[Client Logo]

[Year]

By:

[Consulting Company]

[Month Day, Year]

[Client Name]

ATTACK AND PENETRATION TEST

REPORT

[1. INTRODUCTION 2](#_Toc124312611)

[**Report structure** 2](#_Toc124312612)

[2. EXECUTIVE SUMMARY 3](#_Toc124312613)

[**Scope and objectives of work performed** 3](#_Toc124312614)

[**Assessment summary** 4](#_Toc124312615)

[**High-level Significant Technical Findings** 6](#_Toc124312616)

[**Strategic Recommendations** 7](#_Toc124312617)

[3. METHODOLOGY 8](#_Toc124312618)

[**Reconnaissance** 9](#_Toc124312619)

[**Target Development** 9](#_Toc124312620)

[**Intrusion** 9](#_Toc124312621)

[**Lateral Movement** 9](#_Toc124312622)

[**Data Exfiltration** 9](#_Toc124312623)

[4. TECHNICAL DETAILS 11](#_Toc124312624)

# **INTRODUCTION**

## **Report structure**

The report is structured as follows:

**Executive Summary:** This section contains information about the assessment, what assets were tested, and a high-level summary of findings and recommendations for remedial action.

**Methodology:** This section provides a brief overview of the methodology typically used to simulate this type of assessment.

**Technical Findings:** Contains the technical descriptions of the findings and any associated risks [Client] (“[Client]”) technical team may wish to consider when remediating. This section highlights evidence collected during the tests and proposes steps or activities required to resolve the issues outlined.

# **EXECUTIVE SUMMARY**

## **Scope and objectives of work performed**

[Client] engaged [Consulting Company] (the “Consultants”) to execute Attack and Penetration tests against its network infrastructure, both external and internal. The test’s objectives were to identify attack vectors that a threat actor (e.g. an employee, or malicious actors) could leverage to gain unauthorized access to sensitive [Client] data or systems.

Our consulting team employed the concept of “*path of least resistance*” methodology to execute these tests, which focused on attempting to access [Client]’s resources by exploiting identified security weaknesses, which would provide the least resistance to a threat actor.

Importantly, these tests did not, nor were they intended to, identify all the potential vulnerabilities on all systems within the networks.

|  |  |
| --- | --- |
| **Project Title** | **Attack and Penetration Tests [Year]** |
| **Project Objective** | * Identify and exploit attack vectors a threat actor could leverage to compromise the external network perimeters of [Client] to gain unauthorized access to [Client]’s network assets. * Identify and exploit attack vectors an insider threat actor (e.g., Employees, or malicious actors) could leverage to compromise internal network systems of [Client] to gain unauthorized access to [Client]’s critical assets. * Determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs, crown jewels, etc. |
| **Test Scenario** | * External penetration test against [Client]’s external network infrastructure. * Internal penetration test against internal and critical systems from the perspective of the internal threat actor. |
| **In-Scope Assets** | External Networks  1.2.3.0/24  Internal Networks  1.2.3.0/24 |
| **Testing Date** | * [Month Day, Year – Month Day, Year] |
| **Consultants** | * [Consultant Name] * [Consultant Name] |

## **Assessment summary**

Throughout this report, certain notations are used to articulate the severity of the findings identified. This severity level takes into consideration the following factors:

* Likelihood of a vulnerability or an attack vector being exploited or abused
* Ease of exploitation or abuse
* Resulting level of access to the host and the network
* Impact on business

Ratings have been assessed by the Consultants and should be used as a guide to understand the priority to carry out any remedial actions. However, individual risk ratings should be reviewed in line with [Client]’s knowledge of the technical environment and with the business context of the systems being reviewed. This may result in [Client] assigning different severity levels to the ones highlighted in the report. A guide to the scoring and examples of vulnerabilities that fall into certain scores can be found below:

|  |  |
| --- | --- |
| Risk | |
| *Score* | *Description* |
| ***High*** | The threat actor would gain full control over the system or application (e.g., administrative, root or enable access). This would also relate to attacks that would render the system or its data unusable, irreparably damage the company’s reputation, or extract highly sensitive information that, if made public could cause considerable damage the company. |
| ***Medium*** | Medium risk vulnerabilities relate to findings that would not lead to a direct compromise of the system or data but could be used to gain further access. Exposure could impact business systems and business operations could experience a reduction in performance. These would often be used in a chained attack to obtain access to a resource or network. |
| ***Low*** | This would relate to findings such as information leakage, i.e., a threat actor being able to gather usernames, internal IP address information, technologies in use, or other potentially sensitive data. Exposure should not impact business operations, however, should be addressed to meet expected business operation. |

## **High-level Significant Technical Findings**

1. **Exploitation of Remote Software**   
   Exploiting vulnerable software has been a common attack path for adversaries for a long time. Exploitation of remote software can provide full control of the vulnerable systems and can often lead to additional access based on the compromise. Our consultants discovered several Windows Operating systems vulnerable to issues such as MS17-010, CVE-2021-42278 and CVE-2021-42287.

**Potential impact on [Client]:**

Exploitation of remote software can provide full control of the vulnerable systems and can often lead to additional access based on the compromise. An adversary who successfully exploits these vulnerabilities could run arbitrary code with SYSTEM privileges.

1. **Weak Password Use**  
   Most corporate environments use Microsoft’s Active Directory to manage employee accounts and access. One problem with Active Directory is that it does not allow for comprehensive password complexity requirements. In essence, it does not restrict users from choosing weak passwords, requiring passwords to meet the specific length and contain specific characters sets. However, it takes only one weak password for a threat actor to breach an organization’s network. In this case, the Consultants captured a password hash of an employee and successfully cracked the password because the password was weak and easy to crack. With a valid set of credentials, the Consultants were able to execute further attacks to compromise systems on the network.

**Potential impact on [Client]:**

Passwords are integral part of the overall security and the first line of defense against unauthorized access to organization’s network resources, as such, when employees use easily guessed passwords, it provides opportunities for unauthorized users such as threat actors to gain access to confidential data. Weak login credentials, including weak passwords, are among the top causes of data breaches within organizations. A threat actor needs only one working set of credentials to establish a foothold into an organization’s network and further exploit internal systems.

## **Strategic Recommendations**

While the recommendations in the “Technical Findings" section primarily focus on technical remediation steps, the recommendations in this section also consider managerial and operational controls that may be helpful in addressing the possible root-causes behind the findings of this assessment and/or to improve security-monitoring controls to identify malicious activities.

1. **Maintain Proper IT Hygiene**

Eliminate vulnerabilities such as outdated or unpatched systems and software that may be lurking in your network environment. Exploits can remain hidden for long periods of time before becoming active, and organizations will be exposed if they fail to apply patches and updates across all of their endpoints. Management should implement a patch management program to effectively and efficiently apply patches to systems organization-wide in a risk-prioritized methodology. This ensures low-hanging vulnerabilities are addressed on time.

1. **Password Management**

Management should implement a periodic password audit to ensure password leading practices, such as password complexity, are implemented and enforced organization wide.

1. **Event Monitoring and Endpoint Security Solution**

Many high-profile attacks occur over months of dwell time and move laterally to easily evade standard security. Modern attackers count on the fact that many organizations continue to rely on legacy or standard security solutions, which are easily bypassed by modern hacking tools. Management should upgrade to comprehensive technology such as Endpoint Detection and Response (EDR) solution for detecting and blocking attacks.

# **METHODOLOGY**

The Consultants used an adaptive approach in executing the attack and penetration tests, similar to how advanced threat actors use to operate. Below is the overview of the methodology used for the penetration tests:

Adaptive Penetration Test Methodology

Reconnaissance

Target Development

Intrusion

Lateral Movement

Data Exfiltration

## **Reconnaissance**

Reconnaissance is typically the initial phase of most cyber-attacks and during this phase, the Consultants acquire strategic information about the target Client’s IT environment and organizational structure. To ensure the activities are blended within normal user activities, the Consultants uses built-in utilities and specialized tools to carry such activities. Some of the outcomes from this phase may include the domain names, hostnames, domain users, domain groups, IP addresses, subnets, etc.

## **Target Development**

Using the information gathered from the Reconnaissance activities, the Consultants begin the process of exploring the information to develop a list of targets to attack. The outcome of this phase provides the Consultants with a list of potential targets that would provide the Consultants with entry points on the network.

## **Intrusion**

This phase of the attacks is where the Consultants begin to interact with the targets from the Target Development phase, in attempts to gain access to them. This phase involves cyclical iteration of tactical and strategic attack techniques as the Consultants try different Tactics, Techniques and Procedures (TTPs) to compromise targets.

## **Lateral Movement**

Once the Consultants have gained access to a target, the Consultants try to stay “low and slow” to avoid detection by the target’s defenses from the internal network. The Consultants then map the organization’s internal network infrastructure and creates a battle plan and deploy multiple parallel kill chains to laterally move within the internal network for further attacks. Some of the TTPs the Consultants employ at this stage include privilege escalation (if or when necessary) to ensure the Consultants can execute certain tasks on the network with less restrictions. The Consultants use techniques such as credential harvesting and re-use, Pass-the-Hash, systems misconfigurations, and network service abuse to gain access to key target resources.

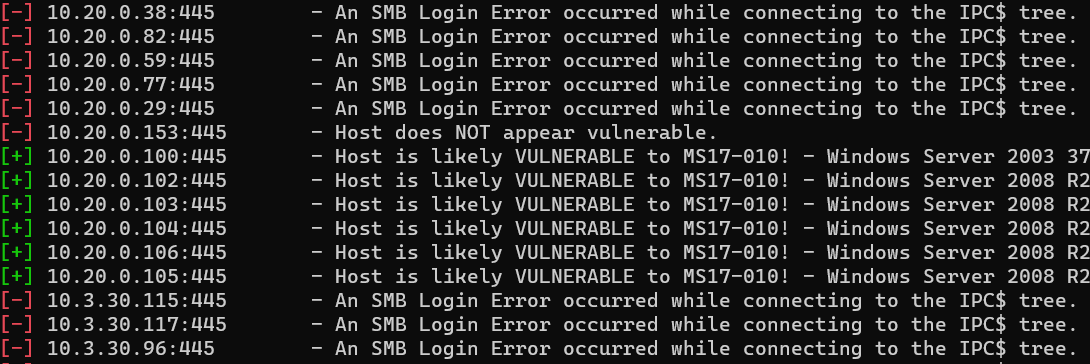
## **Data Exfiltration**

The goal of most cyber-attack threat actors is access to their target’s sensitive data (“the crown jewels”). The threat actor often needs or wants a copy of this information to work with for variety of reasons (e.g. personal financial gains, political gains, social reasons, etc.). Data Exfiltration is how this information is moved from the company to systems under the threat actor’s control.

# **TECHNICAL DETAILS**

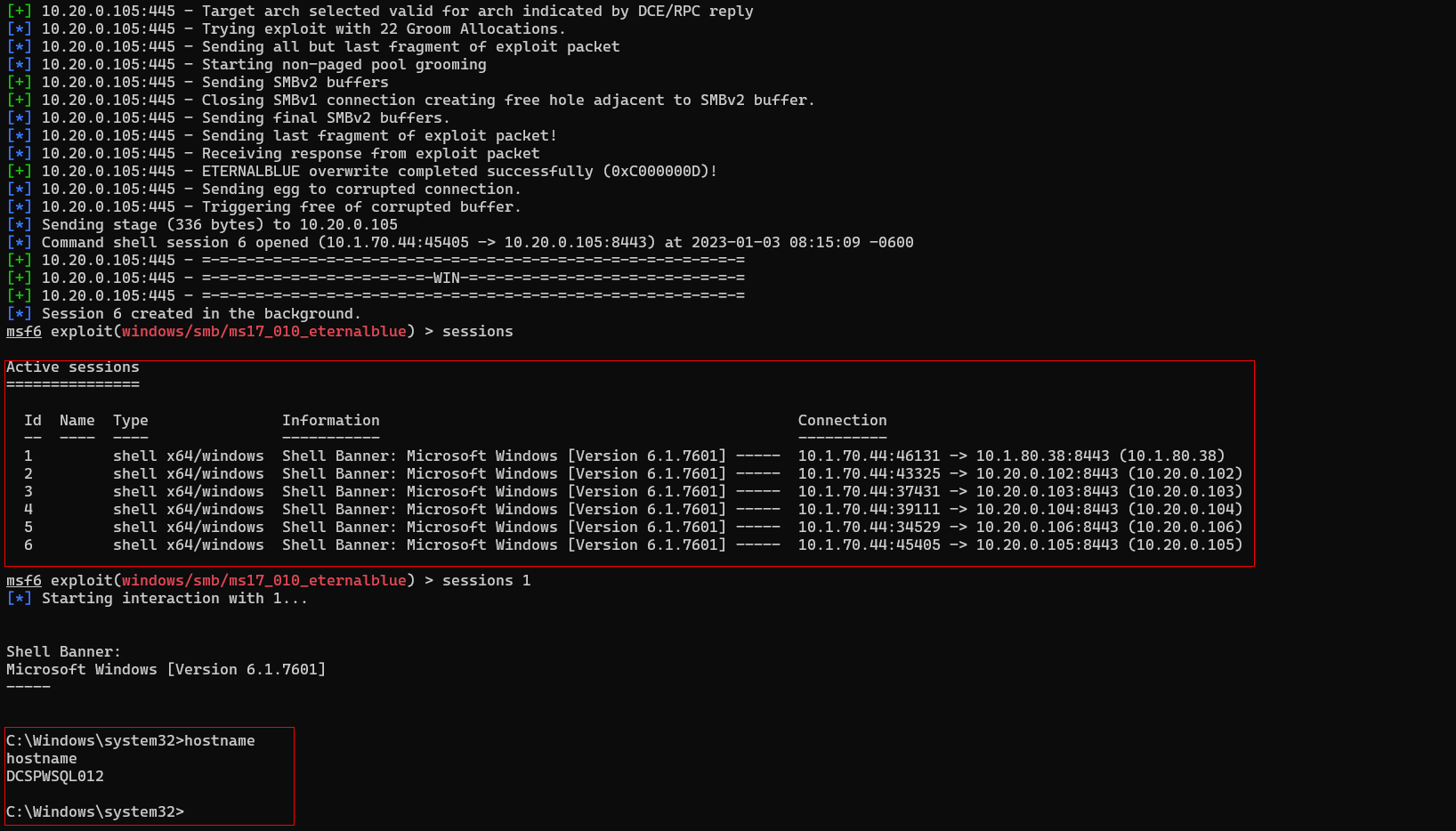
|  |  |  |
| --- | --- | --- |
| ***[Vulnerability Name]*** | | |
|  | *Risk Rating:* | ***High*** |
| *MITRE ATT&CK TTP* | ***Exploitation of Remote Software (T1210)*** |
| **Description and risks:** | | |
| The Consultants identified several Windows Operating systems that are vulnerable to the Microsoft Security Bulletin MS17-010, known as the EternalBlue vulnerability. This vulnerability impacts Microsoft Windows Server Message Block (SMB) version 1 flaws, with a successful exploiting leading to a remote code execution.  **Impact on [Client]:** An adversary who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges. The adversary can also leverage this vulnerability to gain access to the system. | | |
| **Remediation and further information:** | | |
| * Apply the patches as instructed by Microsoft, referenced under the **References** section. | | |
| **References:** | | |
| * https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010 | | |
| **Affected Asset:** | | |
| * 1.2.3.4 | | |
| **Reproduction/Proof of Concept:** | | |

Using both *nmap* and the *Metasploit* framework, the Consultants identified the systems vulnerable to the EternalBlue vulnerability.

**

*Figure 01 – Sample systems vulnerable to MS17-010*

In the screenshot below, a system has been compromised by the Consultants and able to directly access the system:



*Figure 02 – An exploited system with Metasploit*