SANS Institute
Information Security Reading Room

Minimizing Damage From J.P. Morgan's Data Breach

Allen Jeng

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.

Minimizing Damage From J.P. Morgan's Data Breach

GIAC (GSEC) Gold Certification

Author: Allen Jeng, ajeng@adobe.com
Advisor: Tim Proffitt

Accepted: March 15th, 2015

Abstract

Data breaches should not happen to large banks like J.P. Morgan who spend $250 million on security every year. This paper will explore in depth what J.P. Morgan could have done better to prevent and minimize the theft of 83 million customer records by applying techniques from defense-in-depth. In addition to addressing the human factor that enabled hackers to enter J.P. Morgan's network, implementing security measures to stop malware from using employees' computer as entry point, fine-tuning access control, performing better detection of hackers inside the corporate network, and regular pen-testing for catching vulnerabilities are some of the necessary steps needed to strengthen J.P. Morgan's network.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

How did a mega bank like J.P. Morgan get hacked? It all started in June 2014 when one of their employee's personal computer was infected with malware which resulted in stolen login credential (Sjouwerman, 2014). When this employee remotely connected to the corporate network through a virtual private network (VPN), the hacker was able to gain access to the internal network. From that point on, the hacker managed to break through layers of security by unleashing malicious programs designed to penetrate J.P. Morgan's network (Son, 2014). Hackers then successfully obtained the highest level of administrator privileges and were able to take control of more than 90 servers through the use of multiple zero-day vulnerabilities (Robertson, 2014). To avoid detection, data was stolen slowly over a period of several months (Robertson, 2014). The stolen login credential would have been useless if it weren't for the overlooked server that failed to receive the two-factor authentication update (Goldstein, 2014a).

The breach would not have been discovered and stopped in mid-August if the hackers didn't breach one of their charity websites. Hold Security, Inc. was the one that discovered a billion stolen passwords and usernames, some of which belonged to the J.P. Morgan Chase Corporate Challenge site. This is when J.P. Morgan's security team looked into their own corporate network and found out that they too were breached (Yadron, 2014a). The New York Times article mentioned that Hold Security's founder was surprised that information their company gathered was crucial in helping J.P. Morgan discover their own breach. If Hold Security had not discovered the stolen information, hackers would have had longer access to J.P. Morgan's network potentially causing more damage.

The hackers stole contact information including names, addresses, phone numbers and email addresses for 76 million households and 7 million small businesses (Yadron, 2014a). Part of the stolen data includes internal data identifying customers by categories like mortgage, credit card, and private banking (Son, 2014). J.P. Morgan could face future hacking from the stolen lists of applications and programs that runs on J.P. Morgan's computers because it could be analyzed for vulnerabilities (Silver-Greenberg,

© 2015 The SANS Institute Author retains full rights.

2014). Since hackers were successful in covering up some of their tracks by deleting a good number of log files, sources claim that it is possible that the hackers broke in as early as April 2014 (Yadron, 2014a). This is precisely when J.P. Morgan's Corporate Challenge site was compromised.

Gartner predicted in August 2014 that worldwide spending on cyber security will top $71 billion in 2014 (Kobialka, 2014). J.P. Morgan already spends $250 million on security annually with 1,000 employees dedicated to cybersecurity compared to Google's 400 employees (Robertson, 2014). Unfortunately, many of the J.P. Morgan security staff are leaving for other banks with more to follow (Silver-Greenberg, 2014). This means that people with knowledge and experience regarding their network infrastructure are departing, making J.P. Morgan vulnerable to further data breaches.

The chairman of Information Security and Privacy Advisory Board for NIST, Dan Chenok, said, "The only way to 100% protect yourself from attacks is to turn off your computers" (SANS Institute, 2014a). If one has something valuable that hackers want, they will try and steal it. It's how quickly the damage gets contained that matters. This paper will explore in depth what J.P. Morgan could have done to minimize the damage from their breach by applying defense techniques such as uniform protection, protected enclaves, and information centric (SANS Institute, 2014b). Uniform protection means all systems get equal treatment and protection. All systems will get the same configuration, the same end-point security, connection to centralized patch management, and connection to VPN. This basic protection needs to be followed up by segregating the networks, thus limiting access to the entire network, known as protecting the enclave. Engineers do not need access to the sales database just as HR staff have no need to access source code servers. Since security is all about protecting critical assets, information centric means the organization needs to provide layered protection around those assets after identifying what they are. This paper will look at the necessary security measures to prevent and contain malware from using host computers as gateways into the corporate network, fine-tune access control, protect critical assets, perform better detection when adversaries attack the corporate network, and perform regular pen-testing so that vulnerabilities are found by J.P. Morgan instead of by adversaries.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

2. Minimizing the attack surface on client computers

2.1. Deploy Host-based Intrusion Prevention System

The entry point for hackers into J.P. Morgan's network was through VPN from an employee with a malware-infected system and compromised login credentials (Goldstein, 2014a). There are no details as to how this employee got infected or how their credential was stolen but one can guess that this individual probably clicked through a phishing email attachment or visited a site with malware (Fraud.org). A Host-based Intrusion Prevent System (HIPS) has a fighting chance of catching and stopping the malware, because its job is to identify and stop known and unknown attacks (SANS Institute, 2014c).

HIPS is software that uses system calls to do application behavior monitoring. It looks at the correlation of activity and blocks the process when it reaches a high level of confidence (SANS Institute, 2014c). By combining functions of personal firewall, antivirus, IDS, and behavioral analysis, HIPS is able to stop malware from doing harm. The job of HIPS is to block and quarantine activities that it deems suspicious (Chee, 2008). Even though the attack has been stopped by HIPS, some damage has already been done such as modification to the user's system. The biggest advantage of HIPS over Network-based Intrusion Prevention System (NIPS) is that HIPS sits on the computer it is supposed to monitor. That means it has better accuracy than a network-based system, thus drastically lowering false-positives. The other big advantage to HIPS is that it monitors and blocks at the individual computer level instead of the network level. HIPS works well in conjunction with other security protection like antivirus software. In addition to these protections, a bonus advantage to HIPS is the ability to see unencrypted traffic.

HIPS have its drawbacks since it normally eats up 10 to 20 percent of available CPU and memory resources. It also requires a management console to monitor HIPS clients, update HIPS software, and update client rules. Hence, recommendation for J.P. Morgan is to only deploy HIPS on systems that need to leave the corporate premises because internet access for systems that are plugged in permanently on corporate network are protected by corporate firewalls and NIDS.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

The point of origin was a compromised computer that an employee used to VPN into J.P. Morgan's network (Yadron, 2014a). There's a high probability of the malware being stopped before it had a chance to do harm on the corporate network if HIPS was deployed on this employee's computer. In addition to preventing the malware from doing more harm, it would alert security staff regarding the suspicious activities that HIPS just quarantined (Chee, 2008). HIPS can also alert end user when it quarantined suspicious activities, prompting them to notify security staff for further investigation (Kaspersky Lab, 2012).

2.2. Basic Protection are still required

HIPS should not be the only protection installed on employee computers. Antivirus and regular patching are still required to maintain basic protection against attacks. Regular patching allow systems to receive proper fixes to the operating system where if left unfixed would have allowed hackers to exploit the bug. Antivirus will also perform its basic function in protecting the host from known viruses. Despite Symantec's declaration that antivirus software is dead (Yadron, 2014c), many security professionals agree that antivirus is still effective at protecting hosts from known viruses.

2.3. Employee education: dealing with the human factor

Human is always the weakest link in security because not everyone is security conscious. There are people that would blindly click on links or click through phishing emails because they didn't know better. According to Verizon 2014 Data Breach Investigation Report, 78 percent of all cyber espionage malware get inside through email attachments (Barrett, 2014). Thus, one of the most successful entry points for hackers is through social engineering. Social engineering is the technique of tricking or manipulating someone into providing information through the exploitation of human vulnerabilities (SANS Institute, 2014c). Phishing, spam, mail attachments, or the impersonation of someone that they're not are some of the popular forms of social engineering. Develop appropriate security policies, training employees about vulnerabilities and social engineering detection goes a long way in mitigating this attack vector. Security awareness training for employees won't stop phishing attacks from ever happening but it will raise awareness and reduce the percentage of people from

© 2015 The SANS Institute Author retains full rights.

accidentally get infected with malware because they do so out of ignorance (Sjouwerman, 2011). Employee training needs to be a part of J.P. Morgan's security policy. It must be specific, measureable, achievable, realistic and time-based (SANS Institute, 2014b).

2.4. Application Whitelisting

Part of the victory for hackers during J.P. Morgan's breach attributes to malware infection on one of their employee's computer (Sjouwerman, 2014). Application whitelisting would deny the malware from installing itself.

Whitelisting is a software that allows applications to function if they're on the approval list. The "deny all" unless approved methodology is commonly found in fine-tuned firewall rules (Shackleford, 2009). One of the common means of whitelisting policy is through application's code signing (Shackleford, 2009). Big OS vendor such as Microsoft encourage software publisher to sign their application so that integrity and reputation of the application is preserved (Law, 2011). Integrity portion proves that this application has not been tampered with and reputation portion says this came from a trusted reputable company. Reputation is important because any hacker can sign their malware and satisfy the integrity portion. Apple approves developers through their Gatekeeper program by requiring each developer to sign their application with a developer ID, which is controlled by Apple (Apple, 2014). Malware can be signed with reputable stolen digital certificate as the case with Sony (Mathews, 2014). Those are rare instances where whitelisting will allow malware through to do damage.

Whitelisting do require fine tuning and updating. It is important for IT staff to maintain and update policies as needed so that whitelisting doesn't block legitimate updates or software (Shackleford, 2009). Benefits of having whitelisting for J.P. Morgan could have stopped the hacker from infecting the employee's system because it would have prevented the malware from being installed.

HIPS, antivirus, regular patching, application whitelisting and employee awareness training together are effective measures in preventing malware from being an entry point during J.P. Morgan's breach.

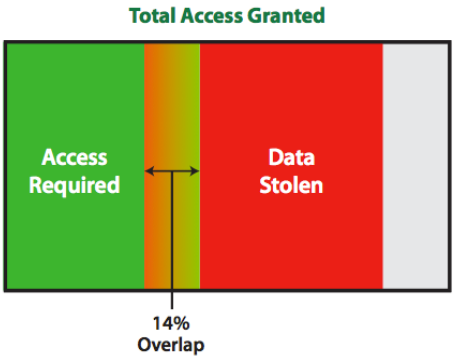
© 2015 The SANS Institute Author retains full rights.

3. Protected Enclaves

3.1. Segregate and Protect critical assets

Segregating the internal network into segments so that it is not one massive zone where everything is visible is the strategy behind protected enclaves in defense in depth. The goal is to restrict access to critical segments so that critical assets are not accessible to everyone on the internal network. One of the best ways to apply this separation is the use of virtual local area network (VLAN) because it allows organizations to group their critical servers and assets into multiple VLAN zones (Northcutt, 2007). Once subdivided into zones, firewall needs to be deployed to further control access. In addition to having firewalls at network perimeters, they are a necessity in protecting and shielding critical assets. Not only do they provide access control at the TCP level, they're an extra level of protection against intelligence gathering because its main function is to filter communication based on the content coming in or going out (SANS Institute, 2014c).

There are no details pertaining to what kind of access this compromised employee had. This paper must speculate that the employee had more access granted than required to do his or her job. Least privilege simply means to give someone the least amount of access to perform his or her job. Statistics from Dr. Eric Cole's research shows that employee whose system was compromised only needs access to 14 percent of the data stolen from hackers. If least privilege control access were applied, these organizations would have reduced the amount of stolen data by 86 percent (Cole, 2014c).



Overlap of access required versus stolen (Cole, 2014c)

One way to implement least privileged access control is with Role-based Access Control (RBAC) because it is based on group membership. The biggest advantage to

© 2015 The SANS Institute Author retains full rights.

Role-based Access Control is that it allows only one role at a time. All access to user's previous role gets removed when he or she gets put into the new role. This ensure that unnecessary access get automatically revoked when the user switches roles. According to Ferraiolo and Kuhn of National Institute of Standards and Technology (NIST), the advantage of RBAC is that once setup by the organization, it is flexible enough to handle existing infrastructure provided that a policy is in place (National Institute of Standards and Technology, 1992). Hazen Weber warns that if the organization does not have skilled and knowledgeable staff, the effort and effectiveness of RBAC implementation will quickly loose its purpose. The lack of well-documented policy or a policy that no one follows will defeat the advantage of implementing RBAC in the first place because doing RBAC without proper planning will cause lots of redesign or work around solutions (Weber, 2003).

The other possible path for hackers would be privilege escalation vulnerability. Privilege escalation is when attacker gain privileged access through the use of a lower privileged user. Vertical privilege escalation is the upgrade from a less privileged user to a higher access or permission level (Palermo, 2013). Exploitation of buffer overflow to gain root access is an example of this type of privilege escalation (McAdams, 2005). Regular patching, keeping antivirus up to date, and the use of Mandatory Access Control (MAC) with RBAC are some of the mitigations against this types of attack (Palermo, 2013). Horizontal privilege escalation is when a normal user gain access or privilege that belongs to another user such as the use of stolen password to gain access to J.P. Morgan's network (Palermo, 2013). The use of HIPS and user education mentioned above are ways to reduce and defuse horizontal privilege escalation (Palermo, 2013). The application of least privileged is a way to fine tune access, thus limiting the amount of data stolen.

3.2. Make Use Network Access Control

The purpose of Network Access Control (NAC) is to prevent a system from accessing trusted network before it is scanned and checked (Snyder, 2010). NAC can be configured pre-connect or post-connect. Post-connect NAC allows initial access but will place device in quarantine if it fails to pass security policy during scanning. Pre-connect

© 2015 The SANS Institute Author retains full rights.

NAC place device in quarantine while being checked for compliance and authorization. It will only allow the device onto the network if it passes security policies. It is able to do this by placing them dynamically in VLANs with different levels of access (Piper, 2014). Due to the nature of J.P. Morgan's business and the assets they must protect, pre-connect NAC is the recommended way. One of the benefits to next-generation NAC is the ability to enforce role-based access control. Most next-generation NAC offers authentication through Active Directory or LDAP (Piper, 2014). Once the user is authenticated, the system can be scanned to ensure that the device connected has the proper security protection such as patches, anti-virus definition, and authorized application installed. All of that is controlled by NAC's basic policy engine (Piper, 2014).

By utilizing NAC and VLAN, organization is able to quickly contain damages through this automated quarantine system. Continuous monitoring is the key since a healthy system that connects to the network in the morning doesn't mean it will stay clean in the afternoon. NAC is one of the pieces in conjunction with least privileged implementation to properly secure J.P. Morgan's network.

3.3. Use Proxy with All Outbound Traffic

Hackers advert detection from organization's security defense by using encrypted in-bound and out-bound traffic because security defenses cannot catch what it cannot see. The hacker that got into J.P. Morgan's network through VPN, had the potential to setup a command-and-control (C2) encrypted outbound channel that can bypass all security defenses. Not only would this allow them to slip under the radar, they no longer need to rely on this compromised employee to make another VPN connection. The way to guard against this is by having all outbound traffic go through proxy. The proxy will have the ability to decrypt or verify that the crypto is authorized because the organization knows what program, which site and the registered keys to the crypto (SANS Institute, 2014d). If unauthorized crypto attempts to leave the network through proxy, it would have been caught and blocked.

The other technique in stopping stealthy hackers is by setting up crypto free zone. This crypto free zone solution from Dr. Cole is a heavily switched LAN so that the "last

© 2015 The SANS Institute Author retains full rights.

mile" on this local LAN is unencrypted (Cole, 2014b). A crypto detector is setup within this crypto free zone so that any encryption that passes through this zone will get caught. Thus, hacker's attempt to setup outbound encrypted C2 channel will get noticed in seconds instead of months (Cole, 2014b). As suggested by Dr. Cole, organizations should opt-in employees who tend to make poor decision when it comes to low trust sites or mindlessly click on any email attachments. The deployment of proxy in conjunction with crypto free zone would have caught hackers when they make an encrypted outbound command-and-control channel. This would alert security staff that an adversary has broken into the network. This is one of the means of performing better detection.

4. Monitoring, Logging, and Scanning

4.1. Penetration Testing and Vulnerability Assessment

The goal of any organization is to reduce risk. Before action can be taken on risk reduction, one of the most important things an organization should do is to perform regular penetration testing (pen-testing). Hackers are successful at penetrating organization's network because they do a great deal of reconnaissance and scanning before performing any kind of exploitation. Organization needs to know what exposures and targets are by first creating a network visibility map (SANS Institute, 2014c). Before organizations begin remediate problems found, they need to identify the top 10 to 15 critical assets and the vulnerability that goes with it. By properly prioritizing vulnerability with associated threats against top critical assets, organizations can stay on track with their risk reduction. Remember to scan in small successions because scanning the whole facility at once will result in a colossal list of problems, which will never get resolved. This is why it is crucial in identifying critical asset the organization wants to protect. This in turn will prioritize the starting point in mitigating vulnerabilities found.

Pen-testing is the technique of attempting to gain access to a network without knowledge of the network itself. The goal is to find out if a pen tester is able to gain access to the network and its critical assets without triggering detection mechanisms such as an IDS. Vulnerability assessment and pen-testing are similar but serve different but important functions. Pen-testing focus on how much information can be accessed during

© 2015 The SANS Institute Author retains full rights.

ethical hacking whereas vulnerability scanner is used to identify weaknesses that need addressing (Northcutt S., Shenk J.m Shackleford D., Rosenberg T., Sile R., Mancini S., 2006). Part of the pen-tester's task is to make detail notes on their reconnaissance and penetration of network while adverting detection. Pen-tester's role is important since if they're able to infiltrate their target, the hackers will be able to do the same. It is also a good health indicator of how efficient the security staff is at detecting and containing breaches. The pen-tester's report serves as a great tool in assessing the security staff's incident handling skills. Performing pen-testing from outside the network will be a good indication of how well the organization's security perimeter is (SANS Institute, 2014c).

Before using pen testing tools like hping3, nmap, nessus, and OpenVAS, always get permission before running them because these tools can break fragile systems. In addition to getting permission, communication and scheduling need to be established so that system owners and users are aware of the necessity of their system scan so that vulnerabilities are found before the attackers. Keep in mind that these tools can be used for harm as well as good. Hping3 has the ability to do stealthy port scans and IP address spoofing in addition to IP address discovery. Thus, it is essential that they be used by trained security professional or IT professional.

Hping3 can be used to find all visible IP address on the organization's network so that a road map to the network is mapped out. Organizations can easily see what systems are visible. A highly sensitive database server should only be visible to the application that accesses it. If that server were discoverable through hping3 scan, the organization would need to fix this vulnerability by fine tuning the firewall or place it in a protected VLAN if not done so already. Identification of critical asset and provide layered protection is the information centric approach. Protected enclave would place this server in a VLAN with restricted access. Nmap is then used to determine which ports and services are running on a given system. If there are no legitimate business reasons for a port to be opened, it must be turned off because they're an invitation for hackers to exploit. OpenVAS is a great open source vulnerability scanner that gets constant updates to its vulnerability database. It uses a suite of tools to test for known weaknesses and exploits on a target computer. The use of this tool can help organization assess how well their servers are protected against known attacks (SANS Institute, 2014c).

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

Knowing what servers and systems are out there on the network with regularly scheduled vulnerability scans would have discovered the server that failed to receive two-factor authentication. J.P. Morgan must discover where they are vulnerable before the adversary.

4.2. High Priority VLANs need dedicated NIDS

Now that critical assets are protected behind VLANs, dedicated Network-based Intrusion Detection Systems (NIDS) need to be deployed to monitor these high priority VLANs. An Intrusion Detection System (IDS) is a system that monitors malicious activities and alert a human for further analysis (SANS Institute, 2014c). Since NIDS are expensive and require constant monitoring, it should be deployed to monitor the organization's critical assets. Doing so would make it harder for hackers to find and exploit critical servers hence reducing the number of servers penetrated. Despite J.P. Morgan's effort in mandatory NIDS deployment on servers that store, process, and access confidential information, the breach went unnoticed (J.P. Morgan Chase & Co, 2013).

For IDS to be effective, they require good signatures and constant monitoring. An IDS alert is useless if security staff isn't actively monitoring them. A good set of signatures are a must because their job is to detect known attacks. Anomaly analysis is then used to detect unknown attacks such as zero-day exploits (SANS Institute, 2014c). For anomaly analysis to work, baseline of network is required so that IDS know what is normal. As security staff actively monitors IDS, they're able to fine-tune the system so that false-positives and noise are reduced as well as the added bonus of detecting misconfigured equipment (SANS Institute, 2014c). Active monitoring, good signature and proper tuning is required in having IDS perform its primary duty of detecting malicious activities.

4.3. Deploy Centralized Logging

One of the most important things an organization must do is logging because they provide insights to the health of systems. In fact, logging is so vital that hackers normally make an effort to delete them so that they can cover their tracks such as the case with J.P. Morgan (Yadron, 2014a). Unfortunately, log entries from a single data source will not be

© 2015 The SANS Institute Author retains full rights.

very useful since there isn't enough information to determine if an entry is an attack or normal daily operation. The attack will surface itself when cross correlating logs from IDS, firewall, operating system, web logs, switches and routers. Correlation of logs would be more efficient if all systems and devices have consistent time stamp through the use of Network Time Protocol (NTP). Having a centralized logging server will assist in better log correlation and protection against log destruction. It is always good to log more than to log less because information can be filtered during analysis (SANS Institute, 2014f). They also serve as evidence during incident handling phase should the organization get compromised (SANS Institute, 2014b). The systems that produce the logs needs to log both locally and to the centralized logging server because the local copy serves as a good backup and as a deterrent for hackers to delete. When hackers make attempts in covering their tracks, they will look for logs to delete.

Since a centralized log server should contain all events occurring in the environment, it needs to be protected. One of the major weaknesses to syslog is that it uses UDP, and does not require authentication. Hackers can send false information to the syslog port or fill up logging area by overwhelming the daemon. The protection against this is to make sure that firewall at the outmost perimeter block outside access to UDP port 514 (SANS Institute, 2014f). Another level of protection is to place this server behind protected VLAN with proper access control configured so that system that does not contribute to this log server is denied access. Syslog-NG is a cure to problems that the original syslog poses. Reliable TCP transport and authentication are some of the benefits to syslog-NG. In addition to better security handling, syslog-NG supports a wide variety of operating systems including Microsoft Windows Server. This allows all servers and devices to integrate their logs to one unified location. Consider using R-syslog because it supports systems with older syslog as well as newer security aware syslog-NG. Upgrading critical Linux servers with syslog-NG is a risk most organization should not take.

Consolidation of logs in one secure centralized location will help organizations to better pin point attacks that seems benign from one single source. The advantage of not being able to delete log files would have benefited J.P. Morgan since it would be difficult if not impossible for hackers to cover their tracks. This would have provided J.P. Morgan

© 2015 The SANS Institute Author retains full rights.

complete record of the breach instead of an estimation of when the hackers penetrated their network. With regular monitoring of logs, J.P. Morgan would be able to detect hackers as the network is being attacked.

4.4. The minimum baseline logging for Windows Servers

Logging is equally important on Windows servers because many organizations have a mixture of Linux servers and Windows servers. Based on the type of Windows server engineer J.P. Morgan is looking for (J.P. Morgan Chase Jobs), it's safe to assume the biggest bank in United States will make use of domain controller, active directory, NTFS as the file system and group policy to manage all the Windows clients out there. The requirements for minimum baseline logging on Windows servers are the access points. Any access or changes to administrator access, privileged access and take ownership access must be logged. Any access to critical data and databases must also be logged. Entry points into the network such as web servers, email servers and DMZ servers must also be logged. Those three areas are hacker's gateway into Windows server penetration. Since syslog-NG supports Windows servers, this is a great way for Windows logs to contribute data to the centralized log server (SANS Institute, 2014e). Having those minimum baseline logging with constant supervision from security staff would have caught and alerted J.P. Morgan when hackers gain access to high-level administrator privileges.

4.5. Anonymous access and guest accounts on Windows

One security measure that must be taken on Windows machines are the disabling of anonymous access and guest accounts. Anonymous access must be disabled because many Windows vulnerabilities are caused by null user sessions. A null user session is essentially a Server Message Block (SMB) session with blank username and password. Hackers can use tools like dumpusers.exe from http://www.ntsecurity.nu to get a list of all user and group name without authentication (SANS Institute, 2014e). If every Windows computer within an organization has been upgraded to Windows 7 or above, disabling anonymous access should not affect anyone.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

If someone is trying to authenticate to a Windows machine with username that this computer or domain controller does not recognize, this remote user will automatically be logged on as guest (SANS Institute, 2014e). The best policy here is to disable guest account across all Windows machines within the domain through domain Group Policy Object (GPO). Not only should guest account be disabled, a complex random password must be set. The other parameter to set is to prevent logon time for all hours and all days so that if guest was ever set active, it can never login. There are no details as to how hackers gain access to the systems. With Microsoft Windows being a part of the important fleet of computers at J.P. Morgan, it is essential in closing simple vulnerabilities loopholes such as guest account and anonymous access (Team3J.P.MC, 2010). This is a good strategy for fine tuning access because anonymous and guest have no legitimate need to access host systems.

4.6. Applying Least Privileged with SELinux or AppArmor

One of the best ways to enhance least privileged access control on Linux servers is with SELinux (SANS Institute, 2014f). Security-Enhanced Linux (SELinux) was designed by NSA and the Linux community with purpose to enhance the security aspects of Linux systems by offering stricter controls on permissions, access, and processes (SANS Institute, 2014f). One of the biggest advantages is that it locks down critical systems with the assumption that users have no rights unless specifically granted. The other advantage is multi-level and multi-category security with defense style Mandatory Access Control (MAC) (Coker, 2004). Since most critical Linux servers have existed within the organization for some time already, the alternative is AppArmor, which function similarly as SELinux. The configuration aspect is easier than SELinux and does not require patching of kernel or daemons. The final decision of using SELinux or AppArmor comes down to how the existing Linux security control is configured. If existing Linux configuration has default deny access setup, there's no need for SELinux or AppArmor. If finite control over security permissions is desired, SELinux or AppArmor is highly recommended (SANS Institute, 2014f). The use of SELinux or AppArmor is a good tool in helping IT staff in strengthening access.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

4.7. Monitor and Make Use of Honeypots

Honeypots are systems that serve no purpose other than to draw attackers (SANS Institute, 2014c). Since honeypots serve no legitimate business purpose, no traffic should happen on that system other than pen-tester and hackers. Traffic on a honeypot are either accidental or hostile and require immediate attention and analysis pertaining to the intent of activities.

Honeypots needs to have proper patches and protection just like critical assets so that it doesn't become a liability for hackers to abuse (SANS Institute, 2014c). One of the interesting methods from Terrence O'Conner is to list honeypots in DNS for would be hackers to find (O'Conner, 2010). Keep in mind that honeypots are not deploy and forget devices because they need to be kept under supervision. As hackers scan for systems to penetrate, honeypots would help filter out true attack traffic and insights into the tactics and tools of choice (SANS Institute, 2014c).

More than 90 servers were controlled by hackers during the J.P. Morgan breach. Honeypot would have help discovered the breach because there's a high probability that hackers would have stumble upon them during their server heist. The use of honeypots, IDS, proxy, crypto free zones, and constant monitoring of log servers will help J.P. Morgan detect attacks on network because detection is a must.

5. Conclusion

Brian Kerbs (2014) said security is all about layers, and not depending on any one technology. Part of the information centric defense in depth strategy is to provide layered protection. The United States Bullion Depository at Fort Knox will not let any employee see or get close to its gold reserve. In able to get to the vault, several members of the highly trusted staff must enter their own code in succession to access the vault. The vault is then surrounded by offices and storerooms with the exterior made out of steel and concrete. Guard boxes, sentry boxes and the most modern protective devices, protect the interior of the building (Fort Knox Bullion Depository, 2011). Similarly, an organization's critical assets should be heavily protected like Fort Knox with fortified VLANs protecting critical assets and NIDS as the sentry box. Firewalls are important perimeter defense while hiding critical assets from prying eyes.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

HIPS, basic protection, employee education, and application whitelisting working together would have caught and stopped the malware from entering J.P. Morgan's network. Employees would have been made aware of social engineering through awareness education, thus, reducing the chance of having their credentials stolen. Pre-connection NAC and VLAN implementation are used to quarantine the infected system while alerting security staff that something bad has entered the network. NIDS' anomaly analysis with honeypots is used to catch zero-day vulnerabilities so that attempts to control servers are caught. Least privileged access control with the implantation of RBAC, SELinux and AppArmor will help reduce the amount of data stolen if the hackers were able to get that far. To guard against privilege escalation, proper logging of access with active monitoring would alert staff so that they're able to stop hackers from doing more damage. With all traffic going through proxy and the use of crypto free zone, NIDS would be able to see ill-intent traffic thus thawing the thieves' attempt in adverting detection. Pen-testing and vulnerability scans would have discovered the overlooked server that failed to receive two-factor authentication and vulnerabilities in the network. Pen-testing would also show J.P. Morgan how hackers could have penetrated their network so that IT staff can better fortify the network against future attacks. No entity is safe from hackers unless they turn off all the computers. Even though protecting critical assets would make it difficult for thieves to break in, detecting their presence is mandatory. With the recommended solutions, J.P. Morgan is able to detect and contain attacks against their network when hackers breach the outer perimeter.

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

References

Apple Inc. (2014, November 14). *OSX: about gatekeeper*. Retrieved from Apple: http://support.apple.com/en-us/HT202491

Barrett, P. (2014, December 22). Forget the gossip. The Sony hack has graver consequences. *Bloomberg Businessweek*, 20-22.

Bell, L. (2014, December 23). *J.P. Morgan data breach could have been avoided with simple security fix*. Retrieved from The Inquirer: http://www.theinquirer.net/inquirer/news/2388071/J.P.-morgan-data-breach-could-have-been-avoided-with-simple-security-fix

Cisco. (2008, May 8). *Securing networks with private VLANs and VLAN access control lists.* Retrieved from Cisco: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/10601-90.html

Chee J. (2008, June 2). *Host Intrusion Prevention System and Beyond* [White paper]. Retrieved from SANS reading room: http://www.sans.org/reading-room/whitepapers/intrusion/host-intrusion-prevention-systems-32824

Coker R. (2004, November). *What is security-enhanced linux?* Retrieved from RedHat: http://www.redhat.com/magazine/001nov04/features/selinux/

Cole E. (2014a, October). *The self-defending network: is it real technology or market speak?* Retrieved from TechTarget: http://searchsecurity.techtarget.com/magazineContent/The-self-defending-network-Is-it-real-technology-or-market-speak

Cole E. (2014b, November). *Using crypto-free zones to thwart advanced attacks.* Retrieved from TechTarget: http://searchsecurity.techtarget.com/tip/Using-crypto-free-zones-to-thwart-advanced-attacks

Cole E. (2014c, August). *Insider threats in law enforcement* [White paper]. Retrieved from SANS reading room: http://www.sans.org/reading-room/whitepapers/threats/insider-threats-law-enforcement-35402

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

Dolmetsch C. (2015, January 15). *J.P.Morgan asked by states for detail on 2014 data breach*. Retrieved from Bloomberg: http://www.businessweek.com/news/2015-01-14/J.P.morgan-asked-by-states-for-more-detail-on-2014-data-breach

Fort Knox Bullion Depository. (2011, May 7). Retrieved from http://www.globalsecurity.org/military/facility/fort-knox-depository.htm

Fraud.org. (n.d.). *Phishing.* Retrieved from http://www.fraud.org/scams/internet-fraud/phishing

Glazer E., & Sidel R. (2014, August 28). *J.P. Morgan working closely with law enforcement on cyberattack*. Retrieved from The Wall Street Journal: http://www.wsj.com/articles/j-p-morgan-not-seeing-unusual-fraud-regarding-reports-of-hacking-1409227168

Goldstein, M., Perlroth N., & Corkery M. (2014a, December 22). *Neglected server provided entry for J.P.Morgan hackers*. Retrieved from The New York Times: http://dealbook.nytimes.com/2014/12/22/entry-point-of-J.P.morgan-data-breach-is-identified/?_r=1&module=ArrowsNav&contentCollection=Business%20Day&action=keypress&region=FixedLeft&pgtype=Blogs

Goldstein M., & Perlroth N. (2014b, October 31). *Luck played role in discovery of data branch at J.P.Morgan affecting millions.* Retrieved from The New York Times: http://dealbook.nytimes.com/2014/10/31/discovery-of-J.P.morgan-cyberattack-aided-by-company-that-runs-race-website-for-bank/

J.P.Morgan Chase & Co. (2014a). *United States Securities and Exchange Commission form 10-Q*. Retrieved from Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/19617/000001961714000409/corpq22014.htm

J.P.Morgan Chase & Co. (2014b). *United States Securities and Exchange Commission form 8-K.* Retrieved from Securities and Exchange Commission: http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm

J.P.Morgan Chase & Co. (2013, October 3). *J.P.MC's minimum control requirements*. Retrieved from J.P.Morgan Chase:

© 2015 The SANS Institute Author retains full rights.

http://www.J.P.morganchase.com/corporate/About-J.P.MC/document/236963_J.P.MC_Minimum_Control_Requirements_3Oct2013_ada.pdf

J.P.Morgan Chase Jobs - Digital – ServerOps Windows Engineer in AP, Indiana, United States. (n.d.). Retrieved from http://J.P.mchase.jobs/ap-in/digital-serverops-windows-engineer/66C009E21B8342AFB3BFB8D45D39E95E/job/

Kaspersky Lab. (2012). *Host-based Intrusion Prevention System (HIPS)* [White paper]. Retrieved from: http://www.kaspersky.com/images/Kaspersky_Lab_Whitepaper_HIPS_ENG.pdf

Kobialka D. (2014, August 26). *Gartner: information security spending will top $71B this year.* Retrieved from MSPmentor: http://mspmentor.net/managed-security-services/gartner-information-security-spending-will-top-71b-year

Koppala A., & Wills K. (2014, October 31). *J.P. Morgan found hackers through breach of corporate event website: media*. Retrieved from Reuters: http://www.reuters.com/article/2014/11/01/us-j-p-morgan-cybercrime-idUSKBN0IL2JM20141101

Krebs B. (2014 May 07). Antivirus is dead: long live antivirus! [Blog post]. Retrieved from http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/

Kurane S. (2014, December 22). *J.P.Morgan data breach entry point identified: NYT*. Retrieved from Reuters: http://www.reuters.com/article/2014/12/23/us-J.P.morgan-cybersecurity-idUSKBN0K105R20141223

Law E. (2011, March 22). *Everything you need to know about authenticode code signing* [Blog post]. Retrieved from MSDN: http://blogs.msdn.com/b/ieinternals/archive/2011/03/22/authenticode-code-signing-for-developers-for-file-downloads-building-smartscreen-application-reputation.aspx

Lewis N. (2010, August). *Prevent a privilege escalation attack with database security policy*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/answer/Prevent-a-privilege-escalation-attack-with-database-security-policy

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

Mallinenib. (2013, November 2). *Privilege escalation* [Blog post]. Retrieved from IT Security Concepts: http://itsecurityconcepts.com/tag/privilege-escalation/

Mathews L. (2014, December 10). *Sony hackers stole digital certificates which someone used to sign malware*. Retrieved from Geek.com: http://www.geek.com/apps/sony-hackers-stole-digital-certificates-which-someone-used-to-sign-malware-1611372/

McAdams S. (2005, February 22). *Local privilege escalation in Solaris 8 and Solaris 9 via bugger overflow in passwd(1)* [White paper]. Retrieved from SANS reading room: https://www.sans.org/reading-room/whitepapers/solaris/local-privilege-escalation-solaris-8-solaris-9-buffer-overflow-passwd1-1600

Mimoso M. (2014, December 24). *Two-factor snafu opened door to J.P.Morgan breach*. Retrieved from Threat Post: https://threatpost.com/two-factor-snafu-opened-door-to-J.P.morgan-breach/110119

Munson L. (2014, October 3). *J.P. Morgan Chase confirms breach, 76 million homes and 7 million businesses affected*. Retrieved from Sophos: https://nakedsecurity.sophos.com/2014/10/03/J.P.-morgan-chase-confirms-breach-76-million-homes-and-7-million-businesses-affected/

National Institute of Standards and Technology. (1992). *Role-based access controls* [White paper]. Retrieved from http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf

Northcutt S., Shenk J.m Shackleford D., Rosenberg T., Sile R., Mancini S. (2006, November 17). *Penetration testing: assessing your overall security before attackers do* [White paper]. Retrieved from SANS reading room: http://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Northcutt S. (2007, February 26). *Protected enclaves defense-in-depth.* Retrieved from SANS.edu: http://www.sans.edu/research/security-laboratory/article/372

O'Conner T. (2010, December 1). *About face: defending your organization against penetration testing teams* [White paper]. Retrieved from SANS reading room: http://www.sans.org/reading-room/whitepapers/testing/about-face-defending-organization-penetration-testing-teams-33553

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

Palermo E. (2013, December 17). *What is privilege escalation.* Retrieved from Tom's Guide: http://www.tomsguide.com/us/privilege-escalation,review-1983.html

Perrin C. (2010, April 19). *Mitigating the privilege escalation threat*. Retrieved from TechRepublic: http://www.techrepublic.com/blog/it-security/mitigating-the-privilege-escalation-threat/

Piper S. (2014). *Definitive guide to next-generation network access control*. Retrieved from: http://www.forescout.com/forms/ebook_definitive_guide_nac_drip/

Riley M., & Robertson J. (2014, August 27). *FBI examining whether Russia is tied to J.P.Morgan hacking*. Retrieved from Bloomberg: http://www.bloomberg.com/news/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-J.P.morgan-hacking.html

Roberts P. (2014, October 3). *Report: hacked password behind compromise of 75m J.P.Morgan accounts*. Retrieved from: https://securityledger.com/2014/10/hacked_password_behind_compromise_of_75m_J.P.morgan_accounts/

Robertson J., & Riley M. (2014, August 29). *J.P.Morgan hackers came in the front door – in June. Two months of mayhem.* Retrieved from Bloomberg: http://www.bloomberg.com/news/2014-08-29/J.P.morgan-hack-said-to-span-months-via-multiple-flaws.html

Rouse M. (2014, November). *Social Engineering*. Retrieved from TechTarget: http://searchsecurity.techtarget.com/definition/social-engineering

SANS Institute. (2014a). *401.1 Networking Concepts.* Bethesda, MD: SANS Institute.

SANS Institute. (2014b). *401.2 Defense-in-Depth.* Bethesda, MD: SANS Institute.

SANS Institute. (2014c). *401.3 Internet Security Technologies*. Bethesda, MD: SANS Institute.

SANS Institute. (2014d). *401.4 Secure Communications*. Bethesda, MD: SANS Institute.

SANS Institute. (2014e). *401.5 Windows Security*. Bethesda, MD: SANS Institute.

SANS Institute. (2014f). *401.6 Linux Security*. Bethesda, MD: SANS Institute.

Shackleford D. (2009 October). *Application whitelisting: enhancing host security* [White paper]. Retrieved from SANS reading room:

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

http://www.sans.org/reading-room/whitepapers/analyst/application-whitelisting-enhancing-host-security-34820

Sherman E. (2014, August 28). *Why $250M didn't protect J.P.Morgan from hackers.* Retrieved from: http://www.cbsnews.com/news/why-250m-didnt-protect-J.P.-morgan-from-hackers/

Silver-Greenberg J., Goldstein M., & Perlroth N. (2014, October 2). *J.P.Morgan Chase hacking affects 76 million households.* Retrieved from The New York Times: http://dealbook.nytimes.com/2014/10/02/J.P.morgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

Sjouwerman, S. (2014, August 28). J.P. Morgan hacked because malware infects employee PC [Blog post]. Retrieved from http://blog.knowbe4.com/bid/395379/J-P-Morgan-Hacked-Because-Malware-Infects-Employee-PC

Sjouwerman. (2011). *Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008*. Clearwater, FL: KnowBe4.

Snyder J. (2010, May 24). *NAC: What went wrong*. Retrieved from NetworkWorld: http://www.networkworld.com/article/2209345/security/nac--what-went-wrong-.html

Son H. (2014, October 2). *J.P.Morgan employee password was key in hack hitting 76 million homes*. Retrieved from Bloomberg: http://www.bloomberg.com/news/2014-10-02/J.P.morgan-says-data-breach-affected-76-million-households.html

Team3J.P.MC. (2010, November 1). Hardware and software [Blog post]. Retrieved from http://team3J.P.mc.blogspot.com/2010/11/hardware-and-software.html

USA.gov. (2014, November 14). *Phishing scams: what you need to know*. Retrieved from USA.gov: http://www.usa.gov/topics/consumer/scams-fraud/types/phishing-scams.shtml

Weber H. (2003, October 8). *Role-based access control: the NIST solution* [White paper]. Retrieved from SANS reading room: http://www.sans.org/reading-room/whitepapers/sysadmin/role-based-access-control-nist-solution-1270

Yadron D., & Glazer E. (2014a, October 31). *J.P. Morgan found hackers through breach of road-race website*. Retrieved from The Wall Street Journal:

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

http://www.wsj.com/articles/j-p-morgan-found-hackers-after-finding-breach-of-race-website-1414766443

Yadron D., Glazer E., & Barrett D. (2014b, August 28). *FBI probes possible hacking incident at J.P. Morgan*. Retrieved from The Wall Street Journal: http://www.wsj.com/articles/fbi-probes-possible-computer-hacking-incident-at-j-p-morgan-1409168480

Yadron D. (2014c, May 4). *Symantec develops new attack on cyberhacking*. Retrieved from The Wall Street Journal: http://www.wsj.com/articles/SB10001424052702303417104579542140235850578

Allen Jeng, ajeng@adobe.com

© 2015 The SANS Institute Author retains full rights.

Last Updated: June 20th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

Security Operations Summit & Training 2019	New Orleans, LAUS	Jun 24, 2019 - Jul 01, 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 Paris July 2019	Paris, FR	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Munich July 2019	Munich, DE	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS London July 2019	London, GB	Jul 08, 2019 - Jul 13, 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 Cyber Defence Singapore 2019	Singapore, SG	Jul 08, 2019 - Jul 20, 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 Pen Test Hackfest Europe 2019	Berlin, DE	Jul 22, 2019 - Jul 28, 2019	Live Event
SANS San Francisco Summer 2019	San Francisco, CAUS	Jul 22, 2019 - Jul 27, 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 July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	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 San Jose 2019	San Jose, CAUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Prague August 2019	Prague, CZ	Aug 12, 2019 - Aug 17, 2019	Live Event
Supply Chain Cybersecurity Summit & Training 2019	Arlington, VAUS	Aug 12, 2019 - Aug 19, 2019	Live Event
SANS Minneapolis 2019	Minneapolis, MNUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Virginia Beach 2019	Virginia Beach, VAUS	Aug 19, 2019 - Aug 30, 2019	Live Event
SANS Amsterdam August 2019	Amsterdam, NL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Chicago 2019	Chicago, ILUS	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS MGT516 Beta Three 2019	Arlington, VAUS	Aug 19, 2019 - Aug 23, 2019	Live Event
SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS New York City 2019	New York, NYUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Cyber Defence Canberra 2019	OnlineAU	Jun 24, 2019 - Jul 13, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced