HACKPICK

Demo Company
Security Assessment Findings Report

Business Confidential

Date: December 21 , 2020
Project: 2020-0777 Version 1.0

Copyright © HackPick, sp. z o.o. sp.k

Table of Contents

Copyright © HackPick, sp. z o.o. sp.k

Copyright © HackPick, sp. z o.o. sp.k

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and HackPick (HPS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and HPS.

DC may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. HPS prioritized the assessment to identify the weakest security controls an attacker would exploit. HPS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

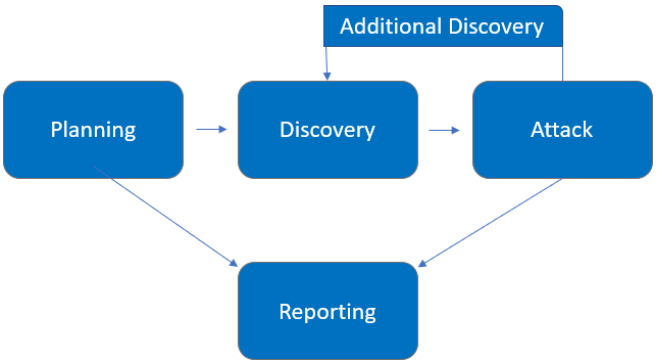
Name	Title	Contact Information
Demo Company		
John Doe	DevOps Engineer	Office: (555) 555-5555 Email: jdoe@democo.com
HackPick, Inc.		
TomaszSmialek	Lead Penetration Tester	Office: (555) 555-5555 Email: tom@hackpick.re

Copyright © HackPick, sp. z o.o. sp.k

Assessment Overview

From December 5, 2020 to December 16 , 2020 , DC engaged HPS to evaluate the security posture of its infrastructure compared to current industry best practices that included external , internal, and web application penetration tests. 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 the following:

- Planning –Customer goals are gathered and rules of engagement obtained.
- Discovery– Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting– Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A HPS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Copyright © HackPick, sp. z o.o. sp.k

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Web Application Penetration Test

A web application penetration test is an in-depth penetration test on both the unauthenticated and authenticated portions of your application. The engineer will test for OWASP Top-10 critical security flaws along with a variety of other potential vulnerabilities based on security best practice. Activities include site mapping and enumeration, automated and manual injection testing, directory traversal testing, malicious file uploads, remote code execution, password attacks and authentication bypasses, session attacks, and other testing depending on specific site content and languages.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess 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.

Copyright © HackPick, sp. z o.o. sp.k

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
External Penetration Test	1.2.1.2/29 – Office IP 1.2.3.1 – Azure Firewall/VPN
Internal Penetration Test	10.64.0.0/24 – Network/Firewall 10.64.2.0/24 – Main subnet 10.64.3.0/24 – VoIPs 192.168.17.0/24 – Guest WiFi
Web Application Penetration Test	https://compromised.com

Scope Exclusions

Per client request, HPS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by DC.

Client Allowances

DC provided HPS the following allowances:

- Internal network access for HPS laptop

Copyright © HackPick, sp. z o.o. sp.k

Executive Summary

HPS evaluated DC's external, internal, and web application security posture through penetration testing from December 5th, 2020 to December 16th, 2020. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Testing Summary

HPS evaluated DC's external network from December 5th, 2020 to December 6th, 2020. The assessment began with vulnerability scanning to identify any potential vulnerabilities on the external surface. Vulnerability scanning did not identify any significant vulnerabilities and triggered alerting by the FortiNet VPN. HPS also searched for historical breached accounts related to DC and found one account involved in a prior breach. This account did not lead to any access during testing. HPS also identified valid email addresses through Office 365 enumeration and attempted password spraying attacks with commonly used passwords, such as "Winter2020!". These attacks were unsuccessful. Overall, HPS found DC's external network to be well-patched, the password policy to be very strong, and noted Multi-Factor Authentication (MFA) on logins.

HPS evaluated DC's internal network from December 7th, 2020 to August 11th, 2020. Vulnerability scanning identified two potential critical patching issues, but neither could be exploited by the tester. Recommendations have been made for patching but have been marked moderate due to the vulnerability not being successfully exploited. HPS attempted common internal network attacks, including LLMNR/NBT-NS poisoning, IPv6 and ARP spoofing, password spraying and credential stuffing, and checking for default credentials. HPS was able to recover two NTLMv2 hashes during LLMNR/NBT-NS poisoning but was unable to crack the hashes due to a strong password policy. HPS was able to recover valid credentials to a webmaster account and phone system via ARP spoofing, but neither account was able to be leveraged for lateral movement in the network. Overall, HPS was unable to compromise the domain and found DC's internal network to have strong password policies and a limited attack surface.

HPS evaluated DC's web application from December 12th, 2020 to December 17th, 2019. The assessment included vulnerability scanning and active testing on the unauthenticated, low-level, and admin users. Methodology strictly followed the OWASP testing guidelines and framework, which allowed for thorough discovery of vulnerabilities. During the assessment, the tester discovered potential issues with session fixation, user enumeration, and denial of service. HPS also discovered several low finding issues related to web application security best practice. It is important to note that these issues did not result in account takeover or remote code execution. Overall, HPS found the application to be well developed and limiting of critical attacks.

Copyright © HackPick, sp. z o.o. sp.k

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted HPS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the HPS engineer's attacker IP address within minutes of scanning and was capable of blacklisting HPS from further scanning actions. SIEM alerts occurred on both the external and internal penetration testing. It should be noted that while the SIEM alerted, some attacks went undetected, signaling that the SIEM can be improved. These attacks have been noted in the technical findings.

Multi-Factor Authentication

HPS noted several instances of Multi-Factor Authentication (MFA) implemented at DC, including the web application and Office 365 webmail. This is a cybersecurity best practice and helps prevent attackers from gaining access, even with valid credentials.

Strong Password Policy

DC utilizes a 12-character password minimum on the web application. This policy falls in line with best practice guidelines. DC also utilizes a strong password policy on Active Directory/domain accounts. HPS security was unable to gain access to any accounts through hash cracking attempts, which signifies strong passwords.

Security Weaknesses

Session Fixation

The web application generates a session ID when a user visits the page. When a user logs in, the session ID should change, but it does not, causing session fixation. The session ID, if hijacked, can be used to act as the user as long as the cookie is valid. HPS also noted that logging out terminated the session, but the session ID stayed the same after a second login. Ideally, the session ID should be destroyed on log out.

Potential Denial-of-Service

The web application provides username enumeration when supplying an incorrect username. The application also performs account lockouts after 5 failed attempts. A malicious attacker could use the usernames gleaned through enumeration to deny service with the failed login attempts and disrupt DC's business activity.

Copyright © HackPick, sp. z o.o. sp.k

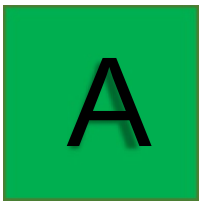
Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations as well as a report card grade compared to companies of similar size and infrastructure:

Network Penetration Test Findings

0	0	4	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Network Penetration Test		
NPT-001: Insufficient Patching – MS17-010 - EternalBlue	Moderate	Apply vendor patches.
NPT-002: Insufficient LLMNR Configuration	Moderate	Disable multicast name resolution via GPO.
NPT-003: Insufficient Hardening – SMB Signing Disabled	Moderate	Enable SMB signing on all network devices.
NPT-004: Insufficient SNMP Community String Complexity	Moderate	Utilize complex community strings.
NPT-005: Insufficient Patching – Microsoft TFTP Server	Low	Apply vendor patches.
NPT-006: Insecure Protocol - IMAP	Low	Utilize IMAP on port 993 for encrypted connections.
NPT-007: Undetected Malicious Activity	Low	Review SIEM strategy for internal network.
NPT-008: Historical Account Compromises	Informational	Train users on password reuse between sites.



Final Network Grade

Copyright © HackPick, sp. z o.o. sp.k

Web Application Penetration Test Findings

0	2	0	6	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Network Penetration Test		
WAPT-001: Session Fixation	High	Ensure SessionIds regenerate at authentication.
WAPT-002: User Enumeration & Account Lockout – Denial of Service	High	Enforce synchronized error messages and implement CAPTCHAs on login pages.
WAPT-003: Insufficient Encryption – Depreciated Ciphers	Low	Disable deprecated TLS encryption ciphers.
WAPT-004: Information Disclosure vi HTTP Response Headers	Low	Remove unnecessary information from HTTP response headers.
WAPT-005: Verbose Error Messages	Low	Disable verbose error messages in the IIS server configuration.
WAPT-006: Login Form Autocomplet Enabled	Low	Disable autocomplete on sensitive form input fields.
WAPT-007: Insecure HTTP Respons Headers	Low	Add security related response headers.
WAPT-008: Undetected Malicious Activity	Low	Review SIEM and WAF strategy for web application.

B+

Final Web Application Grade

Copyright © HackPick, sp. z o.o. sp.k

Technical Findings

Network Penetration Test Findings

Finding NPT-001: Insufficient Patching – MS17-010 - EternalBlue (Moderate)

Description:	DC permitted an unpatched system on the internal network that is vulnerable to MS17-010 (EternalBlue). HPS confirmed that the vulnerability likely exists but was unable to exploit it due to no SMB pipes being open on the system. The vulnerability still exists and is exploitable with any valid credentials.
Risk:	Likelihood: Moderate – Malicious actors have used SMB exploitations like EternalBlue in recent breaches. However, due to limited pipes, valid user credentials must be present in order to exploit. Impact: High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.64.2.12
Tools Used:	Nessus, Metasploit, AutoBlue
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

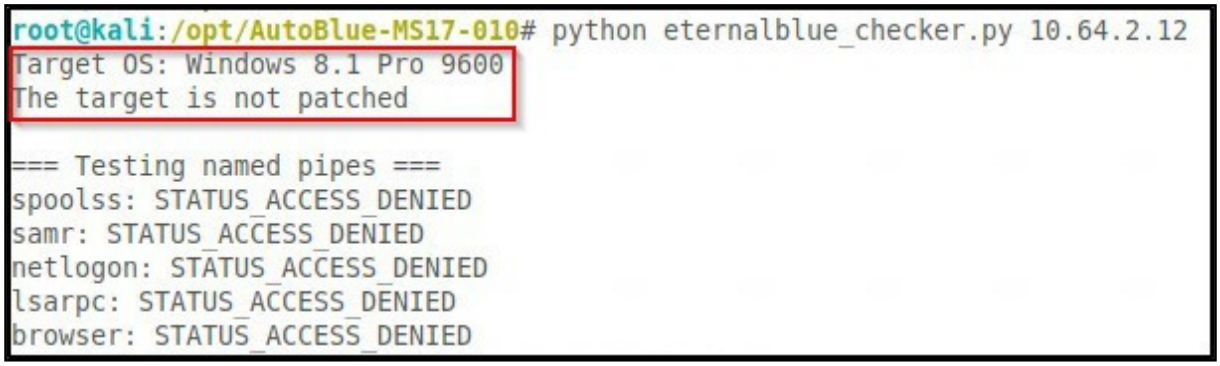


Figure 1: Unpatched MS17-010

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS17-010 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-002: Insufficient LLMNR Configuration (Moderate)

Description:	DC allows multicast name resolution on their end-user networks. HPS captured 2 user account hashes by poisoning LLMNR traffic, but was unable to crack either hash, signifying a strong domain password policy.
Risk:	Likelihood: Moderate – This attack is effective in environments allowing multicast name resolution. Impact: Very High – LLMNR poisoning permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
Tools Used:	Responder
References:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidence

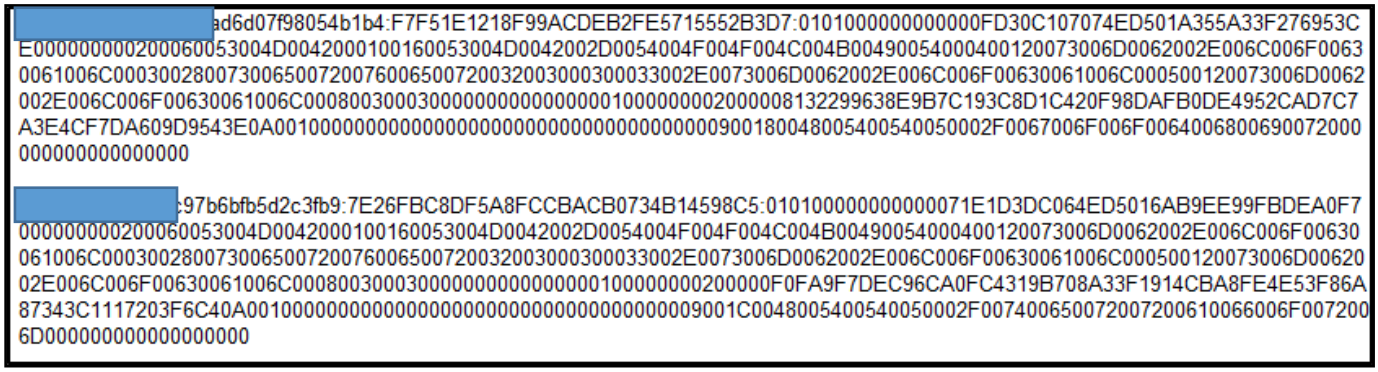


Figure 2: NTLMv2 hashes captured via LLMNR poisoning

Remediation

Disable multicast name resolution via GPO. If DC requires the use of multicast name resolution, Network Access Control (NAC) combined with application whitelisting can prevent these attacks.

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-003: Insufficient Hardening – SMB Signing Disabled (Moderate)

Description:	DC failed to implement SMB signing on 2 machines. Failing to implement SMB signing could lead to SMB relay attacks, yielding system-level shells without requiring a user password.
Risk:	Likelihood: Moderate – Relaying password hashes is a basic technique not requiring offline cracking. Due to DC having a small employee base and low LLMNR attack capabilities, the likelihood is less than most organizations in a similar situation. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	10.64.2.12 10.64.2.201
Tools Used:	Nessus, Nmap, MultiRelay, Responder
References:	CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Evidence

```
root@kali:~# nmap -p445 10.64.2.12 --script smb-security-mode.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 20:09 EDT
Nmap scan report for 10.64.2.12
Host is up (0.0032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 44:39:C4:5A:CA:F4 (Universal Global Scientific Industrial)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Figure 3: SMB signing disabled

Remediation

HPSrecommends that DC enable SMB signing on all network devices that use SMB.

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-004: Insufficient SNMP Community String Complexity (Moderate)

Description:	DC deployed SNMP with default “public” community strings. This configuration exposed read-only access to the system’s management information base (MIB), including the network configurations.
Risk:	Likelihood: High – Basic network scans will identify this vulnerability Impact: Moderate – If exploited, an attacker can profile the device and focus attacks
System:	10.64.0.2
Tools Used:	Nessus, SNMP-Check
References:	NIST SP800-53 r4 AC-17(2) - Remote Access Protection of Confidentiality/Integrity using Encryption

Evidence

```
[+] Try to connect to 10.64.0.2:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.64.0.2
  Hostname                      : HP-2530-48G-PoEP
  Description                   : HP J9772A 2530-48G-PoEP Switch, revision YA.16.05
.0008, ROM YA.15.20 (/ws/swbuildm/rel_venice_qt3_qaoff/code/build/lakes(swbuildm_re
l_venice_qt3_qaoff_rel_venice_qt3)) (Formerly ProCurve)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : -
  Uptime system                 : 2 days, 22:08:24.23
  System date                   : -

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 64
  TCP segments received         : 40101
  TCP segments sent             : 35849
  TCP segments retrans          : 0
  Input datagrams               : 87459
  Delivered datagrams           : 40773
  Output datagrams              : 38067
```

Figure 4: Information disclosure via public SNMP community strings

Remediation

HPS recommends DC consider the following corrective actions:

- Disabled SNMP if not required
- Filter UDP packets going to port UDP 161
- Evaluate migration to SNMPv3
- Use password complexity guidelines for community strings

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-005: Insufficient Patching – Microsoft TFTP Server (Low)

Description:	DC permitted an unpatched Microsoft TFTP server on the internal network that is vulnerable to remote code execution. HPS confirmed that the vulnerability likely exists but was unable to exploit it due to there being no current known exploits.
Risk:	Likelihood: Low – The vulnerability exists per Microsoft, but there have yet to been exploit proof of concepts developed Impact: High – If exploited, an attacker can gain full remote code execution on a system
System:	10.64.2.201
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
tftp> status
Connected to 10.64.2.201.
Mode: octet Verbose: off Tracing: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
```

Figure 5: Validation of TFTP Server

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching CVE 2019-0603 can be found here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-006: Insecure Protocol – IMAP (Low)

Description:	DC permitted IMAP on port 143, which is not encrypted. HPS intercepted the IMAP traffic and gained access to e-mail credentials. The credentials found allowed access to the Street EMR webmaster account and the VCS754 conference phone due to password reuse.
Risk:	Likelihood: Low – The vulnerability requires an attacker to be inside the network to be successful. Impact: Moderate – The attacked permitted access to webmail and business phones, which could have led to Denial of Service to those accounts.
Tools Used:	Ettercap
References:	https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/

Evidence

Figure 6: Captured e-mail credentials

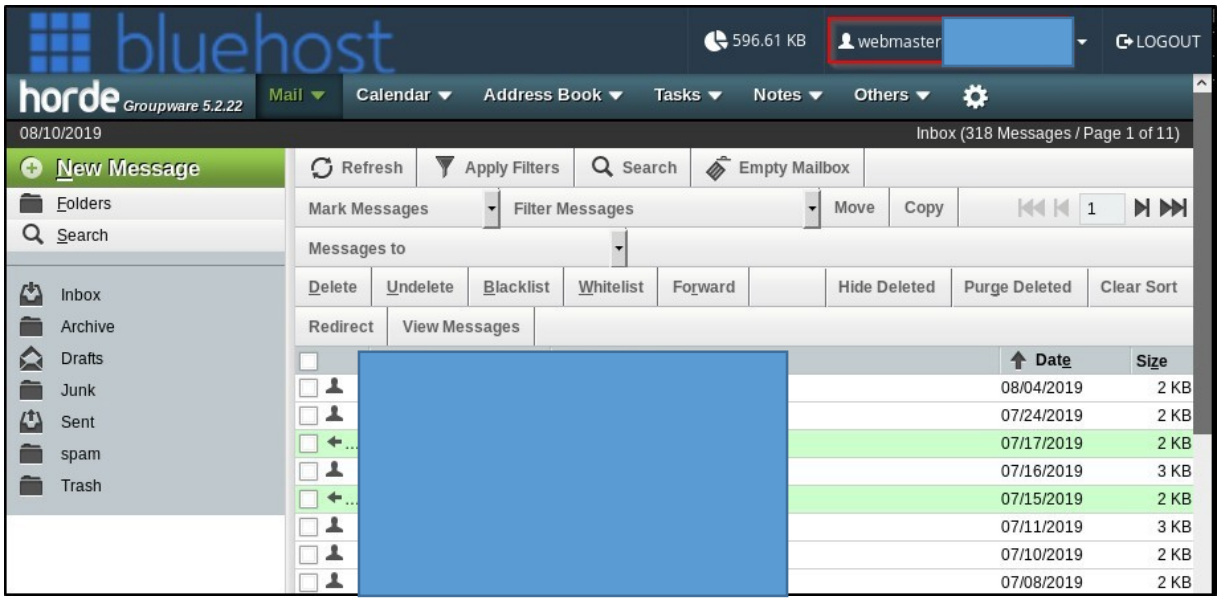


Figure 7: Captured e-mail credentials

Remediation

Utilize IMAP on port 993 for encrypted connections. Avoid password reuse and use complex passwords without the company name added.

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-007: Undetected Malicious Activity (Low)

Description:	DC failed to detect some malicious activity on the network. On the external network, DC performed well with the main office IP detecting any malicious activity against the FortiNet VPN. On the internal network, some malicious activity was detected due to Nessus scanning. However, attacks such as man-in-the-middle, brute force attacks, and direct host vulnerability scans went undetected.
Risk:	Likelihood: Low – These activities occur after primary controls fail. Impact: Moderate – Undetected network attacks allow adversaries to expand control.

Remediation

Review SIEM strategy for the internal network. Combine network and host-based monitoring together to provide the most protection. Some attacks may be difficult to detect but have been noted for information and review.

Attacks Undetected

- Host vulnerability scans with Nmap
- IPv6 poisoning
- ARP poisoning
- LLMNR/NBT-NS poisoning
- Brute force attacks against SMB/LDAPS

Copyright © HackPick, sp. z o.o. sp.k

Finding NPT-008: Historical Account Compromises (Informational)

Description:	HPSidentified one DC account compromised in published breaches. The account identified did not authenticate into the DCenvironment.
Risk:	Likelihood: High – These data sources are publicly available. Impact: High – Previously compromised accounts permit attackers to launch targeted attacks using known credentials. End users recycle passwords with slight variations, making these attacks effective.
Tools Used:	Published breach data
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

Figure 8: Account credentials from previous breach dumps

Remediation

Train users to avoid password reuse between sites. Additionally, train users to not use work e-mails for site registrations unless necessary. Lastly, enforcing password rotation with strict password complexity requirements will limit the effectiveness of attacks. HPS recommends a ‘ haveibeenpwned.com’ subscription for proactive alerting of compromised corporate accounts.

Copyright © HackPick, sp. z o.o. sp.k

Web Application Penetration Test Findings

Finding WAPT-001: Session Fixation (High)

Description:	The web application does not change the session token after a successful authentication or logout event. This configuration could allow an attacker to know the session identifier of another user and hijack their session.
Risk:	Likelihood: Moderate – An attacker would have to hijack a user's session cookie via a social engineering or man-in-the-middle attack. At the time of this report, cookies are well protected with proper flags and encryption. Impact: High – Successful exploitation of this vulnerability would grant an attacker full remote access to the victim's account.
System:	https://compromised.com
Tools Used:	Manual reviewwith BurpSuite
References:	https://www.owasp.org/index.php/Session_fixation

Evidence

```
POST / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: [redacted]
X-Requested-With: XMLHttpRequest
X-MicrosoftAjax: Delta=true
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Request-Id: |D8VFM.GtHf6
Content-Length: 1148
Connection: close
Cookie: ASP.NET_SessionId=gl3qli5gn4figlblb5yiudep;
ApplicationGatewayAffinity=b580c7b286ce9d1f5ed2b5d0bb599134e20623a2aa87ea19ac42e82c237e1a6f;
ai_user=WLtOS|2019-08-12T13:09:06.431Z; isRememberMeSet=[redacted]; theme=Metro;
ai_session=eI0g6|1565724044243|1565725315597

scriptMngr_TSM=%3B%3BSystem.Web.Extensions%2C%20Version%3D4.0.0.0%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D31bf3856
ad364e35%3Aen-US%3Ab7585254-495e-4311-9545-1f910247aca5%3Aea597d4b%3Ab25378d2%3B%3BStreetEMR.Timer%2C%20Version%3D1.0.7
094.33059%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3Dnull%3Aen-US%3A1fe1690f-388a-4cf5-a393-f5f755166bc2%3A36cce6b8&_
_EVENTTARGET=ctl00%24contentBody%24Login%24LoginButton&__EVENTARGUMENT=&__LASTFOCUS=&__VIEWSTATEGENERATOR=CA0B0334&ctl0
0_RadFormDecorator_ClientState=&ctl00_windowTimeOutWarning_ClientState=&ctl00_windowCsh_ClientState=&ctl00_windowMngr_C
lientState=&ctl00_contentBody_windowOrgSel_ClientState=&ctl00_contentBody_windowNoOrg_ClientState=&ctl00_contentBody_wi
ndowMngr_ClientState=&ctl00_notifyMessage_ClientState=&ctl00_notifyMessage_XmlPanel_ClientState=&ctl00_notifyMessage_Ti
tleMenu_ClientState=&__ASYNCPOST=true&RadAJAXControlID=ctl00_contentBody_ajaxMngr&scriptMngr=ctl00%24contentBody%24ctl0
0%24contentBody%24panelLoginPanel%7Cctl00%24contentBody%24Login%24LoginButton&__VIEWSTATE=<snipped>&radioTheme=Metro&Us
erName=heath%40tcm-sec.com&Password=test&RememberMe=on&hdnOrgId=&hiddenState=
```

Figure 9: SessionId set prior to authentication

Copyright © HackPick, sp. z o.o. sp.k

Additional Evidence

```
GET /admin/users HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ASP.NET_SessionId=gl3qli5gn4figlblb5yiudep;
ApplicationGatewayAffinity=b580c7b286ce9d1f5ed2b5d0bb599134e20623a2aa87ea19ac42e82c237e1a6f;
ai_user=WLtOS|2019-08-12T13:09:06.431Z; isRememberMeSet=[redacted]; theme=Metro;
ai_session=RcgSe|1565725895690|1565725918089
Upgrade-Insecure-Requests: 1
```

Figure 10: SessionId remains the same after authentication

```
GET / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: [redacted]
Connection: close
Cookie: ASP.NET_SessionId=gl3qli5gn4figlblb5yiudep;
ApplicationGatewayAffinity=b580c7b286ce9d1f5ed2b5d0bb599134e20623a2aa87ea19ac42e82c237e1a6f;
ai_user=WLtOS|2019-08-12T13:09:06.431Z; isRememberMeSet=[redacted] theme=Metro;
ai_session=RcgSe|1565725895690|1565726162157; redirectURL=~/admin/dashboard
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Figure 11: SessionId remains the same after logout

Remediation

HPS recommends DC consider the following corrective actions:

- Regenerate ASP SessionId authentication
- Timeout and replace old session IDs
- Destroy session IDs on logout and generate new IDs on each login

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-002: User Enumeration & Account Lockout – Denial of Service (High)

Description:	DC allowed user enumeration on the login page. When HPS entered an invalid user , a message stating the user did not exist in the system appeared . Additionally, DC locks accounts after 5 attempts. The accounts are locked out until an administrator unlocks them. With known employee email addresses, an attacker can leverage the account lockout feature to deny service to DC employees.
Risk:	Likelihood: High – This application is internet-accessible in production. Employee e-mails are easily gathered and enumerated through basic reconnaissance. Impact: High – An attacker with a known list of users could cause a Denial of Service, preventing account access.
System:	https://compromised.com
Tools Used:	Manual review
References:	https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration

Evidence

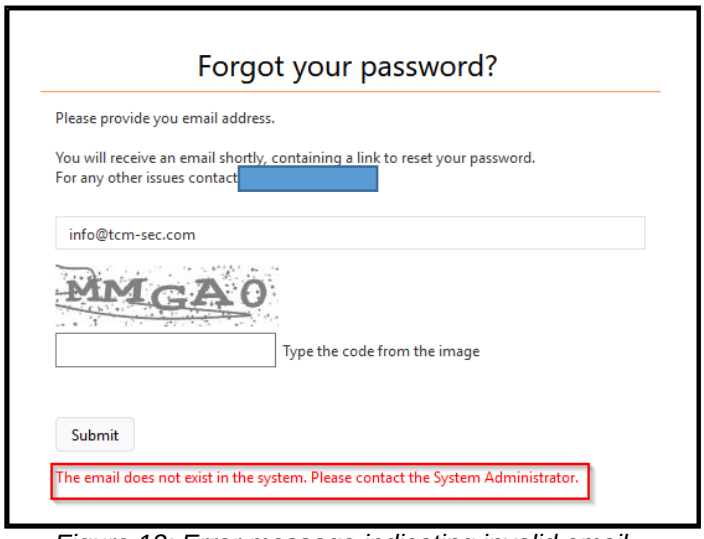


Figure 12: Error message indicating invalid email

Remediation

HPS recommends that DC use synchronized error messages. For example, when an invalid username is entered, the application could return “Invalid username and/or password, please try again”, preventing user enumeration.

HPS also recommends that DC implement CAPTCHAs on the login page after 5 failed attempts with either an invalid username or password. This will prevent attackers from attempting password spraying attacks and prevent denial of service against valid users.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-003: Insufficient Encryption – Depreciated Ciphers (Low)

Description:	These systems expose man-in-the-middle vulnerable protocols. Attackers can use weak encryption algorithms to intercept and manipulate protected traffic. These exploits require a man-in-the-middle position and advanced tools sets. For sensitive systems, only allow the strongest ciphers.
Risk:	Likelihood: Low – Exploitation of deprecated encryption ciphers requires vast computational resources. Impact: High – If exploited, an attacker can decrypt sensitive data in transit.
System:	https://compromised.com
Tools Used:	Nmap
References:	NIST SP800-53 AC-17(2) - Remote Access Protection of Confidentiality / Integrity using Encryption

Evidence

```
TLSv1.2:
  ciphers:
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
    TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
    TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
    TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
    TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
  compressors:
    NULL
  cipher preference: server
  warnings:
    64-bit block cipher 3DES vulnerable to SWEET32 attack
    Broken cipher RC4 is deprecated by RFC 7465
    Ciphersuite uses MD5 for message integrity
least strength: C
```

Figure 14: Deprecated encryption ciphers enabled

Remediation

Disable deprecated TLS encryption ciphers.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-004: Information Disclosure via HTTP Response Headers (Low)

Description:	The assessed web servers disclosed unnecessary information within HTTP response headers returned to client requests.
Risk:	Likelihood: Moderate – These systems are accessible from the internet. Impact: Low – This information could allow an attacker to fingerprint these web servers to better target future exploit attempts.
System:	https://compromised.com
Tools Used:	Burp Suite Pro
References:	https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Technical_Resources

Evidence

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionId=gl3qli5gn4figlblb5yiudep; path=/; secure;
HttpOnly
Set-Cookie: ASP.NET_SessionId=gl3qli5gn4figlblb5yiudep; path=/; secure;
HttpOnly
Set-Cookie: theme=Metro; expires=Wed, 14-Aug-2019 13:09:05 GMT; path=/;
secure; HttpOnly
X-AspNet-Version: 4.0.30319
Request-Context: appId=cid-v1:adcb8e35-be3f-43ec-a573-350cf0a3f5e4
Access-Control-Expose-Headers: Request-Context
X-Powered-By: ASP.NET
Set-Cookie:
ApplicationGatewayAffinity=b580c7b286ce9d1f5ed2b5d0bb599134e20623a2aa87ea19a
c42e82c237e1a6f;Path=/;Domain=[redacted]
Date: Mon, 12 Aug 2019 13:09:05 GMT
Connection: close
Content-Length: 37764
```

Figure 15: Returned response headers

Remediation

Remove unnecessary information from HTTP response headers.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-005: Verbose Error Messages (Low)

Description:	DC exposed sensitive information, including the web server fingerprint and through the generic IIS 404 ‘Not Found’ page. HPS triggered this page by calling a non-existent file on the target web server.
Risk:	Likelihood: High – This information can be discovered with common tools and little skill. Impact: Low – Service fingerprinting alone is not an exploitable vulnerability but may lead an attacker to more focused exploits.
System:	https://compromised.com
Tools Used:	Manual Review
References:	https://www.owasp.org/index.php/Error_Handling#Generic_error_messages

Evidence

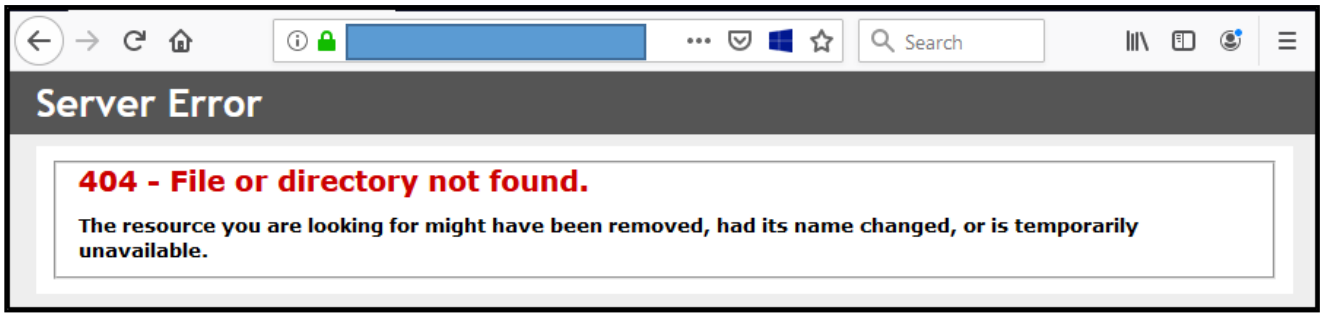


Figure 16: Generic IIS 404

Remediation

Disable verbose error messages in the IIS server configuration.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-006: Login Form Autocomplete Enabled (Low)

Description:	DC is permitting autocomplete on the username and password fields on the login page. This configuration can provide an attacker with access to user accounts.
Risk:	Likelihood: Low – An attacker would have to have access to the victim's browser. Impact: Low – This application uses two factor authentication. In addition, it locks out accounts after five failed login attempts. This could create a user Denial of Service, however it is unlikely that it will cause data compromise.
System:	https://compromised.com
Tools Used:	Burp Suite Pro
References:	OWASP Testing for User Enumeration and Guessable User Account

Evidence

```
<body>
    <form method="post" action="./Default.aspx" onsubmit="javascript:return
WebForm_OnSubmit();" id="frmMain">
<div class="aspNetHidden">
<input type="hidden" name="scriptMngr_TSM" id="scriptMngr_TSM" value="" />
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__LASTFOCUS" id="__LASTFOCUS" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="3gmqUq52xwzNiR7Bv5gGT8zUJf0IKOz6E53HOudT+CBZca/lWllEKmg49hjm6UsRX/EDvXXxcMGBIEvR0brEc
aJzx0S/NPnsqtDeletVA+k=" />
</div>
```

Figure 17: Login form with autocomplete enabled

Remediation

Disable autocomplete on sensitive form input fields. This can be done by including the attribute "autocomplete='off'" within the FORM tag.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-007: Insecure HTTP Response Headers (Low)

Description:	Response headers with issues were observed in the application
Risk:	Likelihood: Moderate – HTTP response headers are low-hanging fruit for attackers to fingerprint a web application. Impact: Low – Information gleamed from HTTP response headers is catalogued for future user, e.g. zero-day exploits.
System:	https://compromised.com
Tools Used:	Burp Suite Pro
References:	securityheaders.com

Evidence

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
Request-Context: appId=cid-v1:adcb8e35-be3f-43ec-a573-350cf0a3f5e4
Access-Control-Expose-Headers: Request-Context
X-Powered-By: ASP.NET
Date: Wed, 14 Aug 2019 20:28:46 GMT
Connection: close
Content-Length: 133290
```

Figure 18: Insecure response headers

Remediation

Add security related response headers. The following response headers should be added:

- Content-Security-Policy: Setting this header allows the web master to declare which sources are approved to serve content on the web application.
- Strict-Transport-Security: Setting this header forces visitors to only access the site via HTTPS. This is preferred over serving 302 web responses to forward visitors to HTTPS.
- X-XSS-Protection: Setting this header value to 1 will instruct modern web browsers to help prevent XSS.
- X-Frame-Options: Setting this header to SAMEORIGIN prevents external domains from framing Associate Connect in an iframe to potentially siphon sensitive information.

Leveraging securityheaders.com will allow DC to measure the effectiveness of the HTTP response header configuration.

Copyright © HackPick, sp. z o.o. sp.k

Finding WAPT-008: Undetected Malicious Activity (Low)

Description:	DC failed to detect all malicious activity on the web application assessment.
Risk:	Likelihood: Low – These activities occur after primary controls fail. Impact: Moderate – Undetected network attacks allow adversaries to expand control.

Remediation

Review SIEM strategy and WAF settings for the web application. Some attacks may be difficult to detect but have been noted for information and review.

Attacks Undetected

- Web vulnerability scans with Nikto and Nessus
- Active vulnerability scans with Burp Suite Pro
- Common OWASP Top 10 attack attempts (e.g. SQLi, XSS, XXE, etc.)

Copyright © HackPick, sp. z o.o. sp.k

Additional Scans and Reports

HPS provides all clients with all report information gathered during testing. This includes Nessus files, full vulnerability scans in executive and detailed formats, and a detailed findings Excel spreadsheet. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by HPS.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the following documents in your shared drive folder:

External Network:

- DC_External_Summary.xslx
- DC_External_Full.pdf
- DC_External_Executive.pdf

Internal Network:

- DC_Internal_Summary.xslx
- DC_Internal_Full.pdf
- DC_Internal_Executive.pdf

Web Application:

- DC_Unauthenticated.html
- DC_Authenticated.html

Copyright © HackPick, sp. z o.o. sp.k

Copyright © HackPick, sp. z o.o. sp.k

Copyright © HackPick, sp. z o.o. sp.k