more with less. The strain this puts on employee’s causes them to cut corners on important duties. Systems will not be updated, logs will not be reviewed and alerts will go unchecked. This creates gaps that can be exploited by the attackers. A poor economic climate may lead to less formal employee training. This leads to policies and procedures not being followed. Liability issues arise and data exposure can occur.

VIII. REDUCED BUDGETS

As there are many threats that have roots in a downward economy. A weak economy leads to companies tightening their budgets. This result in lower headcount and less money for upgrades and new systems. Just because the economy slows does not mean that criminals slow down. In fact, it is often the opposite. There are always those system upgrades, process improvements, and new technologies that were put into next year’s budget that may now be put on hold. **2010** may see reduced budgets, which mean more exposure and security gaps that can lead to a data security breach.

IX. REMOTE WORKERS

Companies that support telecommuting are on the upswing. Remote workers and travelers all pose unique security risks. Often an organization install a VPN box without much thought to security. A VPN only encrypts the traffic between the remote user and the company. If that system is compromised, and effectively encrypting (keeping private) all of the hacker’s traffic. VIPs are usually installed in a way that bypasses edge based security devices such as the corporate firewall. Remote workers have greater exposure to system compromise for several reasons:

1. The company does not own the computer they are working from and it does not have the security software like other corporate systems.
2. Remote users are more likely to allow their systems to lapse in their security protection. They do not update software because they often pay for it out of their own pocket.
3. When something goes wrong, there is no IT person to help them, thus they do whatever it takes to get it working which may disable needed security measures.
4. Theft is the #1 cause of data security breaches. Most people house some sensitive corporate or customer data on their laptops. 1 in 10 laptops is stolen within the first year of ownership.
5. A remote computer is not subject to the same security requirements as a corporate computer. For example, using web content filtering on the corporate network to block access to inappropriate web sites. Remote user traffic is usually not routed through the same system. As a result, the remote user may access a web site that could infect and compromise their system. When that system connects to the network, that compromised system can now spread and attack other internal systems.
6. Children and other household members may use the same computer mom or dad use for work. They install a game; hit a web site, or any of a number of things that can lead to the compromise of the system. All you hear is "Dad, the computer is running really slow again!"

X. UNSTABLE THIRD PARTY PROVIDERS

Most providers have begun to see slowing sales and weaker profits. At the same time, regulators are requiring many providers to achieve and maintain strong compliance. While there is an increase in expenses, there is a decrease in revenues. I believe this will lead many providers to go out of business or cut corners that could lead to a compromise. At this time, it is imperative for organizations to streamline their 3rd party providers. Ensure you are using providers that have been in business for a long time and have seen hard times before. Use providers that have been regulatory focused for years rather than ones that are just trying now. Ask for audited financials and ensure that your provider is profitable. Choose a provider that can offer you multiple solutions to gain the benefits of economies of scale. I am a big proponent of outsourcing, but it must be to the right organization.

XI. DOWNLOADED SOFTWARE INCLUDING OPEN SOURCE & P2P FILES

IT administrators may be tempted to take on more themselves. They may download and install open source software or freeware in an attempt to save money. I have found that these tools in the hands of an inexperienced user may lead to a huge waste of time or a data breach. Almost all security software available commercially has a freeware or open source counterpart somewhere. The installation, configuration, fine tuning and other aspects of a software lifecycle sometimes are more than any individual can handle, especially if they don’t have the time and training to do it. Lastly, users that are allowed to download and install software on their desktops are a huge risk to their company. For example, we have seen unsuspecting users install modified versions of P2P software. Rather than just giving the user the ability to download music and movies (which is a bandwidth problem by itself), these programs can be modified to scan the local system and network systems to catalog sensitive information such as spreadsheets and databases and make them publically available for download anywhere in the world. Firewall and most other security devices cannot detect or stop this activity. All software downloaded and used should be done by a trained IT professional. I believe we will continue to see many data breaches as a result of downloaded software in 2009.

CONCLUSION

This doesn't have to be all doom and gloom. By realizing these threats, we can work to ensure our exposure is limited. Additionally, it gives us the opportunity to look at alternative solutions. A company that has traditionally kept their security management and monitoring in-house may use this as an opportunity to look at the cost benefits of outsourcing this to a leading security firm. Some of the technology you have been using to reduce your risk may be outdated and you can replace it with newer systems that can protect your organization better for the same or less money. Challenges such as this give us the opportunity to rethink the way we have done things in the past and find newer, optimized ways of securing our organizations. With data security, it isn't about having more as much as it is about having the right stuff.

References

[1] Back, A., Goldberg, I., and Shostack, A.Freedom Systems 2.1 security issues and analysis.

[2] Back, A., M¨oller, U., and Stiglic, A. Trafficanalysis attacks and trade-offs in anonymity providing systems.

[3] Berthold, O, Federrath, H., and K¨opsell, S. Web MIXes: a system for anonymous and unobservable Internet access.

[4] Bethencourt, J., Franklin, J., and Vernon, M. Mapping Internet sensors with probe response attacks.

[5] Burnside, M., and Keromytis, A. Low latency anonymity with mix rings. In Proc. 9th International Information Security Conference (ISC) (2006), pp. 32–45.

[6] Camenisch, J., and Lysyanskaya, A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Proc. Advances in Cryptology – EUROCRYPT (2001), pp. 93–118.

[7] Chung, S., and Mok, A. Allergy attack against automatic signature generation. In Proc. Recent Advances in Intrusion Detection: 9th International Symposium (RAID) (2006), pp. 61–80.

[8] Clarke, I., Sandberg, O., Wiley, B., and Hong, T. Freenet: A distributed anonymous information storage and retrieval system. In Proc. International Workshop on Design Issues in Anonymity and Unobservability (2001), vol. 2009 of LNCS, Springer-Verlag, pp. 46–66.

[9] "Threats and Countermeasures against the Invasions in the Ubiquitous Home-Network Environment,"Yoo D. Y., Kim Y. T., Rho B. G. Korea Information Security Agency, 2004.10 Jorunal V31, B2, KIISE.

[10] Bethencourt, J., Franklin, J., and Vernon.M. Mapping Internet sensors with probe response attacks. In Proc. 14th USENIX Security Symposium (2005), pp. 193–208.

[11] Gates, C., Collins, M., Duggan, M., Kompanek, A., and Thomas, M. More Netflow tools: For performance and security. In Proc. 18th Conference on Systems Administration (LISA) (2004), pp. 121–132.