

Case Study on Risk

Kn1ghtl0rd

University of Advancing Technology

NTS350

*Executive Summary**Case:*

Putting these terms to work in an example, let's consider the risk to a public Web server operated by the Polish Ministry of Defense (www.wp.mil.pl). On September 3, 2003, Polish army forces assumed control of the Multinational Division Central South in Iraq. A hypothetical anti-Iraq war hacker group, Code Not Bombs, reads the press release at www.nato.int and is angry about Poland's involvement in the war. One of their young coders, N@te, doesn't like Poland's involvement and wants to embarrass the Polish military by placing false news stories on the Ministry of Defense's Web site. He discovers that although www.wp.mil.pl is running Apache, its version of OpenSSL is old and subject to a buffer-overflow attack. If N@te so desired, he could accomplish his goal. The Polish military spends \$10,000 (or the Polish equivalent) per year maintaining its Web server. Damage to national prestige from an attack would be several times greater."

Summary:

When making controversial decisions it is important to take into account all different points of attack, including public computer systems. Administrators need to be aware of points of entry for their network and also what makes traffic valid or invalid. Understanding security principles is key to making a network defensible and limiting possibilities of attacks and also recovering quickly from them. Analysis of threats, vulnerabilities, and risks are important in defining steps needed to close holes and negate attacks.

By understanding attack structure it is possible to be aware of the current status of an attack and to watch for high risk phases when it will be the easiest to notice abnormal activities and help to find out specific target systems or applications. Activity monitoring can give

administrators the same information that the attacker has and help narrow down possible attack scenarios in order to check for possible weaknesses.

Using good defense and recovery strategies can help prevent attacks and loss of data or integrity after an attack has been completed. By using networking strategies proven to limit attackers the network can become self sustaining and defending making it easier to monitor, update, and plan for attacks.

CASE STUDY ON RISK

1.0 Introduction

1.1 Threat

It is necessary when making a controversial decision to include the possibility of attack from more than just a physical encounter. By performing a military action that could be perceived as wrong the Polish government needs to be able to react to any oncoming threat whether by land, sea, air, or technological attack and public servers should be taken into consideration when planning recovery tactics and damage prevention.

1.2 Vulnerability

A public web server is an easy target for most attackers. There is less access control to a web site because of the fact that it is public. It is necessary to allow traffic to and from the server and depending on the type of site running it may also require transactions to be made and requests to internal databases, etc. By allowing the server to be accessed it is important to take account for what software is running on that server and making sure that the software is kept up to date and that any known vulnerabilities are patched immediately upon discovery.

1.3 Asset Value

Depending on the nature of the site there can be many risks upon the server. In this case the risk is embarrassment and moral degradation. The site in question is there for updates on military activities and the content needs to be factual and reassuring to the public that views it. If the site were to be compromised than public moral would drop and the integrity of the military would be compromised. The risk is very high in this example because the loss would be great to the integrity of the military and would be hard to recover from.

2.0 Defense

2.1 Understanding the Attacker

It is important to understand the steps taken when an attack is performed in order to look for signs before the actual damage is made. There are five basic phases of attack, reconnaissance also known as footprinting, exploitation, reinforcement, consolidation, and pillage. It is easier to notice someone during the reconnaissance process than it is during the pillage process so keeping a sharp eye on server activity is key to preventing an attack.

A good attacker will make sure they have a thorough understanding of their target in order to complete the attack without being noticed. Reconnaissance, or footprinting, is the systematic and methodical footprinting of an organization to create a complete profile of an organization's security posture (Kurtz, McClure, Scambray, 2005, p. 6). By knowing what the target has, the attacker can plan around a defense without elevated risk of encountering the defense during the actual exploitation.

During the next step the target is actually exploited to allow the attacker entry into the system. In this example the attacker would run the exploit on the OpenSSL vulnerability in order to give himself access to the server so he can move to the next step of the compromise. There is medium risk associated with this part of the compromise because most attacks show up in logs as illegitimate traffic so it is easy to spot one and if the exploit is complicated then the risk is elevated even further.

Once the attacker has compromised the system the next step is reinforcement. This step is necessary for the attacker to make sure his goal is accomplished. After the attacker has entry into the system he will then download tools needed to complete his task whether this is a Trojan horse program that allows remote operation or keystroke logging software, etc. These tools will

be used in the next two steps to complete the attacker's mission. This phase has a high risk to it because the traffic coming from the server will look abnormal and outbound traffic is very easy to monitor. Other tools might be included to cover the attacker's presence or tracks of the exploitation and footprinting process.

After the attacker has the tools necessary to complete the compromise or cover the evidence of it, he will then perform the consolidation phase which is the final phase before the actual damage is performed. During this phase the attacker will clean up and then pull out of the exploited hole and then reenter using the back door that he inserted. This allows him to communicate with the machine in a covert mode where his presence will not be noticed and traffic will be masked as legitimate traffic. At this point he is at a low risk level and is safe to perform the next and final step.

The last step is to actually commit the act that the attack was performed for. In our case it is the modification of the web site on the public server. In this instance it is a low risk activity because up until the final save of the new web page the exploit is still unnoticed. He will more than likely make a copy of the original site and modify it, then replace the original with the new site. All of this can take only a few minutes and the attacker can be out before anyone even notices the change. At this point the attack is complete and attacker will possibly remove the back door and his presence will have effectively been masked.

2.2 Traffic Monitoring

As stated in the above section, two of the five phases in the compromise are of high risk which means that it is easy to notice. During the first phase the attacker will be constantly probing the network to find a weakness. In our case study this has already been performed because he has found the vulnerability that will be exploited in his attack, the OpenSSL

application running on the server. We can assume that the logs have recorded the activities he performed during this phase so by reviewing them it should be obvious what he was looking for. With this information it is possible to reconstruct his methods and hopefully reach the same results the attacker did. Armed with the results of the reconnaissance it is then possible to isolate possible issues and then research into existing vulnerabilities. If vulnerabilities are found then it can be patched effectively preventing future attacks on that weakness.

The reinforcement phase is also of high risk to the attacker because his traffic will be monitored and it will look out of the ordinary because the tools likely to be downloaded will not be coming from sites accessed by the web server normally. It is important to monitor outgoing traffic from a public server to make sure it is not performing activities that it shouldn't be. It might also be necessary for the attacker to disable certain services in order for the traffic to be allowed through such as a software firewall. It is easy to spot these kinds of activities as long as the logs are being reviewed on a regular basis.

In order to better protect a network it should be using best practices when routing traffic from the outside as well as inside. NAT policies should be used to isolate traffic from this web server so that no other machines can be compromised following the initial compromise of this machine. It is also effective to keep the machine's services to a minimum. There should be no open services that are not actually necessary to the functioning of the server. Hardware firewalls can help to clean up traffic and look for abnormal packets that might signal possible attack like port scanning attempts or DoS attacks.

2.3 Recovery

A recovery plan is necessary to have when talking about systems that are central to the organization being targeted. Keeping backups and mirrored systems can help the organization

recover quickly and keep a large amount of people from noticing the compromise or from being denied legitimate service from the server. In our case study the administrators of this web server should always make a backup of the site's files when a change is made by them. This way they have a current version should something happen. If the site is being monitored than after the attack they would be able to replace the false site with the copy of the current and alleviate a lot of the damage that would have been caused by the attack being in production for an extended period of time.

3.0 Conclusion

During an attack scenario it is important to understand the attacker and the methods performed during an attack. By watching logs for abnormal traffic it is easy to notice attack attempts during the high risk phases of compromise, reconnaissance and reinforcement. Performing regular updates on software and services limits the possibility of attack and it helps make the network defensible which is ultimately how the network should be. These networks are easier to monitor for possible attacks and can help streamline recovery when an attack has been performed.

References

Bejtlich, R. (2005). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*.

Addison-Wesley: Boston.

Kurtz, G., McClure, S., Scambray, J. (2005). *Hacking Exposed Fifth Edition: Network Security*

Secrets and Solutions. McGraw-Hill: Emeryville, CA.