



THE ART OF CYBERWAR

By Wayne Selk
wayne_selk@symantec.com

In his famous collection of essays, "The Art of War," Chinese general and noted military strategist Sun Tzu claimed that, "All warfare is based on deception." Clearly, Sun Tzu was speaking of physical combat when he made his comment. But even though this declaration was made well over 2,000 years ago—long before enterprise network security, hackers, and the Internet were even issues—it is interesting the parallels that can be drawn with the cyberwars going on today.

Combat tactics in cyberspace have changed dramatically over the last few years, much the way military strategies and techniques have evolved over time. While in the past a castle with a moat provided ample protection from enemy attacks, it would be ridiculous to assume that would be the case now. Similarly, a firewall alone is insufficient in providing necessary security to an enterprise's network.

Attackers are becoming increasingly sophisticated and the arsenal of weapons ready to attack enterprises is growing. Security administrators must be proactive in defending their information and data from threatening attacks. This is where Sun Tzu's comments can aid security administrators in protecting their information. It would be inaccurate to claim that all cyberwarfare is based on deception, but diversions are becoming increasingly important.

Decoy-Based Intrusion Protection

One of the latest mechanisms designed to defend against cyberattacks is decoy-based intrusion protection, or "honeypot" technology. Honeypots are increasingly being used in a complementary fashion with firewalls and intrusion detection systems (IDS) to protect enterprise networks. Much like deceptive tactics in war, honeypots divert attackers into hacking into false systems and networks, thereby protecting important proprietary data.

Originally used for research purposes, honeypots were placed outside the firewall and used to monitor hackers on a network. Researchers and analysts could then study the tactics, tools, and behavior of cyberattackers. This information could then be used to solidify any leaky security measures and anticipate future attacks.

Over time, honeypot use has evolved and now security administrators deploy honeypots as part of their intrusion protection strategies. Instead of primarily being used to gain knowledge about network enemies, honeypots have become vital tools in security prevention and detection. Deception, as Sun Tzu stated, is a security administrator's ally in cyberwarfare.

Technically speaking, a honeypot is a system placed on a network specifically to be probed and attacked. Once deployed, a honeypot can detect, contain, and monitor any unauthorized access. Since a honeypot provides no production value, all activity is unauthorized and is considered a malicious action.

There are two types of honeypots: low-interaction and high-interaction. The difference between the two honeypots is how much activity an attacker is permitted. Low-interaction honeypots emulate operating systems and services, offering limited activity. Relatively easy to deploy, low-interaction honeypots involve minimal risk because attackers never have access to actual operating systems.

High-interaction honeypots are riskier in that they involve real applications and systems. This provides a more realistic target, which provides additional capability in detecting a more sophisticated attacker. High-interaction honeypots also provide more information to analyze because the activity is not as limited as in low-interaction honeypots. Additional technologies are required when deploying high-interaction honeypots to ensure attackers will not use the honeypots as launching pads for future attacks on other systems.

The Advantages of Honeypots

It is important to understand that a honeypot is not an adequate security technology by itself. Honeypots will only capture activity directed towards them and will miss all attacks against other systems. They are not designed to catch all malicious activity throughout the network and treating a honeypot as an all-encompassing security solution will open several doors for cyberattackers to enter.

However, when used to supplement network- and host-based intrusion protection, honeypots play an important role and provide unique advantages as a part of the security infrastructure. These advantages include the following:

Improved Intrusion Detection

Honeypots are unique in that they have the ability to detect a variety of intrusions that other technologies are not designed to catch. For example, a typical IDS would not catch some new attacks or "zero-day" attacks. Since the honeypot captures all activity regardless, these attacks will automatically be caught. In addition, if someone stole credentials and planned to access the network without authorization, a traditional IDS most likely would not be able to discern that the credentials are in fact stolen. With a honeypot, the activity tracked would raise a red flag because the access to the honeypot itself is, by definition, unauthorized. "Zero-signature" attacks, those that do not have unique patterns to match and are indiscernible from regular traffic, also are detected.

Ability to Avoid the Data Deluge

Traditional IDSs create an immense amount of data, not to mention cause headaches for the security administrators who are forced to wade

through the information. Aside from the obvious monetary cost of dealing with the volume of alerts, administrators waste their valuable time concentrating on what sometimes turns out to be “noise” rather than dealing with legitimate threats. Not only must the administrators scan all the data; they must also take on the time-intensive task of analysis.

On the other hand, a honeypot drastically reduces the size of a data set. Since honeypots only collect data when someone is interacting with them, organizations can more easily manage and analyze the data. Administrators can allocate time and resources better because of the more manageable data.

Elimination of False Positives and Identification of False Negatives

One of the biggest flaws with traditional IDSs is how many false positives are created. False positives are legitimate activities that are considered malicious because they share certain similarities. Even organizations that fine-tune their systems experience unwanted false positives. Administrators may begin to be tempted to ignore the IDS technology completely due to the frustration caused by dealing with all of the false alerts.

Honeypots avoid this problem altogether. Any activity with a honeypot is unauthorized, so all activities should be considered threats. Along the same lines, while IDS technologies often struggle to identify unknown attacks, all activity with a honeypot is automatically characterized as a potential threat. This eliminates the possibility of missing any false negatives.

Reduction of Resources

As a company's network gets faster and generates more data, the associated IDS must grow proportionately. An IDS requires more hardware, more databases and more money to maintain. All of these additional resources must also be managed, again taking time away from administrators. In contrast, even on a large network, honeypots require minimal resources. A single computer has the ability to monitor literally millions of IP addresses.

Capture of Encryption Attacks

Due to security issues and increased regulation, corporations have made an investment in data encryption. Not surprisingly, attackers are using similar encryption techniques to sneak into networks undetected. An IDS will be unable to sufficiently monitor network traffic if the attack is encrypted; however, with a honeypot, all activity will be captured—whether or not the data is encrypted.

Divert the Enemy

As discussed earlier, honeypots have the ability to lead enemies away from important data and into a false environment. While this becomes a waste of time for hackers, the would-be cyberattackers end up becoming valuable guinea pigs by providing information regarding tactics and behavior. Based on how much activity an administrator allows, the hacker is attacking a non-production dummy system.


Real-Time Analysis

With most security protocols, attacks can only be analyzed after the damage has already been done. The data must be processed and sometimes the analysis could be incorrect as to how the attack actually happened. With honeypots, administrators are able to watch and analyze the attacks as they are occurring. The attack is immediately recognized as such once it enters the honeypot and an administrator has a front-row seat to a

live cyberattack without the danger posed by an actual attack on an operating system. The information gathered from the honeypot can then be used to create a signature pattern, if previously unknown, for either the network- or the host-based IDS.

Conclusion

Corporations concerned with the ever-increasing threat of external attacks have another option in defending their network access. By deploying a honeypot to collaborate with other network- and host-based intrusion protection, a corporation can gain information about hackers and even prevent current attacks. Aside from being instrumental research tools in providing knowledge about the enemies' tactics, honeypots have the ability to weed out current attacks and prevent future threats.

Acting quickly and effectively to intrusions within your environment, using all available resources, IDS and honeypot, translates into minimal data loss and compromise with greater emphasis on information integrity. Furthermore, by placing one or many honeypots within a network, you lower the overall risk of attack on mission critical data components. By managing the risk against those critical servers, one could even draw a favorable conclusion to the return on investment issue. 

Wayne is a Principal Security Consultant with Symantec Corporation currently engaged as a member of the EDS Navy/Marine Corps Intranet (NMCI) project based at the Raytheon facility in Saint Petersburg Florida. He is the subject matter expert for Symantec's network-IDS product called ManHunt and also the Symantec Decoy Server. Wayne can be reached at wayne_selk@symantec.com.