Interested in learning more about security?

SANS Institute InfoSec Reading Room

Breaking the Ice: Gaining Initial Access

While companies are spending an increasing amount of resources on security equipment, attackers are still successful at finding ways to breach networks. This is a compounded problem with many moving parts, due to misinformation within the security industry and companies placing focus on areas of security that yield unimpressive results. A company cannot properly defend and protect against what they do not adequately understand, which tends to be a misunderstanding of their own security defense systems and relevant atta...

Breaking the Ice: Gaining Initial Access

GIAC (GSEC) Gold Certification

Author: Phillip Bosco, philimanjaro@gmail.com
Advisor: (Chris Walker)
Accepted: 8/1/2015

Abstract

While companies are spending an increasing amount of resources on security equipment, attackers are still successful at finding ways to breach networks. This is a compounded problem with many moving parts, due to misinformation within the security industry and companies placing focus on areas of security that yield unimpressive results. A company cannot properly defend and protect against what they do not adequately understand, which tends to be a misunderstanding of their own security defense systems and relevant attacks that cyber criminals commonly use today. These misunderstandings result in attackers bypassing even the most seemingly robust security systems using the simplest methods. The author will outline the common misconceptions within the security industry that ultimately lead to insecure networks. Such misconceptions include a company's misallocation of their security budget, while other misconceptions include the controversies regarding which methods are most effective at fending off an attacker. Common attack vectors and misconfigurations that are devastating, but are highly preventable, are also detailed.

1. Introduction

Consider the following scenario. You configured your company's firewalls using the industry recommended configurations and installed all of the latest applicable operating system patches; and still, hackers breached your company's network. This ends up in news headlines across the globe and costs your company millions of dollars in damages. Could your company have prevented this devastating security breach? How did the attackers gain initial access into your network? Where were the lapses in critical security controls? With so many aspects of security to focus on, the advantage in the ongoing cyber battle increasingly belongs to the attacker. Even in the most well-guarded networks, hackers are still finding ways to breach networks and obtain access to sensitive information. How are they doing this? After all, the world is now spending more on security than ever before and the amount continues to rise annually (Thompson, 2014). Unfortunately, this increase in spending on security products, seemingly advanced solutions and additional staff is not resulting in fewer breaches.

While attackers are becoming more sophisticated, many of the most successful attacks are exploiting vulnerabilities in more simple ways (Hong, 2013). It is easy to become distracted with the urgency that is typically involved with applying the newest patch to secure your organization against the latest zero-day vulnerability, which may give an attacker a remote shell to your internal server simply by firing a pre-packaged Metasploit module against it. Patch management is very important and we cannot overlook it; however, we seem to be ignoring simpler aspects of securing our networks. Why stress so much over zero-day vulnerabilities, and not pay equal attention to that highly vulnerable Tomcat web server using default credentials running on the external network (Kirk, 2013)? The impact of an attacker exploiting either of these vulnerabilities may be equally as devastating, but simply adding non-default authentication to your Tomcat server disables many of the well-known and well-documented exploitable conditions (Lee, 2012).

The author will outline misconceptions within the security industry and upper-level management that will ultimately lead to insecure networks, how companies are improperly allocating funds and resources that lead to devastating breaches. Following

this, the author will begin to outline how an attacker begins to take advantage of simple oversights and misconfigurations during the preparatory phase of an attack. In addition, highly exploitable attack vectors that are easily preventable take the stage front and center, as well as remediation recommendations. If upper-level management and the information security manager understand what works, what does not work, and how best to allocate their limited and precious resources in their security budget properly, this will ideally result in a significantly hardened network and fewer overall breaches.

2. Death by Misinformation

Numerous factors bring the security industry to a stalemate situation that is requiring companies to increase their spending on security solutions without necessarily seeing the same increase in success for mitigating attacks. One of the largest concerns is the wide spread of inaccurate information regarding security in general. For example, many vendors of security products attempt to sell products that claim to automate a penetration test that discovers all of your company's vulnerabilities. They make this claim while charging an excessive amount of money, which is unfortunate, considering that there is no real way to automate a penetration test (White, 2012). While this vendor's product may be of value to an organization, selling it as an all-in-one solution to automate penetration tests that will completely secure one's network is simply irresponsible. In fact, illegitimate information like this is indeed causing far more harm than good.

When a company buys into the false claims of a vendor, they use their limited security budget and obtain minimal real-world effectiveness in return. This overpriced hardware that under-delivers costs valuable resources that would have been better spent hiring additional staff, sending their current staff to training opportunities, upgrading out-of-date operating systems, and so on (Kerner, 2015). When a company buys into this new hardware, they sometimes do not allocate or consider the funding necessary to have their current staff trained on this new software or hardware solution, minimizing its true potential. If this was not enough, the company may possess a false sense of security. However, can we really blame these companies? After all, in the light of many high-profile attacks, such as the recent cyber-attacks that targeted well-known organizations like Sony and the massive Office of Personnel Management (OPM), many companies

want to prevent being the next to show up on the evening news. They are eager to throw money at their security problems for the quickest and most effective solutions (Shamah, 2015). We wonder why our highly expensive security solutions are not working well enough when the problem lies not so much within the hardware, but the misinformation regarding what the hardware is capable of doing as well as our implementation and sole reliance on it. Security is most effective when implemented in a layered approach, known as defense-in-depth (Hirschmann, 2014). We tend to forget about layering our defenses due to the latest and greatest gizmo that demands a hefty price tag that claims to make things easier and more secure. We cannot effectively defend and protect what we do not adequately understand.

There are numerous possible reasons that a security budget is misspent or improperly utilized. The first reason is due to the aforementioned example of misinformation regarding what is and is not truly effective in protecting a network. A company can remedy this by sending key members of their security team to reputable training opportunities. Not only will the members of the security team receive valuable formal education on security principles and methods, but this is also a great opportunity for network with other security professionals. When at these training sessions, your security team can meet other information security professionals that may be encountering the same types of issues that your organization is facing. Your team may be able to help another team resolve a challenge that they are facing, and their team may be able to help your team. Perhaps one company used an expensive firewall product that your company considered purchasing, but this product simply did not work for them. Making solid connections with other information security professionals with common goals in the industry is just as important as the training itself. Sending your team to a training session that has practical examples, real-world examples, hands-on labs, and taught by individuals who actively work full time in the security industry will greatly improve the value of the training for your security members.

Another reason that companies improperly utilize their security budgets can be due to upper level management not providing enough funding to begin with. With this, the head of the security team must make very difficult decisions regarding where to allocate his limited resources and then must choose where it is most effective to spend it.

Phillip Bosco, Philimanjaro@gmail.com

The number one recommendation here comes down to having a knowledgeable and qualified individual, which may require sending him to training. Additionally, while there are no blanket recommendations on how to spend a security budget properly as this varies greatly at each unique organization, the security team can do a few things as general guidelines that may help turn a misspent security budget around. Depending on the turnover rate for your security and IT team, the budget may be on the fritz due to it changing hands so much with different individuals who may have had different goals. Obtain a print out of your current budget that details where all of your current resources are spent and then take the time to comb through it and challenge every dollar going out. Which security software solutions, such as antivirus and vulnerability scanners, are you currently subscribed? Have these software solutions been working effectively for your organization? Is the current solution providing feature overkill, or are there cheaper and more minimalistic options available?

With a limited budget, your security team will not be able to cover and secure everything; therefore, the team must spend the budget wisely. Have there been any security incidences with your company recently? If so, tailor the budget toward the areas where the most security incidences are occurring. For example, if company employees tend to lose their laptops on a frequent basis due to their high travel and mobility, allocating resources on full disk encryption for each laptop would be a wise use of limited resources. Are employees frequently leaving their passwords on sticky notes and attaching them to their monitors, or leaving other sensitive documentation on their desks unattended? Spending resources on security awareness training may be beneficial. However, if this same company has a very strict controlled access building, perhaps those same funds would be more beneficial when spent on something that may pose an overall higher risk. A company can identify the risks to their business by tracking all incidences across their organization. Additionally, a full-scope penetration test can positively reveal the true risks and weak areas facing an organization.

It is important that any risks facing your organization are addressed effectively by classifying each of the strongest risks into categories or a threat profile, then addressing the profile as a whole. This is a good use of resources as it allows a company to address many of their core risks with minimal overhead. If a company identified their highest

risks as tailgating, employees regularly clicking on phishing emails, and consistently writing down their passwords, the company can address each problem individual or place them all into categories. With those three examples, the company can classify them all under a failure in the employees' security awareness training. Either the security awareness training does not adequately cover these topics in their training, or the employees do not see the regular enforcement of items from their training and do not take it seriously. Rather than tackling each of the risks individually, identifying core issues is the most effective approach for most risks that a company can place into threat profiles.

If your security budget is far too limited and upper level management is not approving more money, equipment, servers, or additional staff, it will be important to make a case for a funding increase. This will greatly depend on the company and the management, but there are a few strong ways to get management's support behind your security goals and objectives. Have there been breaches within your company recently? Could you have prevented this breach if you had additional resources? If your security budget allows for a penetration test, the results from this test could be eye opening for management if the assessors find many critical findings within your network. Use these situations to your benefit in acquiring more funding, but be wise in your approach. It is important to present your reasoning in a professional manner, backed with statistics, graphs, and hard evidence, rather than attempting to place blame on management for not providing funding. If you start looking at them as part of your team who share a common objective rather than an enemy, there is a better chance that they will understand your mission and will want to lend their support. It can be difficult to get their support if every time they hear from you it is negative in context or asking for additional funding. Without being manipulative, show a genuine interest in doing what is best for the company and networking with others inside of your company. Attempt to visit them for positive reasons and develop a relationship outside of the negative interactions, and they will be more likely to assist you when you require support.

3. Halting Reconnaissance

Reconnaissance is an attacker's best friend before diving in blindly, especially on the more restrictive corporate and government networks. An attacker's chances for a

successful attack increases exponentially when he performs the proper reconnaissance ahead of his attack. There are multiple ways that an attacker can perform reconnaissance, but the security industry splits it into two categories (Czumak, 2014).

The first category is passive reconnaissance, which essentially involves an attacker obtaining as much information about the target organization and network without directly interacting with it. As such, passive reconnaissance is a form of reconnaissance that keeps the attacker's hands clean by using information that is already publicly available (Koba, 2014). For example, an attacker may utilize various search engines to obtain information about the target company's ranking structure, discover employee email addresses, and make use of other information gathering websites, like Shodan, to enumerate the type of servers that a company uses (ColeSec Security, 2014). An attacker can use passive reconnaissance to learn a great deal of information about the target organization before attempting an attack or intrusion of any kind. While passive reconnaissance can be an immensely powerful tool for an attacker, many times the information that an attacker can obtain is limited. In this case, the attacker then performs a more aggressive form of reconnaissance.

The second type of reconnaissance is Active Reconnaissance, which involves an attacker directly interacting with the target organization. During active reconnaissance, an attacker may use Nmap to scan open ports on a remote server and enumerate service versions, operating system information, and perform basic vulnerability scanning (Nice, 2010). Active reconnaissance also carries over into the social engineering realm if an attacker begins placing calls to the organization using phone numbers that he discovered during the passive recon phase and asking extracting information from employees, such as software versions running on the company's workstations. This is not to suggest that one method of reconnaissance is superior to the other, as they both have their rightful place in the attacker's toolkit.

When used appropriately, both methods of reconnaissance are equally as useful to an attacker. Many web servers on the internet are misconfigured or running out of date versions of vulnerable software. Using the power of a search engine like Google, an attacker can input certain keywords and phrases into the search engine, known as Google

Hacking reference, to obtain very sensitive results of a target server that Google has fully indexed (Offensive Security, n.d.). For example, an attacker may input the following into a Google search:

"site:fakevictim.com filetype:xls,txt,doc"

The site parameter specifies that target organization, while the file type parameter identifies the file types that the attacker wishes to view. It is far too common for an attacker to locate a publicly accessible file that contains sensitive information about the victim's organization, including usernames, passwords, social security numbers of employees, and so on. This sensitive file disclosure can be due to a misconfigured robots.txt file, which tells search engines specifically which items of their website that they do not want indexed. However, this could also be due to a more serious overarching security misconfiguration on the web server itself that does not assign permissions properly to sensitive directories and files.

In order to prevent this simple passive yet highly effective type of passive reconnaissance attack, ensure that all of your web server's permissions are set appropriately. Give special attention to which directories are accessible externally from web users and keep your robots.txt file updated to ensure search engines do not inadvertently expose other sensitive directories. Lastly, perform Google Hacking yourself against your own organization in order to see exactly what an attacker can see. Ultimately, you will not know how effective your methods are of protecting your sensitive data unless you, your security team, or a professional penetration tester assesses it regularly. On a regular basis, penetration testers shock their clients with the wealth of sensitive information that the assessors dig up via these simple Google Hacking methods.

Other useful items that an attacker may find through the reconnaissance phase include the IP address block that the company owns, which IPs are externally accessible, and what subdomains of a given domain are available. If an attacker has targeted www.fakevictim.com, an attacker may also perform an enumeration of subdomains. An attacker performs this in a variety of ways, with the first method involving additional Google Hacking methods using specialized search queries. It is important for an organization to be aware of what search engines are actively indexing of their site and

their subdomains. The following passive reconnaissance search query will identify any currently indexed subdomains belonging to an organization:

site:.fakevictim.com –www*

Another technique that an attacker can use to identify subdomains involves brute forcing the subdomains using a tool like DNSenum, which matches a wordlist of common subdomains against an organization of an attacker's choice (Pentestlab, 2012). This technique allows an attacker to locate subdomains that search engines do not index. This attack vector is effective, as domains typically possess subdomains such as mail, VPN, and portal. Using this technique, an attacker may uncover previously unknown and unindexed subdomains that can present additional attack surfaces. To prevent against this type of enumeration, a company may opt to use a subdomain-naming scheme that is out of the ordinary and use names that an attacker will not find within a standard wordlist.

From a safety and legal standpoint, passive reconnaissance is far less risky than active reconnaissance. If it is unclear which version of reconnaissance one is performing, consider whether it is possible for the individual to be arrested performing the reconnaissance by the target company or prosecuted by law enforcement. If there is risk of detection or arrest, it is more than likely active reconnaissance. Once the attacker performs both passive and active reconnaissance, he now possesses the necessary information to perform more invasive attacks to break the defensive perimeter.

With most companies, having a known online presence is crucial to the success of their business. Companies must take caution in the type of information that they allow the public to see. A general rule of thumb for determining before releasing or revealing any company related information or documents is to determine first if it absolutely needs to be publicly accessible for the success of the business. If it is not necessary to the success of the business, then do not make that information publicly accessible.

4. Armed and Ready, Captain

The range and sensitivity of information that an attacker uncovers during the reconnaissance phase of the attack will greatly vary from organization to organization. Depending on the information gathered during the reconnaissance phase, an attacker's next steps may differ slightly but the concepts and methodology remain the same. If an

attacker was able to obtain a document that contained server addresses, usernames, and passwords for an organization, the attacker may log into web portals or other services that are available at that time. When an attacker has authenticated access inside of credentialed portal or service, the risk greatly increases, as does the attacker's ability to enumerate additional sensitive information about the organization.

Many web portals contain both standard user interfaces and administrative interfaces, with each level of privilege offering varying functionality. Web applications are powerful for businesses, management, and end-users, but can also be quite dangerous if the application does not segregate itself from the backend server that it currently runs on (Johansson, 2005). As a standard user, certain functionalities and features are limited to protect the integrity and security of the backend server. As an administrative user, the web application grants the user with additional privileges, which in many cases an attacker may be able to exploit to get closer within your network. In one recent web application, a standard user account only allows simple functionality such as viewing server information, network load, and other operational information. With an administrator account, the web application adds additional features like the ability to run tools like traceroute and ping. This may not immediately seem dangerous, but a resourceful attacker realizes that the web application sends these commands directly to cmd.exe within the server itself. The web application only allows a user to employ the ping or traceroute commands and to supply the destination URL or IP address in a field. In this case, the attacker managed to break out of the web application's limited commands and issue whatever he wanted to the underlying cmd.exe by inputting the following text where the destination IP address is supposed to be supplied for the included ping utility:

> *127.0.0.1 & whoami & net user hacker H@ck3r! /add & net localgroup administrators hacker /add & net localgroup "Remote Desktop Users" hacker /add*

By inputting the ampersand after the destination IP address, it effectively broke out of the web application and allowed the attacker to input any additional command of his choosing. With cmd.exe, the ampersand indicates that when the first command is finished running, the command after the ampersand will also run. In this case, the attacker chose

Phillip Bosco, Philimanjaro@gmail.com

to ping the server's loopback address, then used an ampersand to run the whoami command, which revealed that all commands ran with system level privileges. After that, the next command created the user "hacker", while the following commands added the newly created user to both the Administrator and Remote Desktop Users local groups. In a single one-line command, the attacker went from a highly limited web application, to creating a full administrative level user with remote desktop access to the system. To break this attack down piece by piece, the attacker located this web portal using passive reconnaissance methods to find various subdomains belonging to the target organization. Then, the attacker used the default credential set associated with this particular web application and successfully authenticated as an administrator. Lastly, the attacker took advantage of a legitimate administrative feature to take full control of the backend server with system level privileges, all without breaking a sweat.

Without proper reconnaissance, this aforementioned attack vector would not have been successful nor would the attacker have been able to locate this vulnerable web application. If the attacker did not utilize proper passive reconnaissance techniques, he would have been reliant on the Nmap scans that directly hit the victim's servers. Port scans are very noisy and can quickly result in a ban of the attacker's scanning IP address. Alternatively, an attacker would have had to rely on the latest unpatched zero-day sitting on the victim's network, which is not always practical or reliable. Other than ensuring that the company only exposes the necessary information publicly, the other attack vectors here included utilizing a well-documented default password for a web application and the web application not properly sanitizing user-supplied input. Many modern day applications and administrative controls require the administrator to set a new password during the initial set up; however, companies are still using older applications and administrative consoles in production today. If your company is utilizing an older application, verify that default accounts and passwords are not in use. In addition, if using a custom password, ensure the password meets modern complexity and length requirements. As this server suffered from input validation issues, have your web application testing thoroughly for vulnerabilities that could lead to Cross Site Scripting (XSS) vulnerabilities and Structure Query Language injection (SQLi). In this example, the web application was not properly sanitizing user-supplied input, which led to full

command execution on the backend server. Finally, follow the principle of least privileged in regards to your web application implementation (Rouse, 2008). Run all services and web applications with the absolute minimum level of privileges necessary for the desired functionality and operation. As much as possible, avoid running anything with root and system level privileges, which in many cases, is unnecessary to the operation of the application or service in question.

If an attacker was unable to gather useful information about the target's network, such as valid credentials or a vulnerable web application, this would greatly limit the attack surface available. Limiting the attack surface that an attacker can utilize holds incredible value, as it requires them to take a more aggressive approach to obtain that initial foothold in your network. Assuming the proper technical measures are in place that actively block active port scans against the servers and all of the other services are filtered by a properly configured firewall, an attacker must than rely on social engineering methods.

5. "...But, I Have a Clipboard"

Regardless of how much a company spends on the latest and greatest antivirus software, firewalls, or up-to-date applications, social engineering attack techniques continue to be effective. Social engineering attacks are on the rise due to more technical implementations put into place to protect an organization (Social-Engineer, 2015). With social engineering, attackers have the ability to completely bypass and sidestep most, if not all, of the security controls that a company puts into place. Unfortunately, far too many companies place the vast majority of their focus on technical controls rather than on physical and social engineering controls, which open the door for these attacks to carry a high success rate. Social engineering attacks are broken into numerous categories, such as email phishing, phone phishing, or physical in-person exploitations. An attacker performs each of these attacks in a variety of ways. Social engineering involves manipulating or tricking an individual to give up sensitive information that they would not have otherwise given up, or convincing them to give you access to an area that one would not normally have access to. For example, you may train your employees that they must never give up their password over the phone; however, a successful social engineer

may call up an individual, claim that they are with the IT department and mention that the user has to change their password. If the attacker sounds legitimate enough, the employee happily voices their password to the attacker over the phone. If one were to ask any employee anywhere if they would ever give up their password over the phone, their response may be along the lines of, "Of course not!" If this is the case, than how is a malicious social engineer so successful? A few simple case studies may do the trick in determining why social engineers are so successful at doing what they are doing.

Phishing attacks that occur over email are some of the most widely used methods an attacker will use when networks are efficiently hardened (Britt, 2015). In many cases, a sophisticated phishing attack may be an attacker's only way into gaining that initial foothold into a network. Many security awareness programs tend to focus on training employees to spot a phishing email by looking for misspellings, grammar errors, or to report emails that explicitly ask for their username and password. While there are some phishing emails that are easy to detect immediately as fraudulent for most people, attackers are finding ways to not only trick employees easily, but also bypass a company's spam filters for effectively. Many companies set their spam filters to block email from public open-relay Simple Mail Transfer Protocol (SMTP) servers, which attackers commonly use to distribute illegitimate email. Additionally, more advanced configurations for a company's spam filters involve immediately blocking emails that utilize hyperlinked text within an email.

Phillip Bosco, Philimanjaro@gmail.com

Many attackers will use the hyperlinking method, as the victim sees one link, but the underlying web address will direct them instead somewhere malicious, as seen in the figure below.

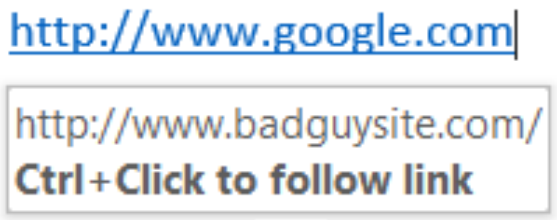

Figure 1: Attackers utilize hyperlinking to mislead their victims

When a company decides to block emails that utilize hyperlinking, the attacker is more limited in the tricks that he can play on a victim. In this case, only direct links can be included in emails to this organization. Attackers then get creative and register a domain name that is visually similar to your actual domain name. For example, if a company's website is 'http://xyzcompanyllp.com', an attacker may register 'http://xyzcompanylllp.com'. The difference between the URLs is nearly indistinguishable, as seen the figure below.

Real Link

http://xyzcompanyllp.com

Fake Link

http://xyzcompanylllp.com

Figure 2: Visually similar links

With a domain that looks visually similar to the real company's domain, an attacker then creates an email account using the new domain and send a convincing looking email to the victim.

Phillip Bosco, Philimanjaro@gmail.com

An example of a convincing looking email may convince a user to take urgent action in a way that will benefit them, as demonstrated in the figure below.

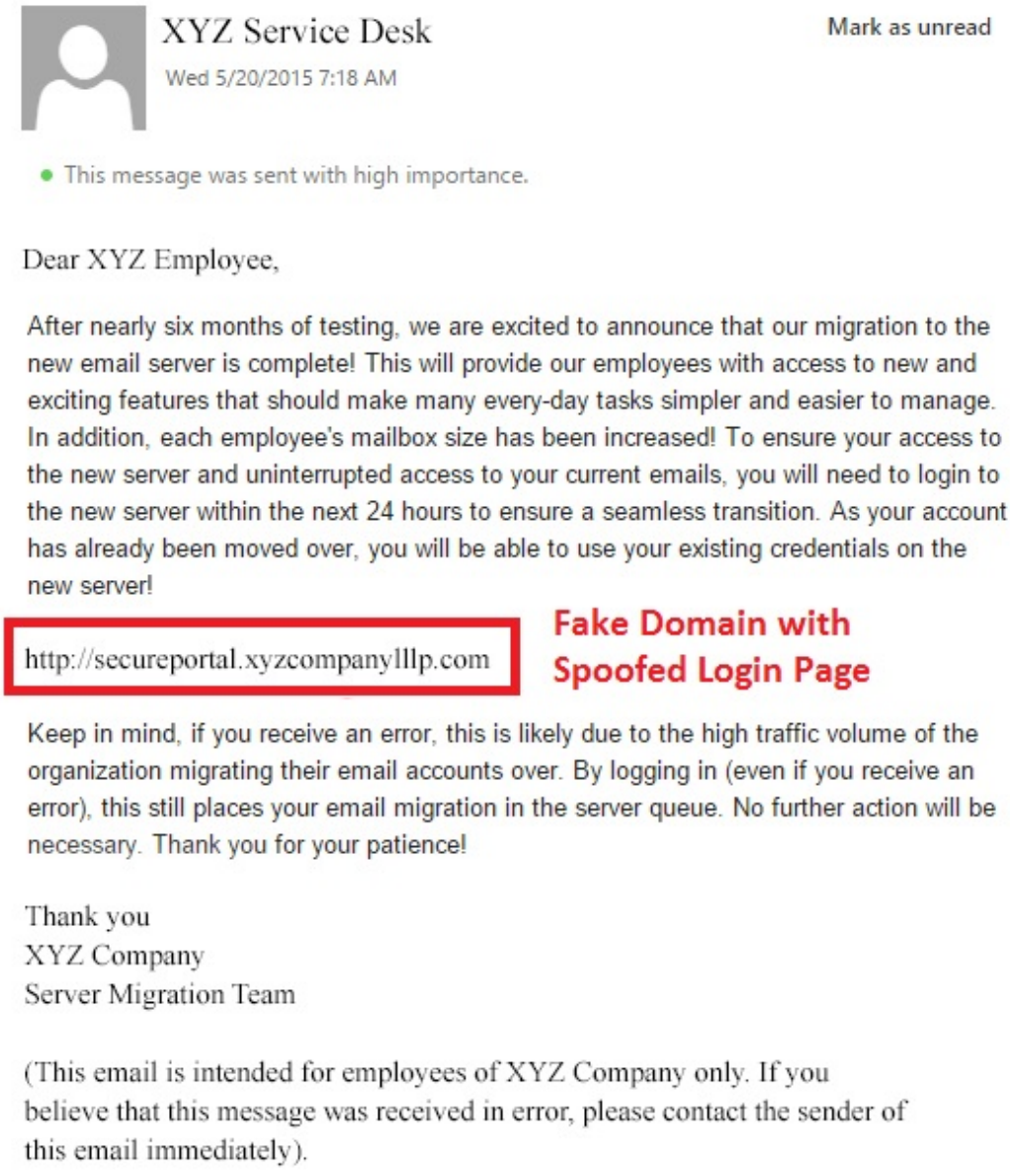

Figure 3: Legitimate looking spoofed email with malicious link

While blocking emails from public open-relay SMTP servers and preventing the receipt of hyperlinked emails is a start, it is not a complete solution. Preventing phishing emails like the one mentioned above from slipping through the cracks and making its way through a company's spam filter is a much more difficult challenge to solve. Blocking all

emails externally that utilize links or attachments may prevent the effectiveness of the majority of phishing emails, but this approach is not realistic for most organizations, as it would hinder legitimate business functions. During an employee's security awareness training, a company should stress that an employee never click on links within emails without first contacting the source of the email first. This particular email appears to come from the company's internal server migration team. Has the employee heard anything about this server migration in the past, or did this email come unexpectedly? Does this company even have a server migration team?

It is important to train employees the proper way to contact the source of an email before clicking on links or opening attachments, as calling the provided number within the email address or replying to email will only lead the victim directly to the attacker. In this particular instance, the employee may utilize their corporate directory to locate their helpdesk or server migration team's phone number and call them directly. While inconvenient, this type of awareness can go a long way to limiting the success of phishing emails and minimize the effectiveness through users reporting the suspicious emails immediately. Lastly, always verify links before clicking on them. While the link in the previous email is visually similar to a legitimate address, an employee that takes the time to peruse the email and double check the link before clicking may very well pick up the inconsistency. Even with more hands-on training, not every employee will be as aware as we would all like; however, if just 30% of employees are more aware due to proper training, that may be enough to keep many of the phishing attack breaches at bay.

During a penetration testing engagement, a gas and electric company tasked the assessors to attempt to break into a building off-hours, to see what information they could find in the form of sensitive documentation, and if possible, take entire laptops and other company equipment. The assessors initially gained access by standing by the Radio Frequency Identification (RFID) reader beside the controlled access door. In the morning when all of the employees are badging in for work, the assessor managed to get close enough to an employee to digitally capture and clone their RFID badge. The assessors returned in the middle of the night, used the previously captured RFID badge on a door, and gained access to the building. During their time in the building, they were able to obtain highly sensitive information from usernames and passwords, bank account

Phillip Bosco, Philimanjaro@gmail.com

numbers for both the employees and clients of the utility company, and two-factor authentication token devices. As they were walking through the building's hallways with each of their arms filled with miscellaneous documentation and equipment, the roaming security guard turned the corner and saw the three assessors. They remained calm and greeted the security guard in a normal manner; then the security guard casually responding with the following.

"Burnin' the midnight oil, eh?"

"Oh yes, work…phew, it never ends!"

"Ha, I hear ya. You guys have a great night, drive safely!"

On paper, this company implemented various layers of security to protect their building and sensitive information. After all, they implemented RFID controlled access badges, cameras in most hallways and entrances, and guards roaming both the interior and exterior areas of the building. How were these assessors successful and able to circumvent a guard who confronted them in the middle of the night?

On the technical side of controls, the company could have implemented better access control, only allowing employee badges to work during the standard working hours of a business day. Any off-hour access would need approval on a case-by-case basis, or if a certain employee's job responsibilities require it. Otherwise, a company should only allow one off-hour entrance into the building through the front door that leads directly to the security guard's booth, where he can check in off-hour employees as necessary. If the company properly managed their access control hours, the assessors would have been strictly limited to tailgating through a door via a smoker's deck or some other exit. However, this would be very difficult as the amount of people in the building off-hours is very limited and there were security cameras at every single doorway.

Victims do not always detect successful social engineers due to their ability to blend in and act as if they belong there in the first place. In this case, the assessors were wearing business casual attire and did not appear threatening. In addition, the demeanor and mannerisms of the assessors were not violent or out of the ordinary. If the assessors had worn all black clothing, a hoodie that covered most of their faces, and ran at the first

sight of a security guard, this would trigger a psychological response within the security guard to detain the assessors. In other cases, like prompting an employee for their password over email, the social engineer acts as if they indeed require that information in the first place. If the social engineer asks, "Can I please have your password?" this suggests that the employee would be doing the social engineer a favor or as if the social engineer is not entitled to possess it. However, if the social engineer maintains the confidence that he indeed is authorized to have it, he might instead say, "At this point, I'll need your password to continue forward with the password reset." The second phrase sounds more confident and is highly successful on phishing engagements that allow for calling victims via phone. Regardless of the various case studies, the principles are universal and remain the same across the board. A social engineer is confident and acts as if he belongs there (Goodchild, 2009). If the social engineer believes himself, the victim will also believe him. In this case, how do we prevent this?

A company makes security awareness training for all employees to report suspicious activity, not click malicious links within emails, and never give their passwords over the phone. Unfortunately, this training is not commonly successful for a variety of reasons. The first reason is due to security awareness training being compliance focused. A company may be legally required to give their employees annual security awareness training to stay within audit compliance for their particular industry. In this case, many security awareness programs utilize a training methodology commonly known as "Death by PowerPoint", where employees sit behind their computer and click through the seemingly endless slides as quickly as possible in order to return to their daily work (Lohrmann, 2014). When security awareness training is long and non-interactive, employees are not as likely to learn much from the training. Compare and contrast this to a security awareness program that is interactive, entertaining, and provides rewards for employees. While the concept of an interactive and rewarding security awareness program is exciting, the implementation of such a program can be very difficult due to the culture and size of an organization. Therefore, a company may need to customize it to fit their unique needs. It is easy enough to fill the technical compliance and obtain the simple "check-in-the-box" that auditors require; however,

attackers are increasingly successful at social engineering methods due to the lack of importance placed on proper, fun, interactive, and educational awareness programs.

6. Conclusion

With so many high profile breaches occurring on a very regular basis, it seems as if the attackers are currently winning the cyber battle. The security industry might have lost the upper hand, but not all hope is lost. This paper intentionally focused on the less technical methods that attackers use that result in high impact losses, while placing emphasis on how preventable many of these common attack vectors are. While attackers become more sophisticated, a company can deter many of their attacks through the proper implementation of firewalls, password protected services and web applications, and educational security awareness training. As companies start to learn from prior incidents and breaches, they can allocate their precious resources more strategically. They need not simply throw away money into the latest and greatest gadget, as doing so does not necessarily equate to a more secure network. In our current world, a larger budget dedicated towards security is welcome, but is frequently misused.

We can improve our overall security posture through knowledge and proper application of fundamental security principles, while continuing to place emphasis on defense in layers. Learning to understand the techniques and strategies that an attacker will use against your company is critical to properly defending against it. No longer is it enough to just keep up to date with the newest patches, as implementing security effectively requires us to look at it through a much broader perspective. By learning an attacker's techniques, we can better secure our networks against them and quickly remove the lowest hanging fruit dangling from our vulnerable organizations. To reiterate a previous point, we cannot properly defend against from what we do not adequately understand. If any company is serious about truly protecting their most valuable assets, it is necessary to take a step back and reassess our current posture. The security industry as a whole has implemented solutions improperly, which only exponentially increase the risk of an attack. Companies all across the globe now carry the unfortunate mindset that it is not a matter of if attackers will breach their networks, but that it is an inevitable matter of when. This should not be the case, nor should be acceptable. There is much more that

we can do to win this cyber battle and to regain the upper hand once again by going back to the basics, educating ourselves and our staff, and allocating our budgets to the aspects of security that are most effective for our organization.

Phillip Bosco, Philimanjaro@gmail.com

References

Britt, P. (2015, March 31). Phishing attacks: Not sophisticated, but successful. Retrieved from http://www.esecurityplanet.com/network-security/phishing-attacks-not-sophisticated-but-successful.html

ColeSec Security. (2014, January 24). Passive reconnaissance with Shodan. Retrieved from http://colesec.inventedtheinternet.com/passive-reconnaissance-with-shodan/

Czumak, M. (2014, February 5). Passive reconnaissance. Retrieved from http://www.securitysift.com/passive-reconnaissance/

Goodchild, J. (2009, July 22). Mind games: How social engineers win your confidence. Retrieved from http://www.networkworld.com/article/2260436/collaboration-social/mind-games--how-social-engineers-win-your-confidence.html

Hirschmann, J. (2014, September 1). Defense in depth: A layered approach to network security. Retrieved from http://www.securitymagazine.com/articles/85788-defense-in-depth-a-layered-approach-to-network-security

Hong, J. (2013, March 22). How do hackers actually break into systems and steal stuff? Retrieved from http://blog.wombatsecurity.com/how-do-hackers-actually-break-into-systems-and-steal-stuff/

Johansson, J. (2005, January). Anatomy of a hack: How a criminal might infiltrate your network. Retrieved from https://technet.microsoft.com/en-us/magazine/2005.01.anatomyofahack.aspx

Kerner, S. M. (2015, March 12). 'False sense of security' and understaffing create risk of attack. Retrieved from http://www.eweek.com/security/false-sense-of-security-and-understaffing-create-security-risk-of-attacks.html

Phillip Bosco, Philimanjaro@gmail.com

Kirk, J. (2013, November 21). Worm targeting Apache Tomcat servers, possibly for DDoS. Retrieved from http://www.infoworld.com/article/2608964/malware/worm-targeting-apache-tomcat-servers--possibly-for-ddos.html

Koba. (2014, October 31). Penetration testing - Reconnaissance. Retrieved from www.rekha.com/penetration-testing-part-2-reconnaissance.html

Lee, T. (2012, September 4). Manually Exploiting Tomcat Manager. Retrieved from http://blog.opensecurityresearch.com/2012/09/manually-exploiting-tomcat-manager.html

Lohrmann, D. (2014, March 9). Ten recommendations for security awareness programs. Retrieved from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Ten-Recommendations-for-Security-Awareness-Programs.html

Mott, N. (2015, April 8). Russians hacked the White House thanks to a simple phishing attack. Retrieved from https://pando.com/2015/04/08/russians-hacked-the-white-house-thanks-to-a-simple-phishing-attack/

Nice, S. (2010, May 5). The hacker's guide to website security: Active reconnaissance. Retrieved from http://www.techradar.com/news/internet/the-hacker-s-guide-to-website-security-687153/2

Offensive Security. (n.d.). Google Hacking Database. Retrieved from https://www.offensive-security.com/community-projects/google-hacking-database/security.com/community-projects/google-hacking-database/

Phillip Bosco, Philimanjaro@gmail.com

Pentestlab. (2012, July 13). DNSenum – Gathering DNS information. Retrieved from https://pentestlab.wordpress.com/2012/07/13/dnsenum-gathering-dns-information/

Rouse, M. (2008, September). What is principle of least privilege (POLP)? Retrieved from http://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

Shamah, D. (2015, April 27). No need to 'throw money' at cyber-solutions, says ex-Shin Bet boss. Retrieved from http://www.timesofisrael.com/no-need-to-throw-money-at-cyber-solutions-says-ex-shin-bet-boss/

Social-Engineer. (2015, February 2). The rise of multifaceted social engineering attacks. Retrieved from https://www.social-engineer.com/rise-multifaceted-social-engineering-attacks/

Thompson, C. (2014, November 21). A bad year for cybersecurity, but a great one for business. Retrieved from http://www.cnbc.com/id/102208309

White, J. (2012, October 22). Don't be fooled! There's no such thing as an automated penetration test. Retrieved from https://www.pcicomplianceguide.org/dont-be-fooled-theres-no-such-thing-as-an-automated-penetration-test/

Last Updated: May 25th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced