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).

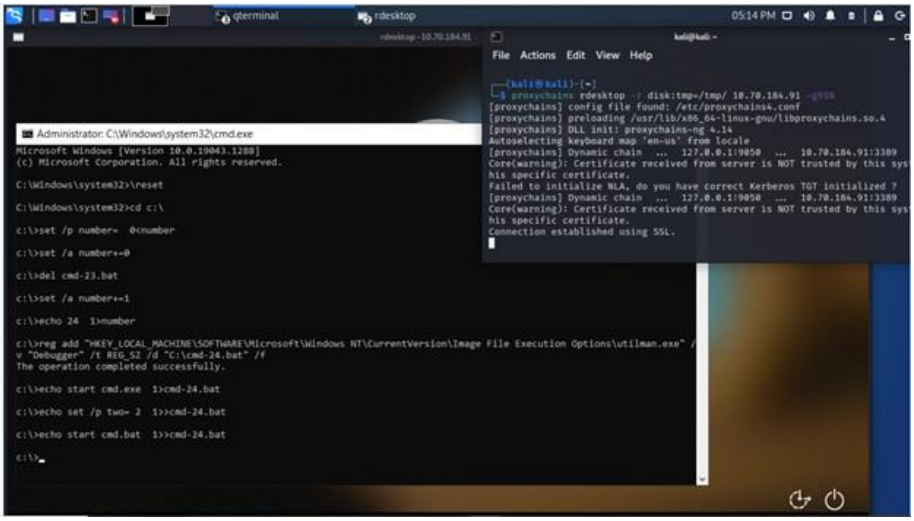

Figure 1:

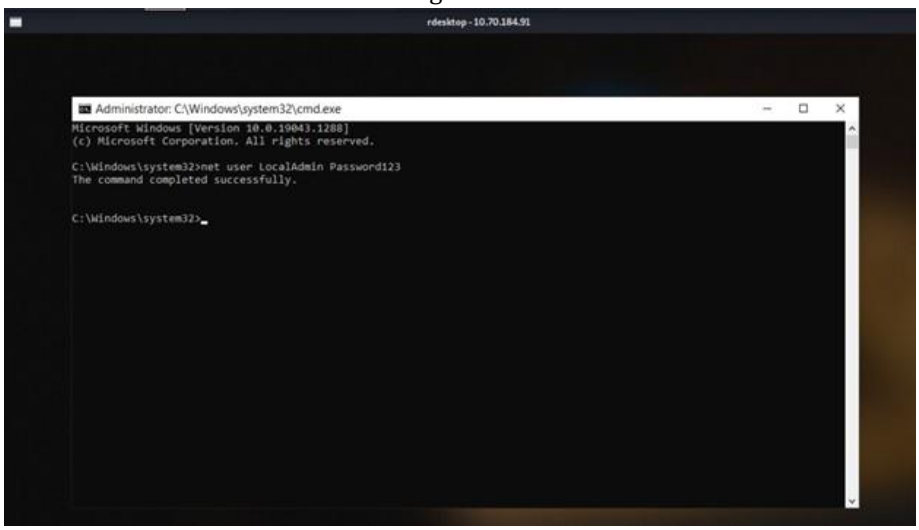

Figure 2:

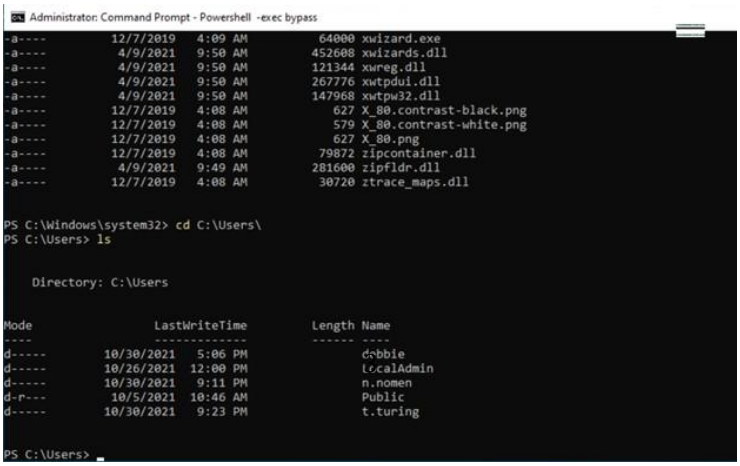

Figure 3:

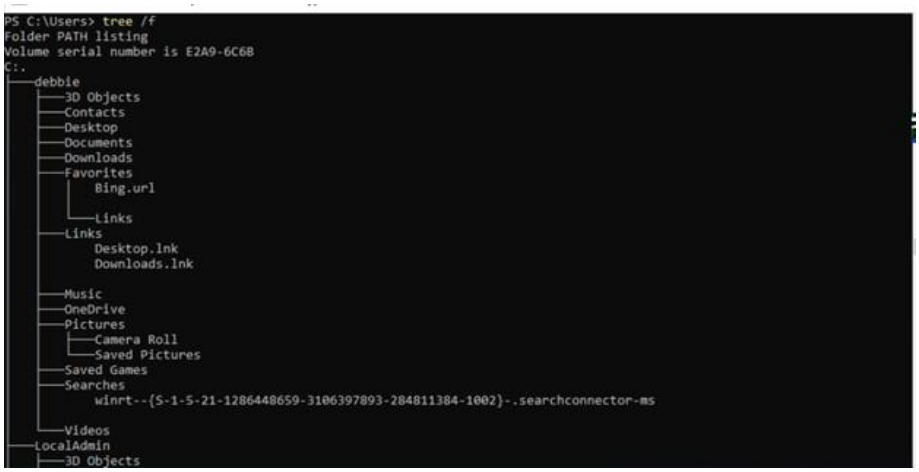

Figure 4:

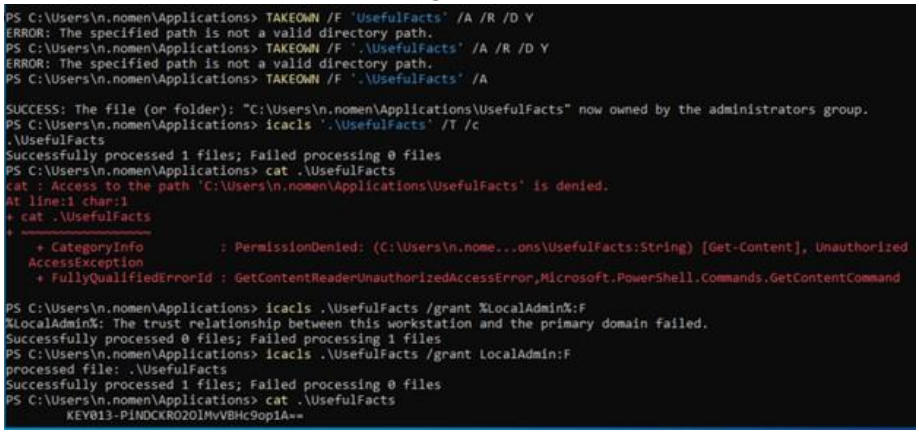

Figure 5:

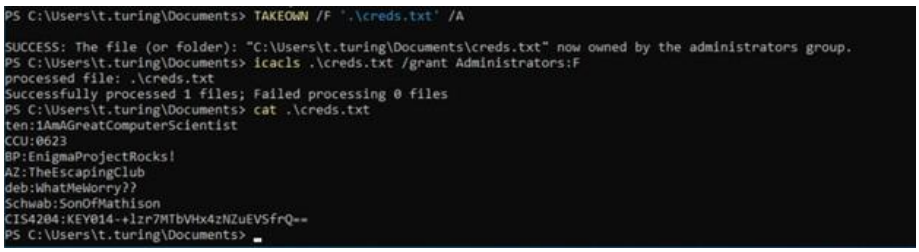

Figure 6: