SANS Institute
Information Security Reading Room

Intrusion Detection and Prevention Systems Cheat Sheet: Choosing the Best Solution, Common Misconfigurations, Evasion Techniques, and Recommendations.

Phillip Bosco

Copyright SANS Institute 2019. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Intrusion Detection and Prevention Systems Cheat Sheet: Choosing the Best Solution, Common Misconfigurations, Evasion Techniques, and Recommendations.

GIAC (GCIA) Gold Certification

Author: Phillip Bosco, PhillipBosco@gmail.com
Advisor: Hamed Khiabani, Ph.D.
Accepted: January 20, 2016

Abstract

Security professionals seeking to secure their networks against constant cyber attacks are challenged by the flood of options. In particular, they can be daunted by the many dimensions of implementing Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). The author will first summarize some of the most effective ways to identify and implement an IDS/IPS for your organization, and then will move into the common misconfigurations identified across the various solutions available and how the misconfigurations can be actively exploited by a malicious actor. The author will first summarize the setups and configurations that companies commonly use for their IDS and IPS solutions, then will move into the many ways that these systems can be bypassed and evaded. With each technique and tool covered, the author will highlight the common IDS/IPS misconfiguration that the tool takes advantage. Lastly, the author will make recommendations for more secure IDS/IPS that aim to increase not only the security of the system itself, but the company's security posture as a whole.

© 2016 The SANS Institute Author retains full rights.

1. Introduction

There are many decisions a company must make while choosing an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) for their infrastructure. Pricing questions will arise to determine if it will fit into their budget. Does the system require only a one-time purchase, or is there a yearly subscription? Will the security team need training to properly setup, operate, and maintain this new equipment? Most importantly, however, should be the all revealing question of, "…but will it work?"

Deciding whether an IDS or IPS system is the right choice for a company will depend on what their unique goals and objectives are (ScriptRock, 2015). In the wake of very successful and high profile cyber attacks against banks (Farrell, 2015), technology companies (Poeter, 2013), retail stores (Wallace, 2013), movie studios (Betters, 2015), and the United States government (Vaughan-Nichols, 2015), a large number of companies are looking to ensure that they are not the next victim to headline on the evening news reporting a devastating breach. This sense of urgency can also entice panic, which commonly results in poorly managed finances and improperly managed security systems. This causes security managers to use their security budgets inefficiently by throwing money at all of their problems in an attempt to find a solution sooner than later (Kotler, 2016). It certainly does not help the situation when misinformation is shown on billboards, brochures, and across the internet which showcase many vendor's claims that their security device is the all-in-one security system. Some claims are as preposterous to say that they "hacker-proof" your network, or even automate penetration tests for you (ENISA, 2013). Regardless, the fewer security professionals that buy into these inaccurate claims and purchase expensive devices for their network, the better. It is important not to let the sense of urgency overtake an educated and responsible decision-making process. A security professional must ask themselves what it is that they are trying to defend and protect, and if a six-figure solution will be a better option for the task over a freely distributed, well-supported, industry standard solution (Lepofsky, 2011).

Once a security professional decides on an IPS or IDS system, it must be installed, operated, and maintained properly. While some IDS/IPS systems require less fine-tuning than others, this should never be an excuse to plug the device quickly in and

© 2016 The SANS Institute Author retains full rights.

expect it to perform all of the vendor's promised tasks that were printed on the side of the box (Shinder, 2005). Hopefully, employee training was taken into the decision-making process when choosing an IDS/IPS. If training or certification is necessary to maximize the benefit of the security solution, then sending employees to training prior to implementing the new security system would be the wisest decision. It is all too common for a company to possess a false sense of security from their improper, incomplete, and insecure configurations on their IDS/IPS system. An experienced penetration tester can attest to seemingly countless kick-off and scoping calls with their clients when the point of contact for the engagement declares the highly secure nature of their network. Statements such as, "I'll tell you now, we execute regular vulnerability scanning, we use full-disk encryption on all workstations, we perform weekly patching of our systems, and have an active IDS and IPS in place. I'm confident you will not be able to penetrate our systems." – To which a seasoned penetration tester might respond with, "Challenge accepted."

While the client may be correct with the information they provided, what they did not say was that their weekly patching of systems excluded the antiquated Windows XP Service Pack 2 system on their network, which exists solely due to compatibility reasons with legacy software. Alternatively, they might have left out that the IDS that they praised and paid tens of thousands of dollars for was taken out of the box, plugged into the network, and powered on without any customization or configuration performed. The same penetration tester is also very successful at dropping the jaws of the client's security manager when he was successful at bypassing host-based antivirus solutions to execute a payload across the network, pass authentication hashes using the Server Message Block (SMB) protocol utilizing the Pass-the-Hash (PtH) technique, authenticating to the domain controller as a domain admin, and creating a new backdoor account on the domain all without alerting a single system administrator. How can this be possible? While the root causes can be a number of things, if we focus solely on IDS/IPS, it commonly boils down to one (or both) of two things: Insufficient IDS/IPS in place or an improper configuration of an otherwise adequate IDS/IPS.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

2. Security-in-Depth Mindset and Methodology

Before covering specific recommendations to harden the network device, we must first address the optimal mindset and thought process behind any successful IT or security professional. This mindset broadens their focus and trains their brain to think in layers and depth, rather than on isolated and individualized issues. For example, a company may keep fully up to date on all of their patches, antivirus signatures, and even perform regular vulnerability scanning within their network; however, this combination does not always translate into an effective defense solution. To think securely, one must significantly broaden their thoughts in order to refrain from focusing only on a single element of security.

Many security professionals are already familiar with the idea and the importance of implementing security in layers (Perrin, 2008). It is all too common for security professionals to misinterpret what a security in layers actually looks like in an organization. It is not just an idea, concept, or term that is used to give people the warm and fuzzy disillusioned sense of security; it is also a methodology (Mah, 2012). Professionals in the security industry, especially penetration testers, know how fundamentally critical it is when a company does not implement security in layers. For example, a penetration tester might obtain credentials through a successful phishing attack that could be used on the externally facing Virtual Private Network (VPN) portal. If the organization had implemented two-factor authentication, the cheer and excitement that a penetration tester previously expressed will be short lived, as this would effectively stop the consultant from authenticating successfully to the company's VPN (Kee, 2013). While this aforementioned implementation of two-factor authentication may be suitable for some companies, this security can always be expanded upon. A company may choose also to limit their employees' access to the internal network when connected through the external VPN, rather than giving a VPN user privileged access to all of their internal systems.

With networks growing in complexity through new technologies and as we step into the generation of the Internet of Things (IoT), it can become very difficult to stay on top of each individual issue that arises (Chickowski, 2014). It is commonplace to add new

© 2016 The SANS Institute Author retains full rights.

Internet-connected devices, such as light bulbs and toasters to our networks, that only increase the available footprint to a malicious actor. Given the convenience and accessibility that these connected devices offer, they are often implemented without given much thought, especially in regards to how they may negatively impact one's security posture. As the IoT is growing exponentially each year, vendors are quickly pushing out new connected devices at a rapid pace and may be underestimating the need for proper security testing prior to release. Windows, Mac, and mobile phone operating systems are updated and patched regularly, but as we are maturing into the IoT generation, regular patching and updating of these potential vulnerable network devices is severely lacking. Convenience and security are always engaged in a constant battle with one another and each struggling for the upper-hand; however, history has taught us that when convenience increases, security will decrease and vice versa. Realizing what the full impact of each server, workstation, or other network connected device will be when added to your network is a significant part of mastering the security in depth mindset.

On any given Monday, a network administrator might be told that their external network is under a Denial of Service (DoS) attack and is denying legitimate user's access to the website due to a misconfiguration in the way that the load balancers route, throttle, and allocate bandwidth to clients. On Tuesday, Microsoft may release a security bulletin for a critical zero-day vulnerability in which there is no patch for, but a series of registry-editing work around methods to temporarily mitigate the issue until an official patch arrives. On Wednesday, the antivirus software that your company uses fell behind the other antivirus vendors and did not release an updated signature for the latest worm that threatens corporate networks. For members of blue teams of any size, this day-to-day picture painted here is not an exaggerated scenario, but an unfortunate reality and accurate depiction for most. Until we think in layers and build and implement a security posture, a strategic mindset, and address issues at their core, we will always be stuck chasing our metaphoric tails and will never get ahead of the new and dangerous threats that emerge daily.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

3. Choosing an IDS or IPS System

The first and most important question to ask yourself when choosing an IPS/IDS solution should not focus on the cost, vendor, or training requirements of the system. But rather, one should ask themselves "What is it we are really trying to protect?" It is easy to get caught up in the details of a complex system, however, we need to be sure that we are focusing on what is most important. For example, when a successful marketing manager is speaking with a client, they will not ask about the client's budget, but instead focus only on what the client's direct goals are and what they truly desire to accomplish. One great question that marketing professionals ask their clients is, "If you had an unlimited budget, what goals would you work towards to rebrand and market your company?" Some may argue that this question is a waste of time, as we all are bound to budget constraints. However, the purpose is to provide a laser focused mindset on the goals and intended end results, rather than cost. Based off the goals that are decided on with an unlimited budget in the forefront of one's mind, only then will the marketing professional start figuring out how to optimally meet their client's goals within the defined budget constraints. It may surprise some how a client's goals differ when presented with the idea of an unlimited budget! With this exercise in hand, it is good practice to put this concept into play within your own mindset when making decisions to secure your company's network and sensitive data.

Once the goals are decided on, we now have what is required to choose a solution that best fits our high-level agenda. This allows us to narrow greatly our search outside of any budget limitations. Searching for an IDS/IPS system is now much easier to manage as one can directly align their goals with the bullet-pointed specifications of each system. Using this method, one may be surprised that they can actually achieve their goals for very little, rather than spending a large and unnecessary mound of resources on a system that is either overpriced or provides features that will never be used by the organization. Just as it is important to ensure that one chooses a system that meets their existing goals, keeping in mind future goals, objectives, and your company's expansion in the near-future will also be highly beneficial in this decision making process. Finding the balance between meeting your current goals, while leaving room for expansion in the near future will minimize the workload and resources required later on when the need for these new

© 2016 The SANS Institute Author retains full rights.

features are required (Evans, 2015). In the same process, it is imperative that one stays grounded in reality and does not become overzealous. Even if the case that a security professional is given a large budget and can afford a powerful system that is loaded with features, overspending on a single aspect of securing your network may result in underspending on other overlooked areas of security. Outlining your goals does not just assist in your ability to pick the most optimal IPS/IDS system for your organization, but also has the potential to maximize and stretch the effectiveness of your existing budget.

Up until this point, IDS and IPS have been used together as if the two systems are interchangeable. While they both serve a similar purpose, determining which system to use for your network is crucial. Placing an IDS where an IPS system should ideally be may completely render the IDS system useless, a waste of resources, interrupting to the company's legitimate traffic, or provide the company with a false sense of security. While it is important to do your own research on the core differences between an IDS and IPS system, the key concept to keep in mind is whether the system should simply detect and log potentially malicious activity or block it entirely. This decision belongs only to the security professional for each organization and should align with the company's objectives. Some may argue that an IPS is better than an IDS as it maintains the ability to block completely potentially malicious traffic, which in turn might completely stop attackers in their tracks; however, this is simply not the case. The choice between an IDS or IPS system depends solely on meeting the goals of your organization, without causing unnecessary network connectivity issues for legitimate users on the network. Likewise, an improperly secured IDS or IPS system is just as useless and hazardous as placing an IDS in the place of where an IPS should be instead, and vice versa.

On a penetration test, a security consultant may find that outbound traffic is being blocked out of all of the attempted ports, either through strong egress filtering or content inspection of his malicious traffic. Eventually, the security consultant attempts Transmission Control Protocol (TCP) port 443 for the reverse connection of his malicious payload and successfully obtains persistent access into the company's network. Why was the security consultant able to achieve this? While there was an IPS configured to block nearly every outbound connection as well as perform traffic inspection, port 443 was an exception. Allowing 443 outbound traffic is not necessarily a security vulnerability on its

© 2016 The SANS Institute Author retains full rights.

own, but the insecurity in this instance was in regards to how the IPS did not perform traffic inspection on this port for malicious payloads. Typically, all traffic occurring on this port is typically fully encrypted. As such, it is a common misconfiguration to deny this common port from undergoing traffic inspection by a company's IPS. Many organizations have not set up their systems to decrypt the encrypted traffic and analyze it before either blocking the traffic or allowing it through the network. To ensure that legitimate users do not see their own traffic blocked, the IPS was configured to allow all encrypted traffic through this port, creating a backdoor that the consultant could take full advantage of!

For some, this may sound like a no-brainer to simply set up the IPS or IDS to decrypt all encrypted traffic before passing it on to the internet. While conceptually simple, the implementation is not quite as straight-forward as many factors must first come into play. First and foremost, not all IPS/IDS devices are designed to work as a proxy that can decrypt traffic, so this feature must always be considered while deciding on the system that will best meet your company's objectives. Additionally, cost will also come into play, as the systems that are specifically designed to work as a proxy typically cost more. This premium cost is also dependent on how much anticipated bandwidth will need to be sent through your network. If the IDS/IPS system is used as a proxy, we must now fully account for all of the traffic of the organization and determine if the proxy IDS/IPS you plan to use can handle the bandwidth necessary without slowing the network or bringing it to a complete stop (Pascucci, 2013).

Another element to consider when choosing an IDS/IPS proxy is how the device reacts when presented with more traffic than it can handle, which may occur during the peak hours of your network's traffic such as first thing in the morning when all of the employees come into work and are authenticating to the network at the same time. This is where a balance of security and usability must be made. Is security so important on this network segment that if an IDS/IPS becomes overloaded with more bandwidth than it can handle, that all traffic must be denied until the device has time to properly analyze all the traffic in its queue? Or perhaps usability is most important and in the case that an IDS/IPS is overloaded, it will simply resort to a fail-open condition that passes all traffic through without inspection until it has the resources available once again to properly

© 2016 The SANS Institute Author retains full rights.

analyze all traffic passing through it? Striking a balance here between what makes the most sense for this network segment and the available budget is critical (Paquet, 2009). In a perfect world, we would all have a proxy IPS that decrypts and analyzes all traffic out of all of the ports, both inbound and outbound, to keep our networks as safe as possible. Unfortunately, this is not always affordable or realistic.

While we suggested to start the decision making process with keeping a budget intentionally out of mind, that exercise was used to cut away the unnecessary details and allow a security professional to fully realize what their true unrestrained goals were. Budget is very important, as outlined above in the discussion of whether to use an IDS or IPS and if a company can afford a system that supports their bandwidth requirements. Another important aspect of budget to consider is whether the IPS/IDS would require sending the employees to a training course provided by the vendor to properly install, operate, and maintain the new equipment. The security manager may have truly found the best IDS/IPS on the market, but unless the employees know how to configure and harness this system, it is just as ineffective as not having any system in place at all! Even if the IDS or IPS does not necessarily require training for operation, allowing the employees the opportunity to further their working knowledge of the systems to learn some advanced techniques may be a great benefit to the company (Juniper, n.d.). The decision on whether or not to send employees to training should never be based on whether or not a company can afford it, as the cost of any necessary training should be considered directly into to the cost of the system itself. For example, if a company has a $10,000 budget to spend on an IDS/IPS, but the system recommends that employees are certified to properly operate the equipment, the cost of the actual hardware and software must be below the $10,000 budget ceiling in order to account for the added cost of employee training. This is not an area of security implementation where it is advised to take shortcuts.

Another aspect surrounding the budget limitations when choosing a system is whether the system requires an annual subscription for support or operation, or if the system requires only a one-time purchase fee. If the system requires an annual fee of $1,000 for support of the system by the vendor, keep in mind that for each fiscal budget year, $1,000 must be taken out of the budget every year that this system is utilized. This

© 2016 The SANS Institute Author retains full rights.

is not necessarily a negative option or a poor choice, especially if it allows you to meet the security requirements and goals for your network; however, it is important to determine if this is a cost that is absolutely necessary or if there are other systems that do not require an annual fee for support or operation from the vendor.

4. The Critical Importance of Penetration Testing

Security is a constant and evolving process and no security solution will ever result in a completely bulletproof solution when presented against time and determined individuals. Even in the best case scenario where a company has, at least on paper, implemented their IDS/IPS securely and their employees have been fully certified to operate the equipment, there will always be exploitable conditions or misconfigurations that may not be immediately apparent. All of the implementation and operational training currently offered may never prepare one against minds and determination of malicious actors. For example, prior to the deadly attacks on September 11th, 2001, airlines were considered safe-enough with the light screening performed on passengers before flying. However, the terrorists exploited weaknesses in the passenger screening systems that enabled them to successfully execute terrible things. In light of these attacks and to ensure that nothing so terrible could happen again, the Transport Safety Administration (TSA) was born (NMAH, 2011). While the TSA provided passengers with much more security screening than ever before, malicious passengers still have been successful in exploiting the process throughout the TSA's short history. Some have brought shoe bombs on the plane or other dangerous and prohibited items (CNN, 2009), which prompted the TSA to further revise their security screening process. Keep in mind that any solution, no matter how seemingly secure in the moment, will stand up against the test of time in conjunction with the brilliant and persistent minds of some malicious actors. Rather than setting up all of the controls and security systems in place and waiting patiently with fingers crossed that an attacker does not successfully penetrate your network, all systems and devices must be tested using a reputable penetration testing company.

© 2016 The SANS Institute Author retains full rights.

Be proactive in assessing your network by security professionals that specialize in penetration testing, as opposed to waiting until all of your most precious company data has been posted online for the world to see by some loosely knit hacker organization. Even the TSA themselves undergo penetration testing by trusted government officials to assess the effectiveness of their current screening policies and procedures. These tests determine if malicious items can be brought on board of a flight without detection. Similarly, a company that does not undergo penetration testing is unlikely to discover configuration oversights in the IPS/IDS, or other critical security vulnerabilities in the network as a whole (Basu, 2013). A penetration test performed against your IDS/IPS and your network as a whole should, at least internally, be considered a requirement rather than an optional commitment. In July 2015, penetration testing became a requirement for companies that fall under the Payment Card Industry (PCI) compliance standards (Thomas, 2015). PCI 3.0 lists its own penetration testing requirements that must be included within the scope of the test in order to meet the compliance standards. However, if a penetration test is being performed outside of the PCI mandatory compliance, it is important to not leave anything out of the testing scope. Some may choose to leave some outdated machines out of the testing scope for one reason or another, but a cyber criminal will not respect the same scope of limitations that is placed on the penetration tester. Therefore, allowing the penetration testing access to all of your systems and not leaving anything out of scope will ensure that your true risk is fully assessed and realized during the engagement.

5. Attacker Techniques and Methodologies

In a previous example, a penetration tester effectively bypassed a company's installed IPS. This is the same type of mindset that an attacker possesses by leveraging a company's budget constraints and through exploitation of common misconfigurations within a network. While some attacks utilize brand new techniques and brilliantly bypass security measures in place, most of the common attacks seen today exploit predictable and common misconfigurations within the target environment. For example, if a malicious actor has determined that a company utilizes a predictable naming structure for their corporate email accounts, such as "john.smith@company.com", then the malicious

© 2016 The SANS Institute Author retains full rights.

actor has successfully solved half of the authentication puzzle for most organizations. By quickly executing a search on the popular professional networking site LinkedIn, a malicious actor can build a list of hundreds or even thousands of valid employee email accounts in a matter of minutes (Larch, 2015). Once a malicious attacker builds this list, they may attempt to locate a publicly accessible portal to authenticate with via Domain Name System (DNS) subdomain enumeration against a common wordlist of subdomains that include entries like, "mail.company.com" or "vpn.company.com" (Perez, 2014). After the malicious actor has enumerated an external portal to authenticate with, the only key that a malicious actor is missing at this point are the employees' passwords.

In many cases, companies implement a password policy that requires employees to change their password every 90 days. In theory, this is a secure and recommended policy; however, this can easily be abused by malicious actors. Almost coincidentally, every 90 calendar days we are presented with a new season of the year. Therefore, we start identifying a trend on 90% of penetration testing engagements whereby the security consultant identifies weak passwords following the 'season/year' pattern such as "Fall2015" in use (NPDN, 2015). If two-factor authentication is not enabled, the malicious actor would have gained access into this company's network and systems by simply abusing common misconfigurations and insecure trends without any Hollywood-style "hacking" required.

While IDS and IPS are not typically the target of direct exploitation, ensuring that the systems are not only configured securely but also do not possess the same predictable weaknesses that other systems of its category possess is crucial to the system's effectiveness. By attackers understanding the most common configuration flaws and trending oversights in intrusion systems, effective evasion techniques are born and used in the wild. As in a previous example, a penetration tester bypassed the IDS by simply choosing to flow his malicious traffic through port 443, which in that case, did not undergo traffic inspection by the IDS/IPS since traffic on port 443 is usually encrypted. This was one of very many common trends that the penetration tester took full advantage of to evade the security system in place.

Many tools, such as the network port scanner Nmap or the web scanning vulnerability tool Nikto utilize various IDS/IPS evasion techniques (Gerg, 2004). The

© 2016 The SANS Institute Author retains full rights.

incorporated evasion methods take advantage of commonalities between popular intrusion systems. These programs can make evading an IDS/IPS trivial for a malicious actor or penetration tester by simply providing the appropriate flags within the command syntax. Nmap, for example, supports many methods for evasion and can be changed based on the particular environment (Nmap, n.d.). One supported method includes throttling the timing of the scan to slow Nmap's traffic down, which may be effective in evading some systems. Additionally, fragmenting the packets in a scan into multiple chucks through manipulation of the MTU settings may also be effective at evading IPS/IDS. In other cases, it may take a combination of various supported methods to skirt around a system's detection boundaries. Of course, port scanning a target or attempting to identify vulnerabilities with a scanner using IDS/IPS evasion is only the beginning. Once potentially exploitable vulnerabilities or misconfigurations are identified, the next step is attempting to exploit them.

IDS/IPS are typically configured to detect common exploits crossing the network, such as the widespread MS08-067 vulnerability and exploit (Hittel, 2008). However, there are tools exist that can exploit vulnerabilities while still evading common IDS/IPS configurations and signatures. Metasploit Pro allows its users to set predefined levels of evasion, ranging from transport layer evasions or application layer evasions depending on the particular environment (Kirsch, 2012). Also supported are the common and previously mentioned IDS/IPS evading method of fragmenting the exploit traffic as well as the ability to encode the payload to bypass signature based systems. These industry standard tools leverage the common misconfigurations of popular IDS/IPS because many of the methods are still effective today. One of the best tools in a penetration tester's toolbox is to simply have as many options as possible while performing a test. Possessing numerous options when encountering an unknown network or system is important as is not a one-size-fits-all approach to penetration testing, and oftentimes, systems and networks must be poked and prodded with various tools to identify the weaknesses within.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

6. Remediation

As there are many methods that can be used to bypass a company's IDS/IPS, just as many remediation and mitigation solutions exist to secure against the common attacks. Unlike an application security flaw, a single patch from the vendor will not be able to solve your IDS/IPS insecurities and make them immune from these evasion methods. This underscores the importance of following the proper steps when choosing an IDS/IPS for your organization which enables the user to ensure that the system can achieve the goals required to keep an organization secure. Making certain that the individual or team that will be responsible for implementing the IDS/IPS also receives the appropriate training or certification for the system will only increase the success that the system will be able to resist the common evasion techniques used in the wild. One cannot protect their organization against attacks when they do not fully realize the defensive and logging mechanisms available to them at their disposal.

It can be a daunting task to defend against such a vast array of tools that offer numerous forms of IDS/IPS evasion techniques; however, the silver lining to malicious actors having access to a large number of tools that support evasion methods is that there are now established security expectations that can be aimed for in how your system reacts to various stimuli from these tools. When we have access to the same tools that support evasion that are actively used by attackers, we can test our own systems against these industry standard tools and the included evasion methods to determine where the systems demonstrate weakness and make the appropriate configuration tweaks to secure them against common attacks. It may be out of a network engineer's skillset to not only understand the various tools used against their network but to also test their systems' defenses themselves. In this case, a third-party consultant can be hired specifically for this purpose. Depending on how advanced your current security setup and policy is, it might not be the most appropriate use of resources to hire a security consultant to start immediately poking holes at your IDS/IPS and other systems on your network. Rather, it may make more sense for the security consultant to start with a configuration review of your IDS/IPS, as well as other security related gear on your network, and enforced security policies. This allows the consultant to make detailed and personalized recommendations on where your policy and configurations are either lacking or

© 2016 The SANS Institute Author retains full rights.

exceptionally adequate. Once these changes are understood and implemented, the systems within your network can then be put under fire in the next testing phase by actively using the numerous tools available to attempt to evade the current configurations.

If no other remediation or mitigation recommendations are followed, the most important of them is to put your current infrastructure and devices through a penetration test from a reputable company. Without actively testing the systems, there is truly no other way to state with absolute confidence that your security systems are effective at reducing risk and securing your organization. Whether five dollars was spent on your security program or 500,000 dollars, it is important to be proactive in your security by having the systems fully tested in a penetration test. Some companies will sit with a false sense of security due to the large sum of money they spent on security; eventually they end up on the evening news headlining the massive breach that occurred against their organization. Be proactive, and have the systems tested to determine flaws that pose a security risk to your organization.

7. Conclusion

Intrusion Detection and Prevention systems are just one more piece of the always-evolving security puzzle. Just as is the case with antivirus solutions, firewalls, password policies, patch management, and security awareness training, intrusion detection and prevention systems must be implemented in conjunction with all other existing security solutions to achieve the best results. Ensuring a security in depth mindset by not relying on one system or countermeasure more than another is crucial to obtaining the highest level of protection on a network. Once the proper balance of security solutions and the layered security approach is achieved, choosing the proper IDS/IPS to meet the organization's goals is important; but this will only be effective when employees understand how to implement, maintain, and harness a system's ability to defend their organization. Executing penetration tests against your company will assist in identifying previously unknown configuration flaws in your IDS/IPS and should be performed regularly and whenever a large change in configurations or devices takes place on your network. While penetration testing is highly valuable in increasing a systems

© 2016 The SANS Institute Author retains full rights.

effectiveness at reducing risk, no system or network is ever impenetrable. As history has shown us, an attacker with enough time has overcome many security systems in place. Performing regular tests against your infrastructure will ensure that your systems continue to hold up against the rapid changes in technology and attack methods. Last but certainly not least, implementing security in layers is the most effective way at reducing risk as each standalone security system may be bypassed on its own, but a proper combination and balance of all security devices, software, and policy in place may be just enough to stop the attackers dead in their tracks.

©2016 SANS Institute, Author retains full rights.

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

References

Basu, E. (2013, October 13). What is a penetration test and why would I need one for my company? Retrieved from http://www.forbes.com/sites/ericbasu/2013/10/13/what-is-a-penetration-test-and-why-would-i-need-one-for-my-company/

Betters, E. (2015, February 5). Sony Pictures hack: Here's everything we know about the massive attack so far - Pocket-lint. Retrieved from http://www.pocket-lint.com/news/131937-sony-pictures-hack-here-s-everything-we-know-about-the-massive-attack-so-far

Chickowski, E. (2014, July 29). Internet of things contains average of 25 vulnerabilities per device. Retrieved from http://www.darkreading.com/vulnerabilities---threats/internet-of-things-contains-average-of-25-vulnerabilities-per-device/d/d-id/1297623

CNN. (2009, December 25). Shoe bomber: Tale of another failed terrorist attack - CNN.com. Retrieved from http://www.cnn.com/2009/CRIME/12/25/richard.reid.shoe.bomber/

ENISA. (2013). No such thing as hacker proof a Deloitte Infographic | ENISA. Retrieved from http://brianpennington.co.uk/2014/01/02/no-such-thing-as-hacker-proof-a-deloitte-infographic/

Evans, B. (2015, July 8). The importance of building an information security strategic plan. Retrieved from https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

Farrell, G. (2015, November 10). JPMorgan's 2014 hack tied to largest cyber breach ever - Bloomberg Business. Retrieved from http://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds

Gerg, C. (2004, August). IDS evasion - managing security with Snort & IDS tools. Retrieved from https://www.safaribooksonline.com/library/view/managing-security-with/0596006616/ch04s04.html

Hittel, S. (2008, October 24). MS08-067 exploited in the wild. Retrieved from http://www.securityfocus.com/blogs/1244

Juniper. (n.d.). Intrusion detection and prevention certification - Juniper Networks. Retrieved from http://www.juniper.net/us/en/training/certification/certification-tracks/idp-track/

Kee, B. (2013, March 8). PCI DSS requirement 8.3: What is two-factor authentication, and when is it required? | Dell SecureWorks Security and Compliance Blog. Retrieved from http://www.secureworks.com/resources/blog/general-pci-dss-two-factor-authentication/

Kirsch, C. (2012, January 6). Metasploit: How to fly under the radar of AV and IPS. Retrieved from https://community.rapid7.com/community/metasploit/blog/2012/01/06/flying-under-the-radar-of-av-and-ips-with-metasploits-stealth-features

Kotler, I. (2015, November 20). SafeBreach 2016 predictions: Top security trends in 2016 : @VMblog. Retrieved from

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

http://vmblog.com/archive/2015/11/20/safebreach-2016-predictions-top-security-trends-in-2016.aspx#.VnyAQJMrLBI

Larch, M. (2015, June 1). Gather contacts from LinkedIn. Retrieved from https://blog.netspi.com/collecting-contacts-linkedin-using-linkedin_crawl/

Lepofsky, R. (2011, February 23). Intrusion detection: Why do I need IDS, IPS, or HIDS? | Network World. Retrieved from http://www.networkworld.com/article/2228598/security/intrusion-detection--why-do-i-need-ids--ips--or-hids-.html

Mah, P. (2012, February 23). How to build multiple layers of security for your small business | CIO. Retrieved from http://www.cio.com/article/2399075/security0/how-to-build-multiple-layers-of-security-for-your-small-business.html

NMAH. (2011, September 1). September 11 and the Transportation Security Administration | National Museum of American History. Retrieved from http://americanhistory.si.edu/blog/2011/09/september-11-and-the-transportation-security-administration.html

Nmap. (n.d.). Firewall/IDS evasion and spoofing. Retrieved from https://nmap.org/book/man-bypass-firewalls-ids.html

NPDN. (2015). Strong and weak passwords | National Plant Diagnostic Network. Retrieved from https://www.npdn.org/infosec_pw_strong

Paquet, C. (2009, June 8). IPS best practices: Network security using Cisco IOS IPS. Retrieved from http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=6

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

Pascucci, M. (2013, March). Determining ideal IPS throughput for new implementation. Retrieved from http://searchsecurity.techtarget.com/answer/Determining-ideal-IPS-throughput-for-new-implementation

Perez, C. (2014, January). DNSRecon | Penetration Testing Tools. Retrieved from http://tools.kali.org/information-gathering/dnsrecon

Perrin, C. (2008, December 18). Understanding layered security and defense in depth - TechRepublic. Retrieved from http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/

Poeter, D. (2013, October 3). Adobe hacked, data for millions of customers stolen | News & Opinion | PCMag.com. Retrieved from http://www.pcmag.com/article2/0,2817,2425215,00.asp

ScriptRock. (2015, April 8). Top free network-based intrusion detection systems (IDS) for the enterprise. Retrieved from https://www.scriptrock.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise

Shinder, D. (2005, July 13). SolutionBase: Understanding how an intrusion detection system (IDS) works - TechRepublic. Retrieved from http://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/

Thomas, T. (2015, May 18). 5 PCI best practices becoming required | PCI Compliance Guide. Retrieved from https://www.pcicomplianceguide.org/five-pci-dss-3-0-best-practices-about-to-become-requirements/

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

Vaughan-Nichols, S. J. (2015, June 29). OPM: The worst hack of all time. Retrieved from http://www.computerworld.com/article/2941754/data-security/opm-the-worst-hack-of-all-time.html

Wallace, G. (2013, December 23). Target credit card hack: What you need to know. Retrieved from http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

Wilkins, S. (2011, June 29). Basic intrusion prevention system (IPS) concepts and configuration. Retrieved from http://www.ciscopress.com/articles/article.asp?p=1722559

Author Name, email@address

© 2016 The SANS Institute Author retains full rights.

Last Updated: May 23rd, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
Enterprise Defense Summit & Training 2019	Redondo Beach, CAUS	Jun 03, 2019 - Jun 10, 2019	Live Event
SANS Zurich June 2019	Zurich, CH	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS London June 2019	London, GB	Jun 03, 2019 - Jun 08, 2019	Live Event
SANS Kansas City 2019	Kansas City, MOUS	Jun 10, 2019 - Jun 15, 2019	Live Event
SANS SEC440 Oslo June 2019	Oslo, NO	Jun 11, 2019 - Jun 12, 2019	Live Event
SANSFIRE 2019	Washington, DCUS	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Cyber Defence Canberra 2019	Canberra, AU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS ICS Europe 2019	Munich, DE	Jun 24, 2019 - Jun 29, 2019	Live Event
SANS Cyber Defence Japan 2019	Tokyo, JP	Jul 01, 2019 - Jul 13, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS London July 2019	London, GB	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Cyber Defence Singapore 2019	Singapore, SG	Jul 08, 2019 - Jul 20, 2019	Live Event
SEC450 Security Ops-Analysis Beta 1	Crystal City, VAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Pittsburgh 2019	Pittsburgh, PAUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Charlotte 2019	Charlotte, NCUS	Jul 08, 2019 - Jul 13, 2019	Live Event
SANS Rocky Mountain 2019	Denver, COUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MDUS	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS San Francisco Summer 2019	San Francisco, CAUS	Jul 22, 2019 - Jul 27, 2019	Live Event
SANS Pen Test Hackfest Europe 2019	Berlin, DE	Jul 22, 2019 - Jul 28, 2019	Live Event
DFIR Summit & Training 2019	Austin, TXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS Riyadh July 2019	Riyadh, SA	Jul 28, 2019 - Aug 01, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
Security Awareness Summit & Training 2019	San Diego, CAUS	Aug 05, 2019 - Aug 14, 2019	Live Event
SANS London August 2019	London, GB	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Crystal City 2019	Arlington, VAUS	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Melbourne 2019	Melbourne, AU	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Krakow May 2019	OnlinePL	May 27, 2019 - Jun 01, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced