

Threats to Network Security and Its Countermeasures

Indu Bala Grover^{#1}, Priya Tiwari^{#2}
Apeejay College of Engineering and Technology, Gurgaon
MD University Rohtak
ibg7in@gmail.com

Abstract - Recent media coverage of hacker incidents against well-known Internet companies has started to promote a better understanding of the growing threat hackers pose to computer security. The information technology revolution has changed the way business is transacted, governments operate, and national defense is conducted. Protection of these systems is essential and continuous efforts to protect them have resulted in exponential growth in reported security incidents. There are threats from hackers, spies, corporate raiders, terrorists, professional criminals, and vandals -- all of whom have a vested interest and well defined objectives for challenging the technology for financial and political gain, leading to damages to the enterprise infrastructure. The current approach to security is based on perimeter defense and relies on firewalls, intrusion detection systems, and intrusion prevention systems. In this paper, we are reviewing the various myths regarding network security and discussing its countermeasures with special focus on IDS & IPS.

I. INTRODUCTION

In a recent survey commissioned by VanDyke Software, some 66 per cent of the companies who responded said that they perceive system penetration to be the largest threat to their enterprises.

The survey revealed that the top eight threats experienced by those surveyed were *viruses* (78 per cent of respondents), *system penetration* (50 per cent), *DoS* (40 per cent), *insider abuse* (29 per cent), *spoofing* (28 per cent), *data/network sabotage* (20 per cent), and *unauthorised insider access* (16 per cent).

Although 86 per cent of respondents use firewalls (a disturbingly low figure in this day and age, to be honest!), it is apparent that firewalls are not always effective against many intrusion attempts. The average firewall is designed to deny clearly suspicious traffic. Firewalls are also typically employed only at the network perimeter. However, many attacks, intentional or otherwise, are

launched from within an organisation. Virtual private networks, laptops, and wireless networks all provide access to the internal network that often bypasses the firewall. Intrusion detection systems may be effective at detecting suspicious activity, but do not provide *protection* against attacks. Recent worms such as Slammer and Blaster have such fast propagation speeds that by the time an alert is generated, the damage is done and spreading fast. Before dealing with the countermeasures for the network security, first we need to understand the various myths about hackers, information security and the various sources of exposure to network.

A. Hacker Myths

1) *Hackers are a well-organized, malicious group:*

There is indeed a community within the hacker underground. There are hacking-related groups such as Alt-2600 and Cult of the Dead Cow, IRC "hacking" channels, and related newsgroups. However, these groups are not formed into a well-organized group that targets specific networks for hacking. They share a common interest in methods for avoiding security defenses and accessing restricted information.

2) *Security through obscurity:*

Myth 4 implies that because you are small and unknown or you hide a vulnerability, you are not at risk. For example, according to this myth, if you create a Web site but give the URL only to your friends, you don't have to worry about it being attacked. Another example we have seen is the creation of a backdoor around a firewall by putting a second network card in a DMZ system and directly connecting it to the internal network. People using such a strategy think that because they have hidden the weakness, no one will find it and the organization is safe. However, security through obscurity does not work. Someone will

find the weakness or stumble upon it and the systems will be compromised.

3) *All hackers are the same:*

This myth is borne out of a lack of knowledge among the general public about the hacker community. All hackers are *not* the same. Different hackers focus on different technologies and have different purposes and skill levels. Some hackers have malicious intent; some don't. They are not all teenagers who spend far too much time in front of a computer. Not all hackers are part of a group that defaces Web sites and creates and distributes hacking tools. The range among hackers is great, and you need to defend against them all.

B. Information Security Myths

1) *Virus scanning software provides total virus protection:*

Virus scanning software can detect and defend against viruses with known signatures. New viruses, whose signatures have likely not been determined, may not be detected and can still pose a threat to systems. Virus scanning software needs to be upgraded regularly (at least monthly) and is generally sold on a subscription basis to automatically provide customers this level of protection.

2) *Computer connections are untraceable:*

Many people assume they cannot be traced when they are online. They erroneously believe that if they give a fake name and address when signing up for free e-mail or with an ISP for an Internet connection, they have hidden themselves among the millions of users speeding around the World Wide Web. In reality, the use of anonymizing systems, remote networks (sometimes in different countries), and spoofing software is required to achieve even a small degree of anonymity. Even then, your ISP is probably logging your initial point of entry onto the Internet.

It is easy to go to one of the countless free e-mail services on the Internet, supply bogus information, and get an account. However, our privacy is not protected. That e-mail service knows from which Web site (if any) we came to its site and the IP address of the machine we used. It can find the owner of the IP address from a "whois" query. If we signed up from home, our ISP has likely dynamically assigned us an IP address from the

collection it owns. It records the time and day that it gave this address and can share this information with federal, state, and local authorities as well as interested corporations (though a legal warrant may be required). Additionally, the use of cookies on the Web makes information about what sites we visit and what software we own easier to track.

Even if we are able to access the Web from a private ISP, the use of Caller ID software and system callback are making it increasingly difficult to remain anonymous. As authentication mechanisms improve and the cost of disk space for logs drops, it will become even harder to obtain anonymity.

3) *Once we delete a file, it's gone!*

When you delete a file, it is not removed from the disk. Additionally, it has been proven by some forensics experts that a file can be retrieved even after it has been overwritten nine times. At that level, an electron microscope is required. However, files overwritten up to two times can be retrieved using currently available software. To effectively remove a file permanently, a program such as Wipe Disk, which overwrites a file or drive with 0s, 1s, and then 0s again, should be used. (There are some individuals who believe they can still successfully retrieve at least portions of the data from the actual physical memory.)

C. Where the exposure lies

Due to lurking threat to computer security, we need to look at where the holes lie in systems and networks that allow these hackers to be successful. These security holes, which can be due to misconfiguration or poor programming, should be identified for several reasons. First, common security holes are the areas the organization should address quickly. We need to either close the hole or learn more about it in order to mitigate the risk created by the exposure. Second, the common holes are the areas we need to look for during our penetration test. These holes are often called the "low-hanging fruit" in reference to being fairly easy to identify and exploit.

Breaking into systems can be relatively simple if someone has not properly patched and secured the systems against the latest vulnerabilities. Keeping systems up to date has become increasingly difficult with larger multi-OS distributed networks and smaller staff budgets. The issue facing administrators trying to keep systems up to date is that 20–70 new vulnerabilities are published each month on Bugtraq, eSecurityonline,

and other vulnerability services. Unfortunately, hackers have a window of opportunity between the time someone publishes the vulnerability and the time the vulnerability is patched or addressed on the systems. The longer this window stays open, the more the odds of compromise increase. One of the keys to keeping our network secure is to constantly monitor for emerging vulnerabilities and to patch our systems against them. The more responsive administrators are to closing the holes, the more secure our systems will be.

Configuration errors create a risk that enables attackers to penetrate systems. Examples of configuration errors include leaving unnecessary services open, assigning incorrect file permission, and using poor controls for passwords and other settings that a system administrator can set. Organizations can reduce configuration errors by creating baseline standards and configuration management procedures. In addition, proper penetration testing will identify many configuration holes that could allow an attacker to gain access to systems.

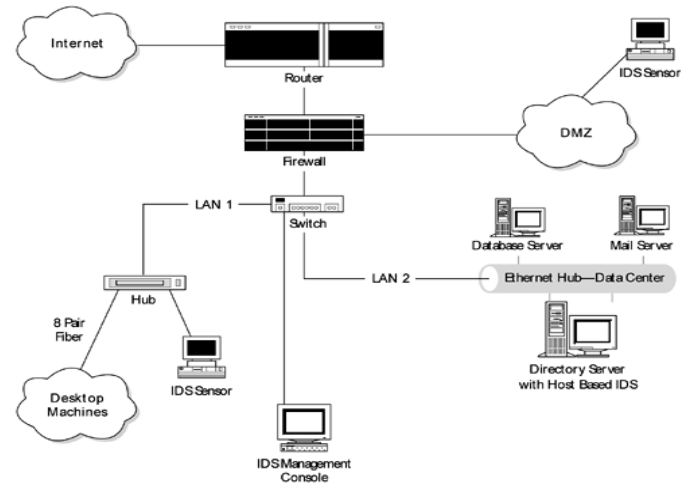
There is no way to close all possible access points to a network. With enough time or money, any system could be compromised. However, keeping patches up to date and testing our systems will effectively close 80–90 percent of the holes.

II. INTRUSION DETECTION SYSTEM (IDS)

Of the security incidents that occur on a network, the vast majority (up to 85 percent by many estimates) comes from inside the network. These attacks may consist of otherwise authorized users who are disgruntled employees. The remainder comes from the outside, in the form of denial of service attacks or attempts to penetrate a network infrastructure. Intrusion detection systems remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate network.

One of the key countermeasures against network compromise is an intrusion detection system (IDS). A well-configured IDS is a critical element in information system security. Given ample time to probe defenses and find holes in a system, a hacker will find a way to compromise the network, even against the best perimeter defenses. Therefore, no security posture is complete without a way to detect and respond to hacker activity. This is what an IDS offers.

Now we offer techniques for evading IDS during penetration testing and explain when they should be used. Based on these techniques, we present a few leading practices for properly configuring an IDS to detect intrusion attempts.



Generally, IDSs are deployed with multiple sensors in various locations on the network reporting to a central management console through which IDS alerts can be seen and the sensors can be managed. An IDS sensor monitors traffic running across its interface into the network and looks for traffic patterns that match particular rules and signatures within the tool's rule set. When a particular rule is matched, an alert is sent to the management console. In addition to alerts, IDS can be configured to send pages, e-mails, and other notification actions.

A rule set contains rules that identify unusual or unwanted behavior as well as traffic signatures representative of known attacks and exploits. A rule can identify one or more options or thresholds, such as protocol, source and/or destination domain, IP address and/or port, and quantity of occurrence. For example, attempts by a user to access root-level files can cause alerts. An alert triggered by three consecutive failed login attempts is a classic example of a rule designed to alert an administrator of unusual activity. Also, rules can be developed to send alerts about certain events only if they involve a particular source or destination (determined by domains, IP addresses, ports, and so on). For example, zone transfer queries against a domain name server from a machine other than a domain name server may raise enough suspicion to trigger an alert.

A signature is code representing the traffic patterns associated with particular attacks. For

example, the Tribe Flood Network 2000 (TFN2K) distributed denial-of-service tool, which floods its target with various TCP, UDP, and/or ICMP packets, uses the same value in the header length field of the header of each TCP packet it transmits. Further, each packet ends in a string of 'A's (hex 0x41). These recognizable characteristics can form the signature for this attack. When the IDS sensor identifies packets matching this signature, it can signal an alert for TFN2K and can be configured to take further action, such as sending an automatic e-mail or a page. Further action is also possible, such as executing a script and forcing a connection to be dropped at the firewall.

IDSs can be either network-based or host-based. As their names suggest, a network-based IDS monitors traffic over the network and generally looks for traffic that is evidence of network-based attacks. SYN flood denial-of-service attacks and port scanning are two examples. A host-based IDS, on the other hand, monitors and protects a single host and looks for evidence of unusual activity on or against that host. You can configure host-based IDSs to monitor and alert for traffic signatures such as an unusual number of login attempts to single or multiple users' accounts, login at an unusual time, or attempted access to file(s) in a directory to which the user does not have access privileges.

These two kinds of IDSs are generally located in different places on the network. In either case, you must locate the IDS sensors in positions where they can view all the traffic of concern. The sensor for a network-based IDS (NIDS) is generally placed on segments that contain critical servers. NIDSs may also be deployed behind the firewall or on the main router or switch for the network. A host-based IDS (HIDS) more commonly is found on hosts that are of particular interest or are more likely to be targets of attack, such as a DMZ Web server or a back-end database server. One of the most well known and widely used intrusion detection systems is the open source, freely available Snort. It is available for a number of platforms and operating systems including both Linux and Windows

III. INTRUSION PREVENTION SYSTEM (IPS): NEXT GENERATION IDS

The inadequacies inherent in current defences have driven the development of a new breed of security products known as Intrusion Prevention Systems (IPS). Whilst it is true that firewalls, routers, IDS

devices and even AV gateways all have intrusion prevention technology included in some form, still IP systems are proactive defence mechanisms designed to detect malicious packets within normal network traffic (something that the current breed of firewalls do not actually do, for example) and stop intrusions dead, blocking the offending traffic automatically before it does any damage rather than simply raising an alert as, or after, the malicious payload has been delivered.

An IPS is the next security layer to be introduced that combines the protection of firewalls with the monitoring ability of IDS to protect our networks with the analysis necessary to make the proper decisions on the fly.

IDS provide real-time alerts and reports. What they do not provide is the necessary intelligence to notify all network components downstream and upstream from the point of identification. This is where IPS becomes part of the overall layered approach to security. IPS gathers all network information and makes the determination of the threat, then notify all other devices of those findings. Upstream providers can notify downstream customers of possible attacks before or during the event as that malicious attempt arrives and vice versa.

Within the IPS market place, there are two main categories of product: Host IPS and Network IPS.

- Host Based:** A host based IPS (HIPS) is one where the intrusion-prevention application is resident on that specific IP address, usually on a single computer.

- Network Based:** A network based IPS is one where the IPS application/hardware and any actions taken to prevent an intrusion on a specific network host(s) is done from a host with another IP address on the network (This could be on a front-end firewall appliance.)

Network intrusion prevention systems (NIPS) are purpose-built hardware/software platforms that are designed to analyse, detect, and report on security related events. NIPS are designed to inspect traffic and based on their configuration or security policy, they can drop malicious traffic.

IV. CONTRAST WITH INTRUSION DETECTION SYSTEM (IDS)

IPS systems have some advantages over intrusion detection systems (IDS). One advantage is they are designed to sit inline with traffic flows and prevent attacks in real-time. In addition, most IPS solutions have the ability to look at (decode) layer 7 protocols like HTTP, FTP, and SMTP which provides greater awareness. However, when deploying network based IPS (NIPS), consideration should be given to whether the network segment is encrypted or not as many products are unable to support inspection of such traffic.

V. IMPLEMENTATION CHALLENGES

Although similar to IDS, IPS has challenges of their own. These include:

- Network design
- Network traffic saturation
- Frequent updates
- False positives

Like IDS, IPS must be designed and scalable enough to accommodate any network design. Network traffic saturation must also be considered to ensure the additional IPS network traffic does not bring down the network. Finally, frequent updates and false positives are the same menace to IPS as they are to IDS. Simply put, software and signature files will need updating. This poses problems simply due to the manpower or work involved. False positives, on the other hand, have been the very reason IDS programs or projects collapse. IPS have a distinct advantage in this area only because other network device information will be gathered, and decisions are not based on one set of data but many. False positives are always an issue due to the large amounts of data IDS must collect and then analyze in real-time with limited AI. Signatures do a decent job of analysis, but they still do not contrast to the interaction IPS will provide.

IDS appear much easier to implement into a network with the use of TAPS (device used to tap a wire and not disrupt communication) and other devices. The introduction of IPS may require more work only because they must be introduced into the entire network infrastructure, not simply tap in on a network segment. IPS will need to the following first configured, then maintained: rules setup/management, system tuning, packet decode/tune, packet rules, console and database. As

with many other technologies, these are the bare bones essential functions, thus acceptable.

VI. REQUIREMENTS FOR EFFECTIVE PREVENTION

Having pointed out the potential pitfalls facing anyone deploying these devices, what features are we looking for that will help us to avoid such problems?

In-line operation - only by operating in-line can an IPS device perform true protection, discarding all suspect packets immediately and blocking the remainder of that flow

Reliability and availability - should an in-line device fail, it has the potential to close a vital network path and thus, once again, cause a DoS condition. An extremely low failure rate is thus very important in order to maximise up time, and if the worst should happen, the device should provide the option to fail open or support fail-over to another sensor operating in a fail-over group.

Resilience - The very minimum that an IPS device should offer in the way of High Availability is to fail open in the case of system failure or power loss. Active-Active stateful fail-over with cooperating in-line sensors in a fail-over group will ensure that the IPS device does not become a single point of failure in a critical network deployment

Low latency - when a device is placed in-line, it is essential that its impact on overall network performance is minimal. Packets should be processed quickly enough such that the overall latency of the device is as close as possible to that offered by a layer 2/3 device such as a switch, and no more than a typical layer 4 device such as a firewall or load-balancer.

High performance - packet-processing rates must be at the rated speed of the device under real-life traffic conditions, and the device must meet the stated performance with all signatures enabled. Headroom should be built into the performance capabilities to enable the device to handle any increases in size of signature packs that may occur over the next three years. Ideally, the detection engine should be designed in such a way that the

number "signatures" (or "checks") loaded does not affect the overall performance of the device.

Unquestionable detection accuracy - it is imperative that the quality of the signatures is beyond question, since false positives can lead to a Denial of Service condition. The user **MUST** be able to trust that the IDS is blocking only the user selected malicious traffic. New signatures should be made available on a regular basis, and applying them should be quick and seamless.

Fine-grained granularity and control - fine-grained granularity is required in terms of deciding exactly which malicious traffic is blocked. The ability to specify traffic to be blocked by attack, by policy, or right down to individual host level is vital. In addition, it may be necessary to only alert on suspicious traffic for further analysis and investigation

Advanced alert handling and forensic analysis capabilities - once the alerts have been raised at the sensor and passed to a central console, someone has to examine them; correlate them where necessary, investigate them, and eventually decide on an action. The capabilities offered by the console in terms of alert viewing (real time and historic) and reporting are key in determining the effectiveness of the IPS product.

VII. CONCLUSIONS

Security is a very difficult topic. Everyone has a different idea of what "security" is, and what levels of risk are acceptable. The key for building a secure network is to *define what security means to your organization*. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy.

IPS may not be the final answer to computer security, but it is a good start that further supports the firewall-to-IDS protection methodology. As with any other technology, there are testing results and configuration changes that can make or break the use of IPS in any company. The associated return-on-investment (ROI) must also be considered due to the already considerable amount of money spent on current network components. Senior management must be informed that IPS are an additional technology that will enhance and layer the ability of the firewalls and IDS to mitigate the risk of attacks and malicious code, thereby protecting the company and customers. As the

threat increases almost daily this new technology will provide another layer of protection to our already well-protected systems. We can no longer afford the manpower necessary to monitor the many network components and computers that exist today. IPS provides the solution to automatically response in a trusted solution to threat as it occurs, not afterwards or when a human has time to verify the event.

REFERENCES

- [1] *Introduction to Network Security* by Matt Curtin March 1997
- [2] *Hack Proofing your own network* by Michalis Georgiou
- [3] http://nsslabs.com/WhitePapers/intrusion_prevention_systems.htm
- [4] *IDS and IPS: Information security technology working together* by Edward P Yakobovicz, CISSP
- [5] *Introduction to Intrusion Detection Systems (IDS)* from Tony Bradley, CISSP, MCSE2k, MCSA, A+