Sample Penetration Test Report - Example Institute

Prepared By

Document History:

Version	Date	Person	Notes, Comments, Reasons
1.0			

Table of Contents

1.0 Executive Summary

1.1 Overview

Example Institute (CLIENT) engaged PurpleSec, LLC to conduct penetration testing against the security controls within their information environment to provide a practical demonstration of those controls' effectiveness as well as to provide an estimate of their susceptibility to exploitation and/or data breaches. The test was performed in accordance with PurpleSec Information Security Penetration Testing Method. PurpleSec's Information Security Analyst (ISA) conducted all testing in coordination with CLIENTs Information Technology (IT) staff members to ensure safe, orderly, and complete testing within the approved scope.

CLIENT's information environment is protected by endpoint antivirus and administrative controls managed by an Active Directory. The environment contains numerous vulnerabilities, including some very serious security flaws such as EternalBlue which makes them susceptible to data breaches and system takeovers. Highly important files which contain HIPAA and payment information are easily accessible and very visible; putting the CLIENT at great risk to compliance violation and potentially subject to large fines and/or loss of business reputation.

1.2 High-Level Test Outcomes

Internal penetration test: Intended to simulate the network-level actions of a malicious actor who gained a foothold within the internal network zone.

Overall, CLIENT presents a high-risk attack surface with major critical vulnerabilities that allowed complete root access to multiple systems exist within CLIENT's critical infrastructure.

The EPO server and the Remote Desktop Server were both susceptible to EternalBlue; a shell was opened on both remotely by exploiting the SMBv1 vulnerability using a Publicly available exploit module which remotely attacked the spoolsv.exe service via port 445 (SMB). The Remote Desktop server contained numerous user files of CLIENT's staff members. Traversing the user profile data revealed many files that contained private patient healthcare information including diagnostics, health insurance information, and transaction receipts. The ability to control the system as NT Authority makes data exfiltration trivial as any user specific permissions are not applied to NT Authority user.

Two other systems had the SChannel (CVE-2014-6321) vulnerability which makes them susceptible to DoS via code over Schannel. A script can be written to exploit this vulnerability and cause the receiving system to open multiple threads and lockout the processor. This was not exploited as PurpleSec does not use DDOS in its testing.

1.3 Overall Risk Rating

Having considered the potential outcomes and the risk levels assessed for each documented testing activity, PurpleSec considers Example Institute's overall risk exposure regarding malicious actors' attempts to breach and/or control resources within their information environment to be EXTREME (as determined using PurpleSec Risk Matrix).

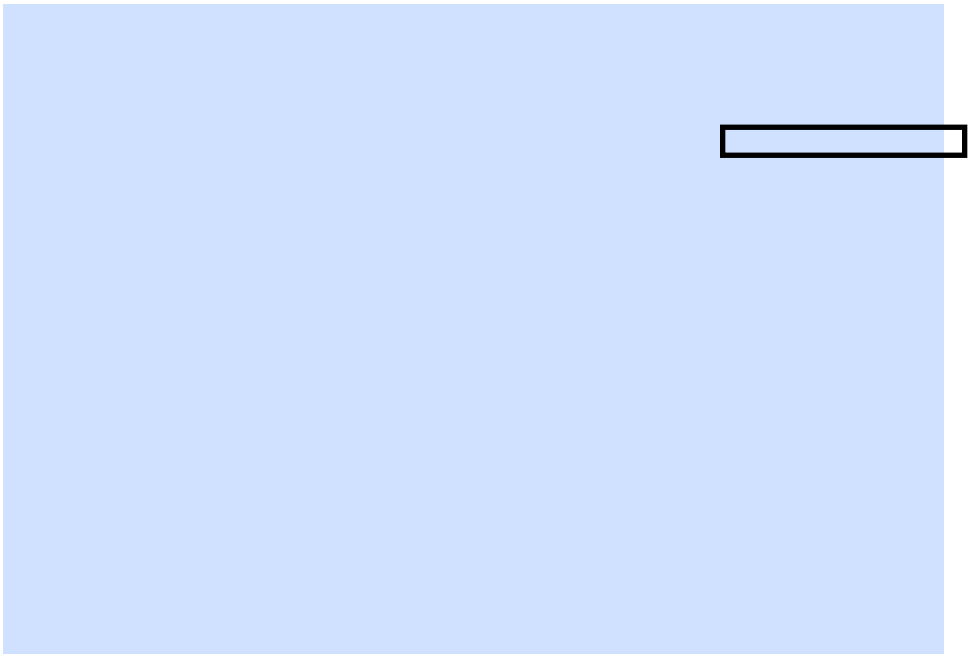


Fig. 1-1: PurpleSec Risk Matrix

1.4 Prioritized Recommendations

Based on the results achieved during the test project PurpleSec makes the following recommendations (presented by order of priority):

- Patch critical systems (Microsoft Security Bulletin MS17-010 –Critical)
- Run Vulnerability Scans on at least monthly basis (scan-patch-scan again)
- Change passwords (10+ complex characters) on all systems that contain ePHI.
- Social Engineering training for every employee.
- Disable SMB and spoolsvc on McAfee server.

2.0 Test Scope and Method

2.1 Extent of Testing

Example Institute engaged PurpleSec to provide the following penetration testing services:

- Network-level, technical penetration testing against hosts in the internal networks.
- Network -level, technical penetration testing against internet facing hosts.
- Social Engineering, phone phishing against CLIENT employees.
- Social Engineering, email phishing against CLIENT employees.

2.2 Test Scope Summary

The following information environment zones were included in the scope of the penetration test:

- Internal Network: Example Institute's general internal networks.

The test was conducted in two phases:

- Internal stage: Starting from the internal network zone. Intended to simulatethe network-level actions of a malicious actor who gained a foothold within the internal network zone.

(Remainder of page left intentionally blank)

3.0 Internal Phase

3.1 Phase Summary

PurpleSec's ISA conducted various reconnaissance and enumeration activities. Port and vulnerability scanning, as well as other reconnaissance activities revealed serious security holes. The most concerning vulnerabilities allow complete system takeover on important servers, most critically the McAfee Security server; compromise of which could allow a potential attacker to render the endpoint security for the entire internal network inoperable or ineffective.

Once server compromise was achieved, directory traversal to search for important data was conducted. The analyst was able to identify many directories with private patient data and numerous other data that would fall under HIPAA and PCI compliance.

3.2 Actions Taken

To determine and practically demonstrate the feasibility of expanding access given a foothold within the internal network, the ISA conducted the following activities:

From Zone: Internal network
Via: N/A
To Zone: Internal network
Method: Network-level penetration testing

Current Zone Activities:

The ISA used a SecureSensor deployed inside Example Institute's facilities to conduct port, service, and vulnerability scanning as well as other reconnaissance techniques within Example Institute's internal networks. Vulnerabilities were found and validated. SMB vulnerability ETERNALBLUE was exploited to gain root level access to multiple critical systems including the McAfee system security server.

Microsoft Windows SMBv1 Multiple Vulnerabilities *(ETERNALBLUE)*

CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148

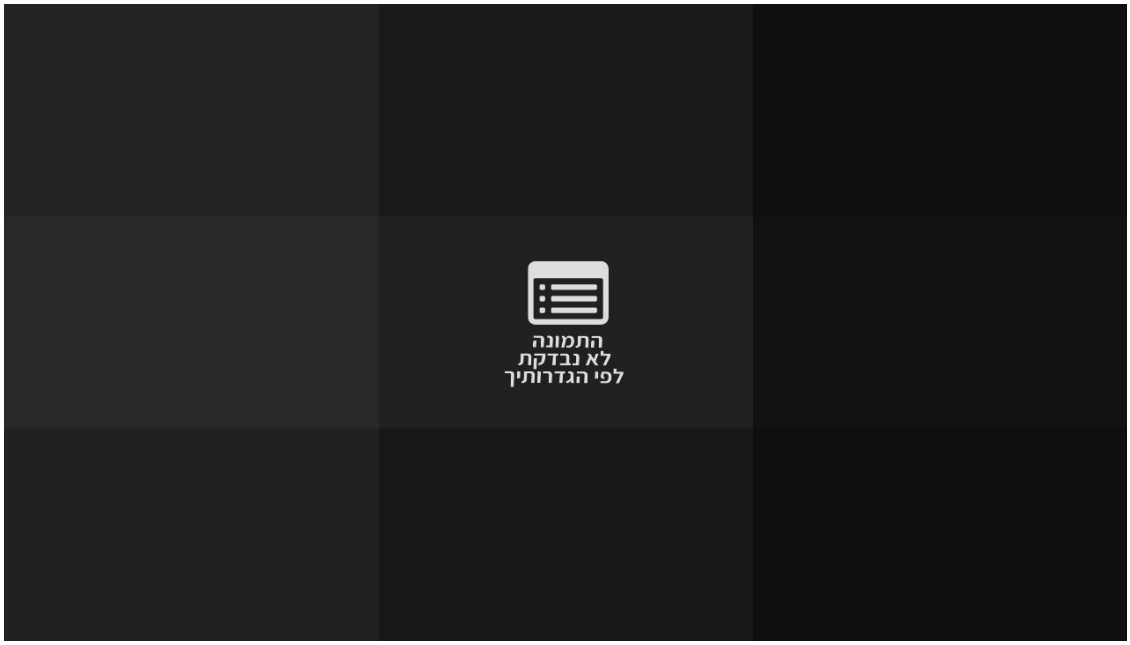
EternalBlue is an exploit developed by the NSA and leaked via ShadowBrokers in 2017. Recent similar “Eternal” exploits have been developed to attack systems from Windows Server 2000 up to the latest OS releases.

EternalBlue gives the attacker complete root access to the target system via a buffer overflow when sending specially crafted SMB packets to the server. The overflow executes code in a target service such as ***spoolsv.exe.*** Once the remote shell is opened, the attacker has control of the system as “NT Authority” which is kernel access in Windows systems, allowing complete system takeover.

The SMB SMBv1 vulnerability opens the system up to the possibility of Ransomware attacks such as WannaCry, which are delivered as payloads via EternalBlue type attacks.

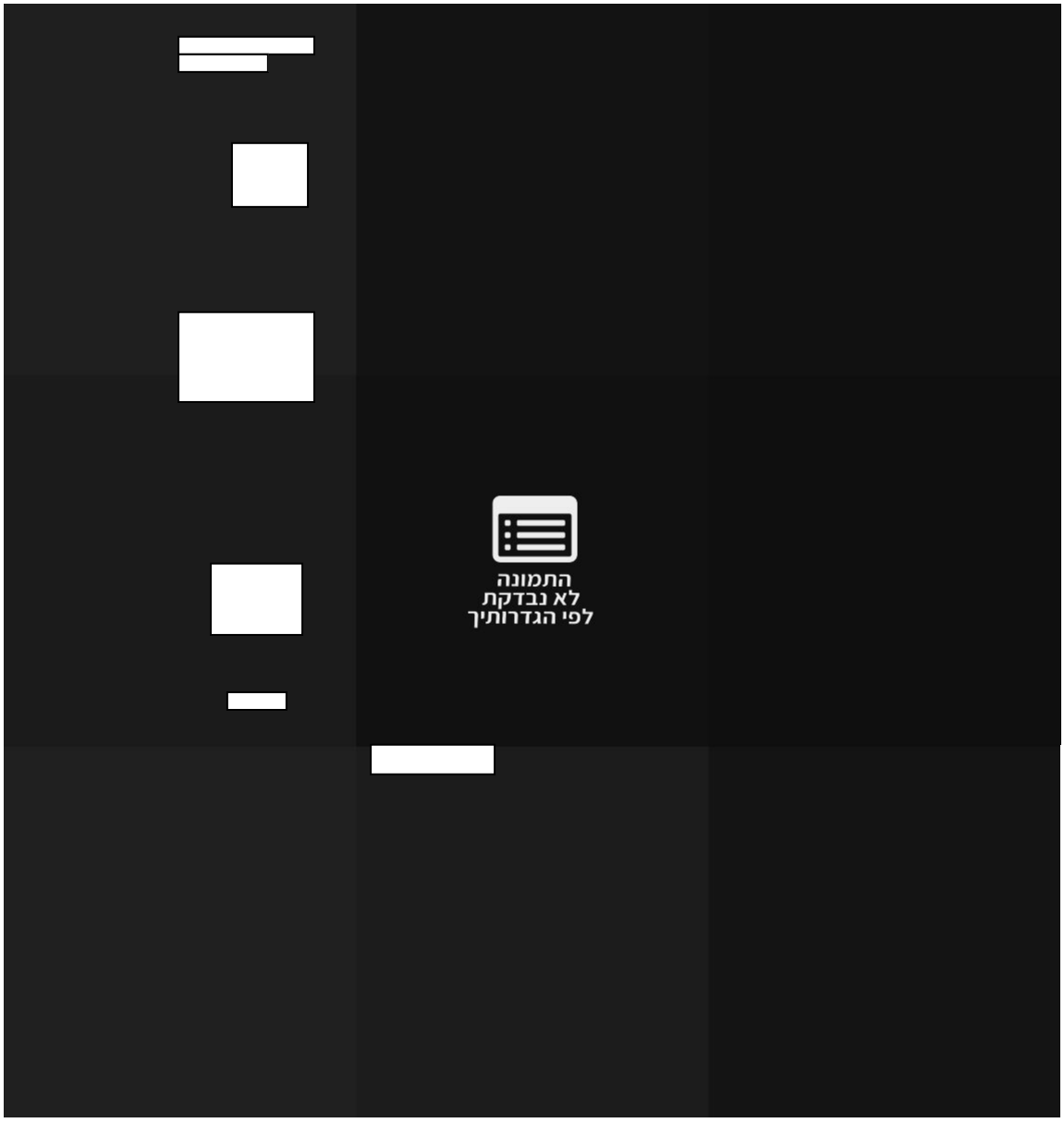
PurpleSec’s ISA was able to gain root access to the system <hostname> 192.168.1.235 and <hostname> 192.168.1.222 (McAfee Security Server) via CVE-2017-144. The analyst attempted to connect to the remote system via the SMB port 445 and without any credentials as a reconnaissance step to validate whether the remote system was honoring SMB connection requests.

Once the connection was validated, the analyst used publicly available tools to exploit the vulnerability.



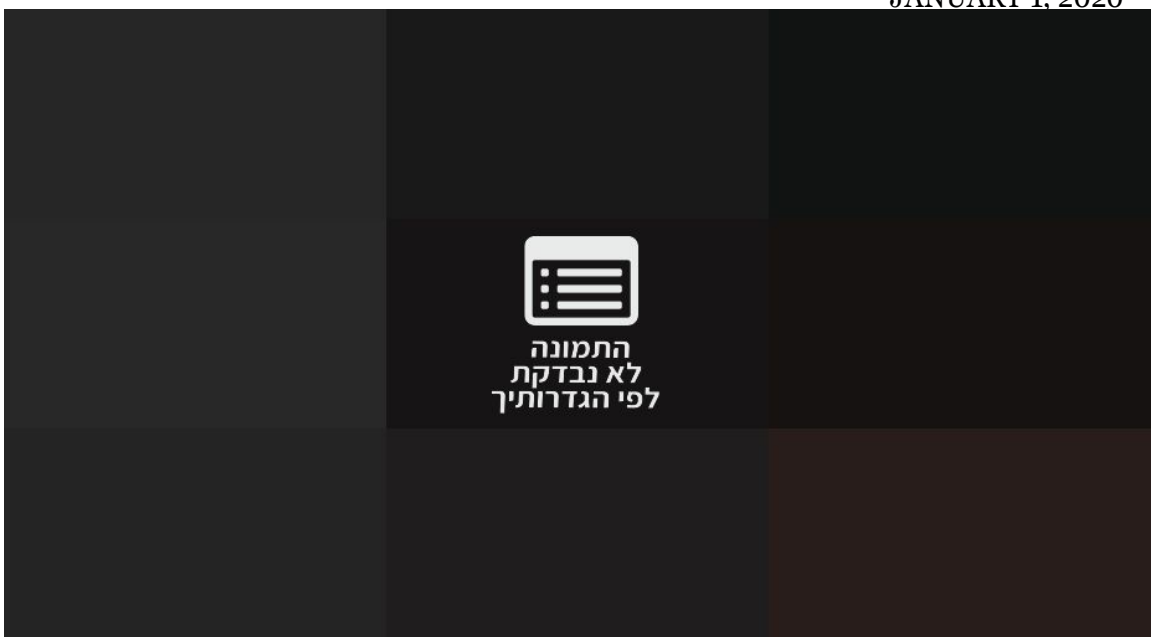
Prompt changes to C:\windows\system 32, indicating that a remote shell has been established at the root of the target OS.

From here the analyst performs several directory traversals to move to the root drive and begin reconnaissance for critical files such as patient information, ePHI, PII, and payment information. Traversing user profile document folders revealed several folders with sensitive, confidential patient and hospital information. Due to attaining access as the NT Authority user, no permissions settings or passwords prevent access to any of the files on the system.



User profiles contain various files that, if breached, could make Example Institute liable for fines.

In addition to the noted HIPAA and ePHI files, a PFX certificate file was also located on the server.



PFX Files are encrypted files which may contain data or be used as secret keys to access other encrypted data or systems. PFX files have been breached under research conditions Additionally, if an attacker as root system accesses the **%Appdata%\Microsoft\Protect\<SID>\BK-<NETBIOSDOMAINNAME>** path, they can use the stored backup key here to take over all the identities and secrets in the domain.
I recommend any secrets on systems be evaluated at the minimum

This risk of this critical vulnerability can be further demonstrated. With root access an attacker can do any administrative and system level action without any need for passwords or logins. Using this vulnerability, the ISA was also able to create a local RDP user that would allow me Remote Desktop access to the server using a username and password of my choice. There is further risk of privilege escalation because NT Authority user can promote any other users to Admin level access, including Domain Admin, if the target system is an Active Directory server or has rights to configure Domain settings remotely.

The McAfee Security Server (192.168.1.222) was vulnerable to the same ETERNALBLUE exploit. As SMB and spoolsv.exe services were running on the McAfee server the attack was executed using the same method described above. Initially the shell failed to open, which is common with this exploit; a retry resulted in successful execution.

SSL Version 2 and 3 Protocol Detected*:*

A network reconnaissance scan detected multiple hosts with a vulnerable version of SSLv2 and SSLv3. 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'.

Hosts Affected:

192.168.1.248	192.168.1.230
192.168.1.251	192.168.1.39
192.168.1.252	192.168.1.204
192.168.1.221	192.168.1.198
192.168.1.205	192.168.1.200
192.168.1.182	192.168.1.194

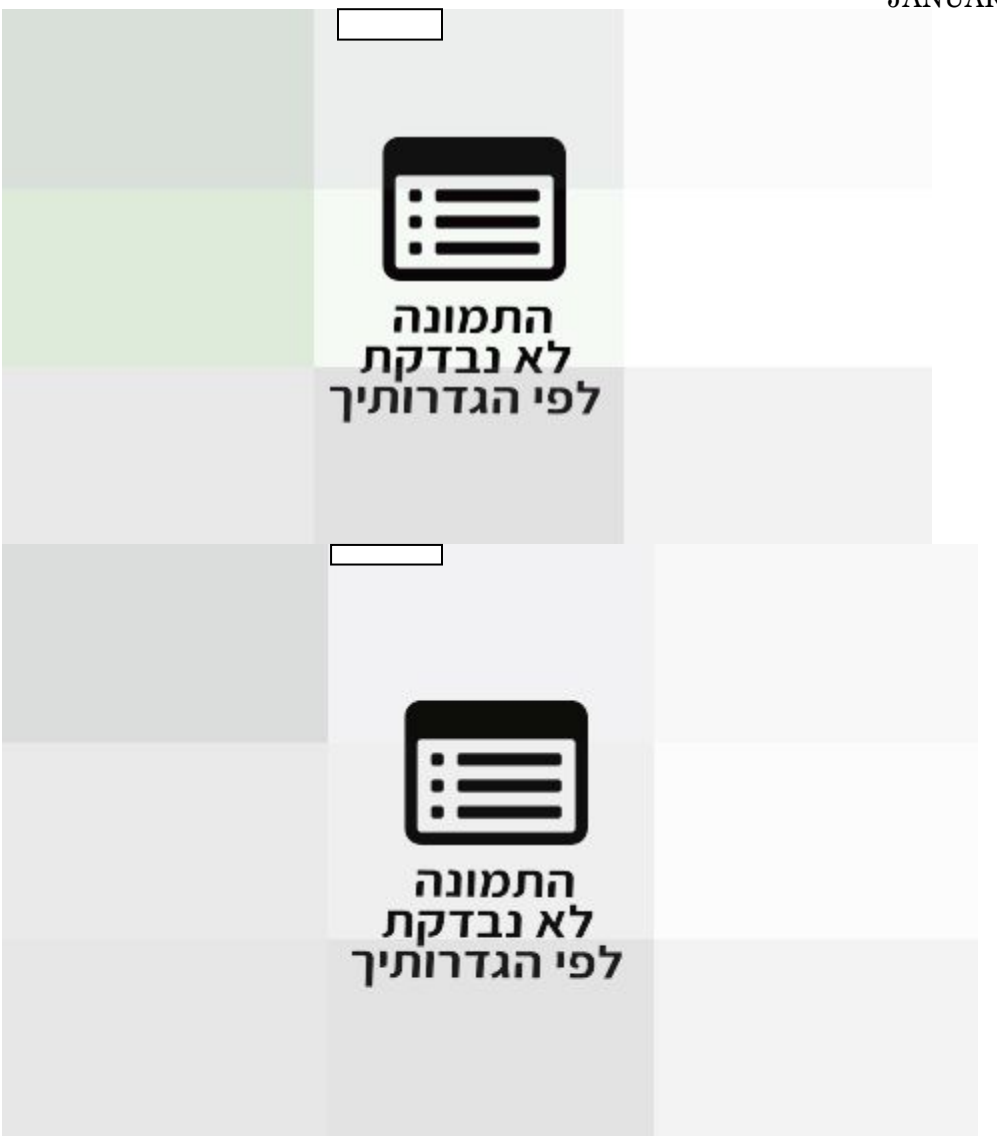
Affected hosts were validated with a network level cipher scan using the nmap tool. Analyst targeted the scan at these specific hosts using a script that would display the cipher suite information for blocks of open ports on the targeted systems.

The output scan was filtered to display only those systems which contained insecure versions of SSL.

All the below affected hosts were validated to contain the vulnerable SSL.


התמונה
לא נבדקת
לפי הגדרותיך


התמונה
לא נבדקת
לפי הגדרותיך



MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)(WINSHOCK)

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the SecureChannel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

EXPLOIT:
The exploit for this vulnerability is a remote code execution that typically results in a

Denial of Service (DoS) Attack. Due to the nature of the testing, this exploit is out of scope for the exercise.

Outsider Risk Rating:

Insider Risk Rating: EXTREME

Bottom Line:

Nearly all CLIENT's internal networks hosts appear to be properly patched and up-to-date. Attack vectors are available to an adversary who targeted CLIENT. Considering CLIENT's lack of IT personnel or Security Engineer, an attacker could find success through Social Engineering or Physical attack methods due to the lack of training and resources found during this penetration testing.

Recommendations:

- Disable SMB on all systems where it is not required for business purposes. The service may be shut down via GPO on the domain, or through manual service disabling on local admin accounts.
- Disable spoolsvc.exe and other non-essential processes on Critical Security Infrastructure such as the McAfee Security Server. Processes running increase the attack surface of the systems. Disabling these services can help harden the systems and create a smaller, more secure risk landscape.
- Disable SSLv2 and SSLv3 on any system where legacy encryption is not necessary. Most applications use better encryption built-in but use SSL as a fallback option when needed for legacy support.

(Remainder of page left intentionally blank)

4.0 External Phase

4.1 Phase Summary

The external phase of the pentest focused on the assets which are publicly accessible. Reconnaissance and scanning were conducted to identify opportunities for intrusion or malicious modification of the systems.
Attacks were launched from PurpleSec network via Internet to the externally accessible assets at CLIENT using BurpSuite and network scanner NMAP.

4.2 Actions Taken

To determine the risk level of CLIENT's externally accessible hosts and servers, the analyst conducted internet-level scanning and analysis.

From Zone: Internet
Via: N/A
To Zone: External Network
Method: Internet penetration testing

Current Zone Activities:

xxx.xxx.93.188
The server's certificate is not valid for the hostname.
Cert is issued to www.examplecom, www.example.com, but you can reach the https certificate through this IP address. The hostname is technically not covered by the cert.

HSTS is not enforced
The application fails to prevent users from connecting to it over unencrypted connections. This opens the possibility of man-in-the-middle attacks performed on the site by users who visit unencrypted links. To remedy this, add a response header with the name "Strict-Transport-Security" with an acceptable max-age expiration time.

Nmap Warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
Broken cipher RC4 is deprecated by RFC 7465
Ciphersuite uses MD5 for message integrity
Key exchange (dh 2048) of lower strength than certificate key
Key exchange (ecdh_x25519) of lower strength than certificate key


התמונה
לא נבדקת
לפי הגדרותיך

xxx.xxx.11.67

The server's certificate is not valid for the hostname.

Cert is issued to mail.example.com, but you can reach the https certificate through this IP address. The hostname is technically not covered by the cert.

Nmap Warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
Broken cipher RC4 is deprecated by RFC 7465
Ciphersuite uses MD5 for message integrity
Key exchange (dh 1024) of lower strength than certificate key

xxx.xxx.11.82

HSTS is not enforced.
The application fails to prevent users from connecting to it over unencrypted connections. This opens the possibility of man-in-the-middle attacks performed on the site by users who visit unencrypted links. To remedy this, add a response header with the name "Strict-Transport-Security" with an acceptable max-age expiration time.

Nmap Warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
Broken cipher RC4 is deprecated by RFC 7465
Ciphersuite uses MD5 for message integrity
Key exchange (dh 1024) of lower strength than certificate key
Key exchange (secp256r1) of lower strength than certificate key

xxx.xxx.119.235

Nmap Warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
64-bit block cipher IDEA vulnerable to SWEET32 attack
Key exchange (secp256r1) of lower strength than certificate key

התמונה
לא נבדקת
לפי הגדרותיך

xxx.xxx.11.66

The server's certificate is not valid for the hostname.
Cert is issued to 192.168.168.168, but you can reach the https certificate through this IP address. The hostname is technically not covered by the cert.

HSTS is not enforced.
The application fails to prevent users from connecting to it over unencrypted connections. This opens the possibility of man-in-the-middle attacks performed on the site by users who visit unencrypted links. To remedy this, add a response header with the name "Strict-Transport-Security" with an acceptable max-age expiration time.

xxx.xxx.91.182

The server's certificate is not valid for the hostname.
Cert is issued to web.example.com, www.web.example.com, but you can reach the https certificate through this IP address. The hostname is technically not covered by the cert.

HSTS is not enforced.
The application fails to prevent users from connecting to it over unencrypted connections. This opens the possibility of man-in-the-middle attacks performed on the site by users who visit unencrypted links. To remedy this, add a response header with the name "Strict-Transport-Security" with an acceptable max-age expiration time.

xxx.xxx.167.106

HSTS is not enforced.
The application fails to prevent users from connecting to it over unencrypted connections. This opens the possibility of man-in-the-middle attacks performed on the site by users who visit unencrypted links. To remedy this, add a response header with the name "Strict-Transport-Security" with an acceptable max-age expiration time.

Cookie missing HttpOnly
The XSRF-TOKEN Cookie, if this site is indeed intending to use it as some form of CSRF Prevention, should be set to HttpOnly that way it cannot be read or modified by client-side JavaScript

4.3 Actions taken

To determine and practically demonstrate the feasibility of gaining physical access to facilities Non-Public and High-Security zones or gaining of unauthorized, authenticated access to CLIENT's workstations, the ISA conducted the following activities:

From Zone: External communications
Via: N/A
To Zone: Internal network
Nexus Point: Frontline staff members
Method: **Telephone-based pretexting**

Current Zone Activities:

PurpleSec's Social Engineer performed phone-based social engineering with the goal of getting credentials and have staff perform tasks on their workstation. This is intended to simulate a malicious actor attempting to gain credentials and a foothold in the environment by a phone call.

10 phone contacts were made with 3 Full Breach's with multiple (6) passwords given to the Social Engineer. One contact stated most of the systems use the same password for everyone.

Nexus Point Activities:

PurpleSec's Social Engineer called the numbers over a three-day period and spoke with CLIENT staff members. Each time a live staff member was reached, the Social Engineer claimed to be a technical support worker authorized to contact CLIENT's personnel to provide critical support. If challenged, the Social Engineer would then drop Information Security Staff member names in a statement that they are working on their behalf. The Social Engineer's program included the following activities:

- Requesting that the user provide his/her domain username.
- Feigning an attempt to perform a technical operation on the user's behalf, and then requested that the user provide his/her domain password when the operation 'failed.'

Three of the personnel engaged by the Social Engineer provided domain usernames or passwords. The passwords revealed were eight characters long with only alphanumeric characters. Cloud-based servers may be able to break these passwords within a manner of weeks or days depending on the resources allocated to password cracking efforts. PurpleSec recommends increased complexity and

length. Risk Rating: MEDIUM

Bottom Line: It was found to be feasible to induce Example's users to provide logon information through deceptive telephone communications.

Recommendations:

- Conduct Social Engineering Training to help staff properly validate the identity of the phone callers and do not provide confidential credential information.
- Ensure procedures have employees report unusual or suspicious phone calls to appropriate staff.
- Change password requirements to at least 10 complex characters, including alpha-numeric and special characters.

***4.4** Current Zone Activities:*

PurpleSec's Social Engineer worked with staff to compile 175 email addresses to perform the social engineering test. A phishing template with appropriate signage and logos was created.

Nexus Point Activities:

PurpleSec's Social Engineer sent a phishing e-mail to all the in-scope addresses. The e-mail originated from a spurious IT support company and claimed to be a legitimate technical support request authorized by CLIENT's IT Department. The e-mail also requested that the user navigate to an PurpleSec-controlled Website and:

- Provide his/her domain username,
- Provide his/her e-mail address (in lieu of password), and
- Download a benign executable file,
- Run the executable locally on his/her workstation.

Of the 175 email addresses tested, 13 users interacted with untrusted content (hyperlink) and 9 provided domain usernames/e-mail address.

Figure 3.49 – Screenshot showing the email phishing results.

Risk Rating: Medium

Bottom Line: The response and click rates for CLIENT's staff tested via email are just under 10% and should be considered a vulnerability for the organization. It should be noted that most malware needs only a single response, and full response from a user to username/password requests may lead to significant breaches.

Recommendations:

- While click and interaction rates were calculated as Medium it is highly recommended that CLIENT engage in Cybersecurity awareness training immediately.

5.0 Conclusions

5.1 Most Likely Compromise Scenarios

An attacker would most likely start an attack against CLEINT with social engineering techniques. (this is the most successful type of attack) and given that ETERNALBLUE is easily exploited, this is the most likely compromise of the entire system. Attacking the McAfee Security Server would be an ideal first target; once an attacker has attained root access to this system, they can disable all the security controls and systems in place, allowing for much more evasive traversal of the internal network, as well as potentially creating more targets without the hindrance of the security systems.

From here, the ideal goals of an attacker would be data exfiltration of ePHI, Personally Identifiable Information (PII) and PCI data - for purposes of fraud, ransom, targeted phishing, sale, etc. - and any payment information that may be available for similar purposes. An adversary would attempt to access to the Domain Controllers to help facilitate network traversal and further compromise of security controls and monitoring systems. With Domain access, complete infrastructure compromise is likely; with this level of access an attacker presents numerous serious security risks to critical and confidential information systems.

Internet facing assets at CLIENT have little to no interactivity and so pose less of a threat to intrusion through these systems. However, the systems are vulnerable to Man-in-the-middle (MITM) type attacks which could be utilized by an attacker to gain access to private communications and potentially steal passwords to gain further access into the network.

5.2 Implications

Based on the above testing activities, the average risk level across the board is EXTREME

Complete system compromise is trivially achieved on critical security and file servers, systems that contain myriad important and confidential files which, if breached, can put CLIENT at great risk to large fines and significant business impact.

Disable SMB on any system that does not require it for business functionality. Even with recent patches, Windows systems using SMB remain vulnerable to ETERNALBLUE type exploits so long as the service is running.

System hardening needs to be implemented immediately to shrink the risk landscape of the infrastructure. Controls and configurations should be centrally managed; management and security systems such as the McAfee server should be secured using

controls designed around Least Privilege and Critical Infrastructure NIST recommendations. Compromise of these systems pose a critical threat.

Implement system patching management cycle to ensure that all systems are regularly receiving important security updates from vendors.

Revoke or replace PFX files in user profiles as a precaution

Data compliance and end user social engineering training should be implemented to promote safer practices. HIPAA data should be contained to ONLY systems that require access to the data; it is encouraged that these systems employ good data at rest encryption and least privilege access controls to prevent unauthorized access. Best practice is to centrally store these types of files on a managed, hardened network location, users should access the files only via network connectors in their in profiles with configured security permissions.

References

Open Web Application Security Project (OWASP). (2014). *Testing Guide v4.0*. https://www.owasp.org/images/1/19/OTGv4.pdf

Assured Compliance Technology. (2015a). *Information Security Project Quality Assurance Manual v1.4*. ACT Policy Library.

Assured Compliance Technology. (2015b). *Information Security Penetration Testing Method*. ACT Policy Library.