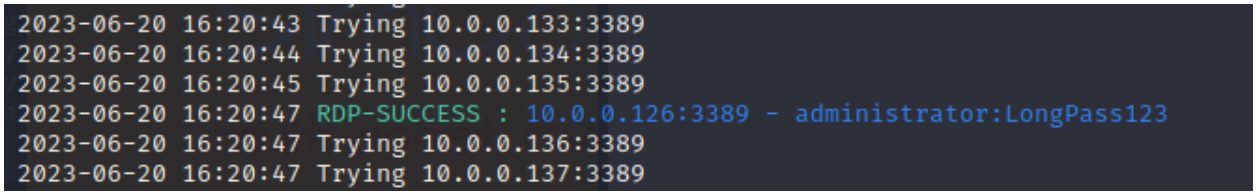
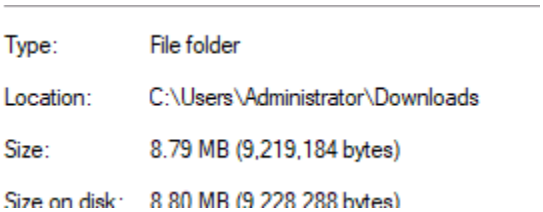
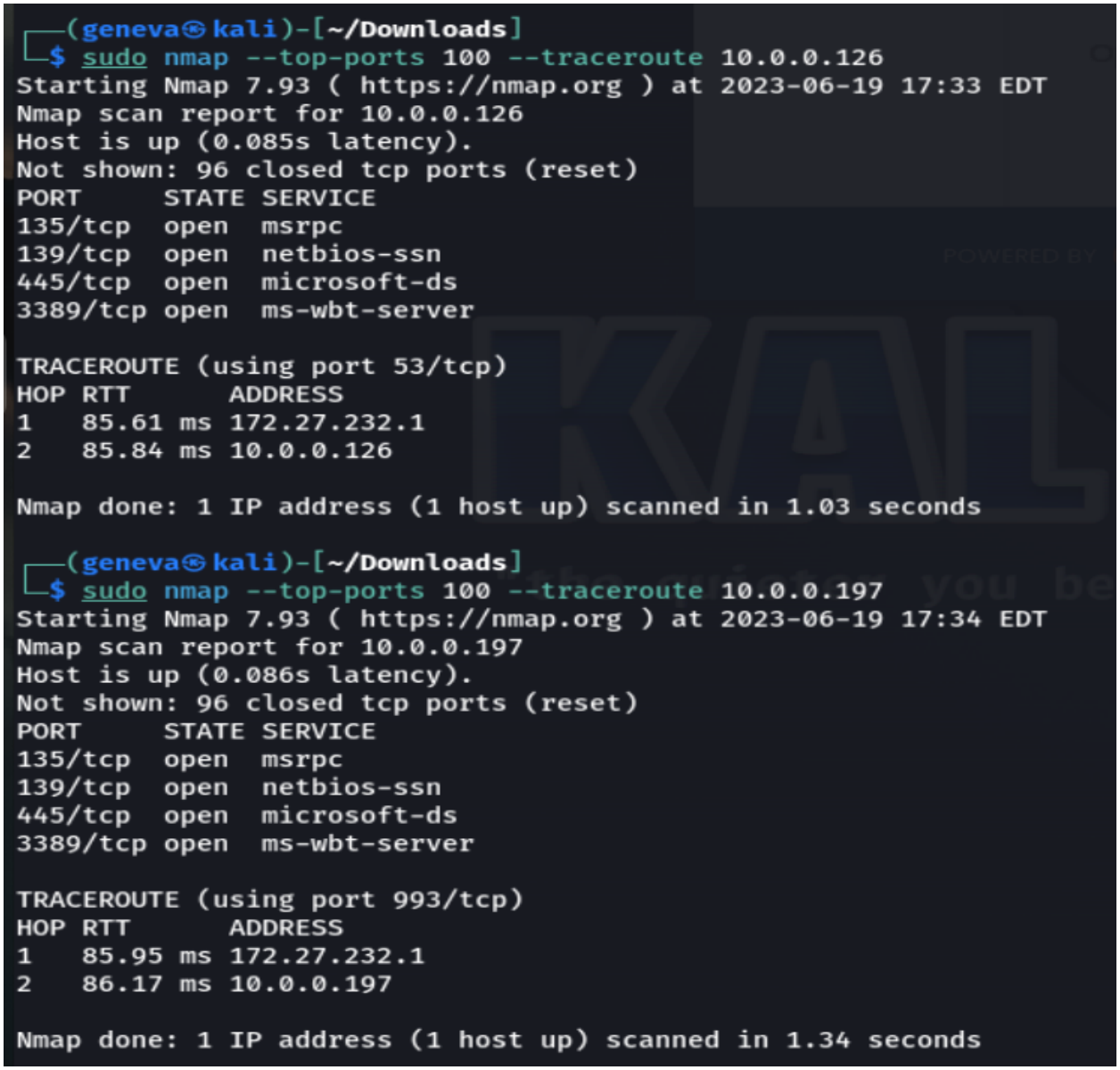
Geneva ACCOUNTING 1 10.0.0.126

We utilized Crowbar to conduct a brute force attack. We had limited knowledge about the target system, and relied on the assumption that the system has weak or easily guessable passwords or encryption keys. We were able to successfully gain access to the password.

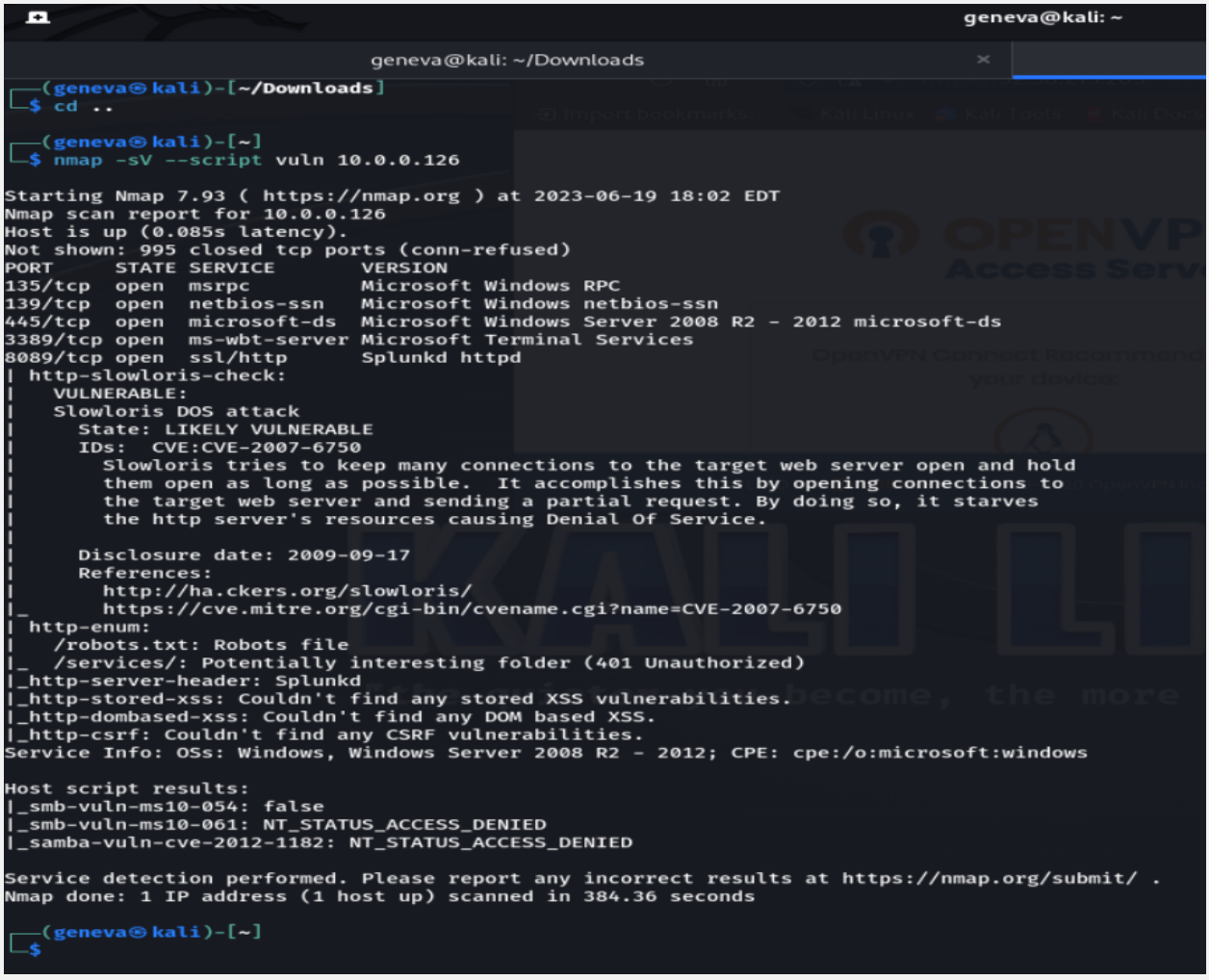


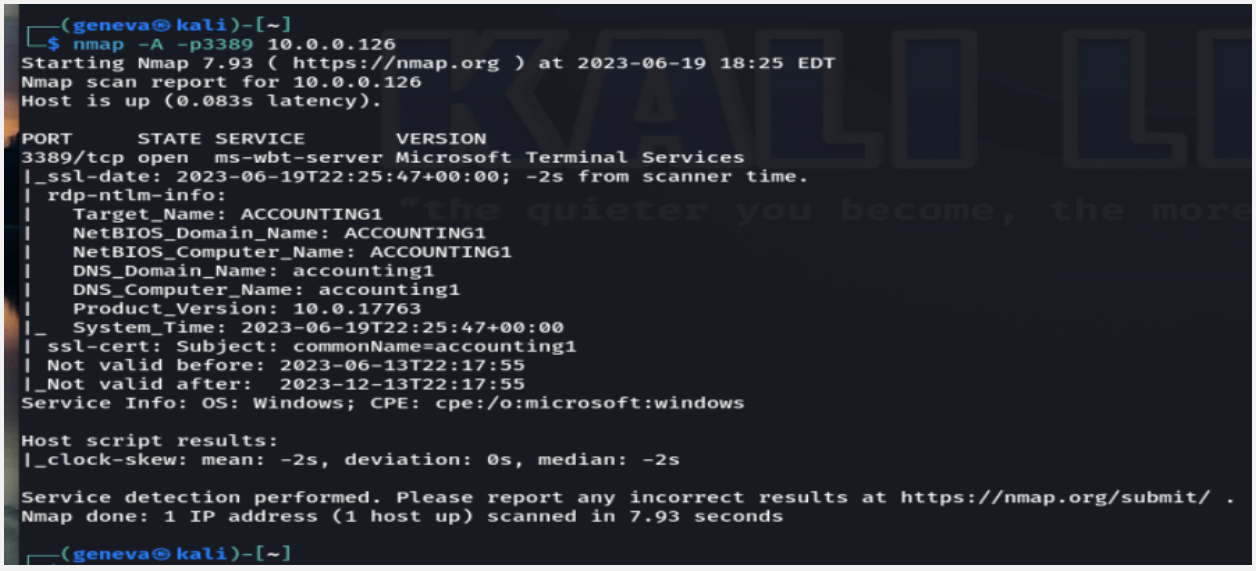


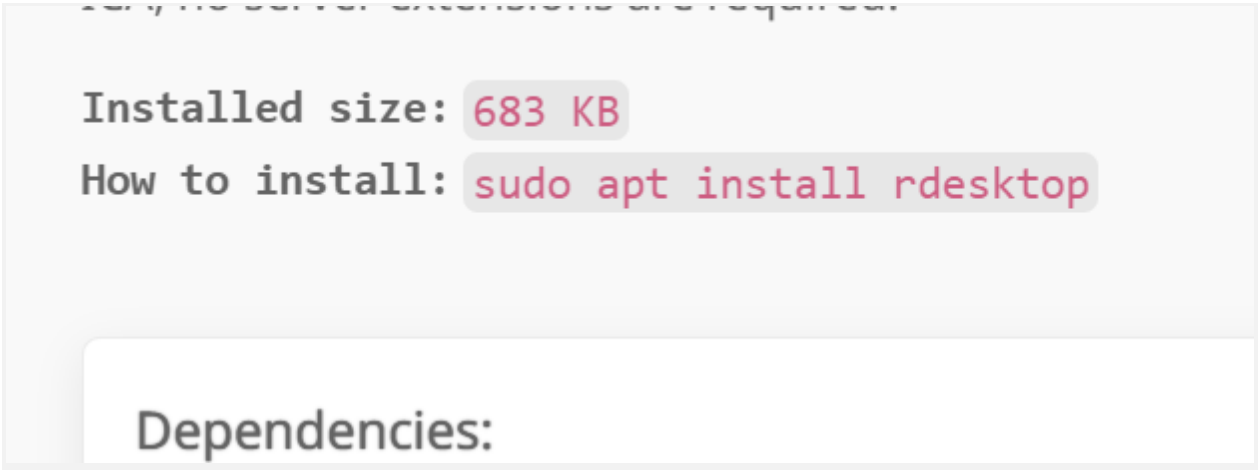
Nmap (Network Mapper) a popular and powerful open-source network scanning tool used for network exploration and security auditing is designed to discover hosts, services, and open ports on computer networks. We used this tool to discover several hosts and identify open ports to exploit.



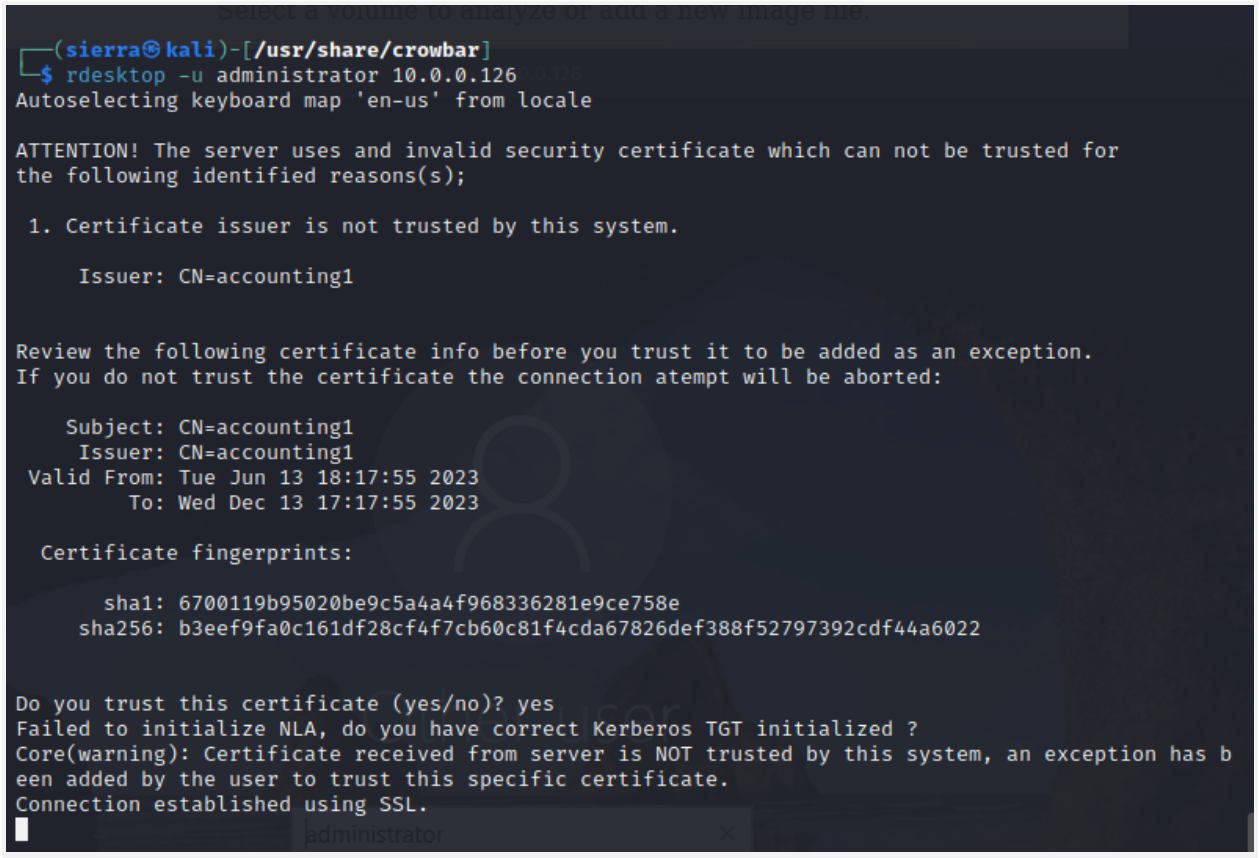
I ran nmap -sC -sV -script vuln 10.0.0.126


geneva@kali: ~
geneva@kali: ~/Downloads
(geneva㉿kali)-[~/Downloads]
$ cd ..
(geneva㉿kali)-[~]
$ nmap -sV --script vuln 10.0.0.126
Starting Nmap 7.93 (https://nmap.org) at 2023-06-19 18:02 EDT
Nmap scan report for 10.0.0.126
Host is up (0.085s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server Microsoft Terminal Services
8089/tcp open ssl/http Splunkd httpd
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-enum:
| /robots.txt: Robots file
|_ /services/: Potentially interesting folder (401 Unauthorized)
|_http-server-header: Splunkd
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 384.36 seconds
(geneva㉿kali)-[~]
$

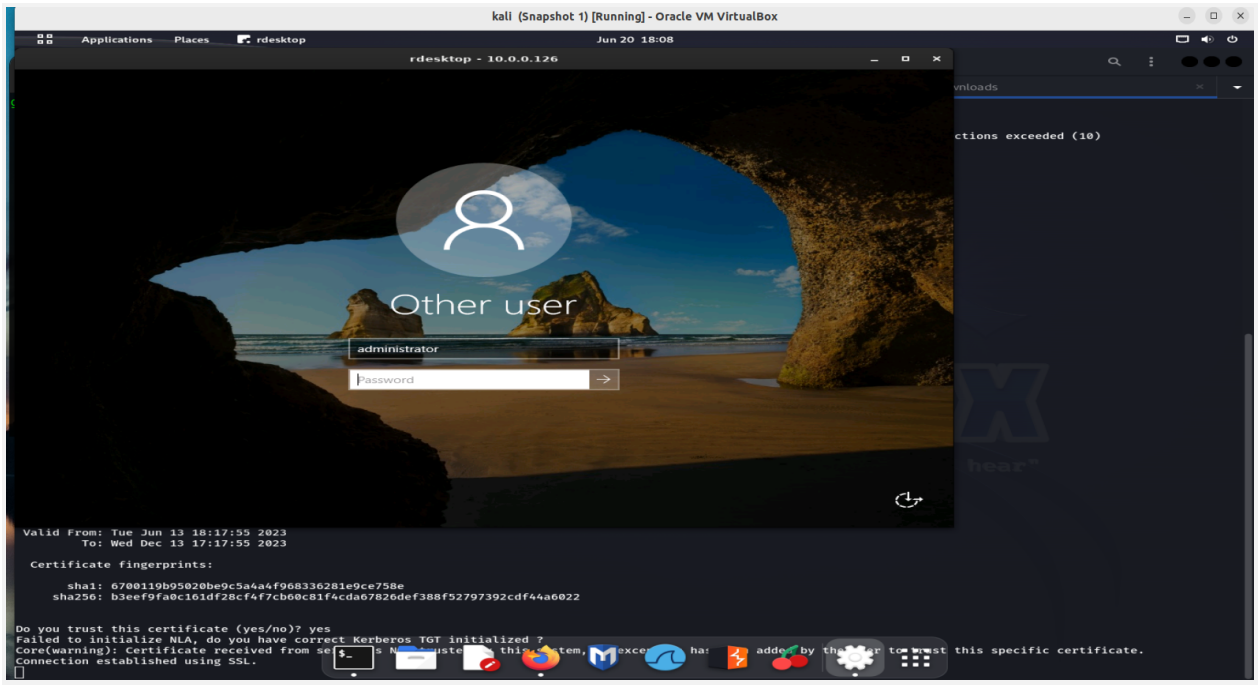

(geneva㉿kali)-[~]
$ nmap -A -p3389 10.0.0.126
Starting Nmap 7.93 (https://nmap.org) at 2023-06-19 18:25 EDT
Nmap scan report for 10.0.0.126
Host is up (0.083s latency).
PORT STATE SERVICE VERSION
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-06-19T22:25:47+00:00; -2s from scanner time.
| rdp-ntlm-info:
| Target_Name: ACCOUNTING1
| NetBIOS_Domain_Name: ACCOUNTING1
| NetBIOS_Computer_Name: ACCOUNTING1
| DNS_Domain_Name: accounting1
| DNS_Computer_Name: accounting1
| Product_Version: 10.0.17763
|_ System_Time: 2023-06-19T22:25:47+00:00
| ssl-cert: Subject: commonName=accounting1
| Not valid before: 2023-06-13T22:17:55
|_Not valid after: 2023-12-13T22:17:55
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: mean: -2s, deviation: 0s, median: -2s
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.93 seconds
(geneva㉿kali)-[~]

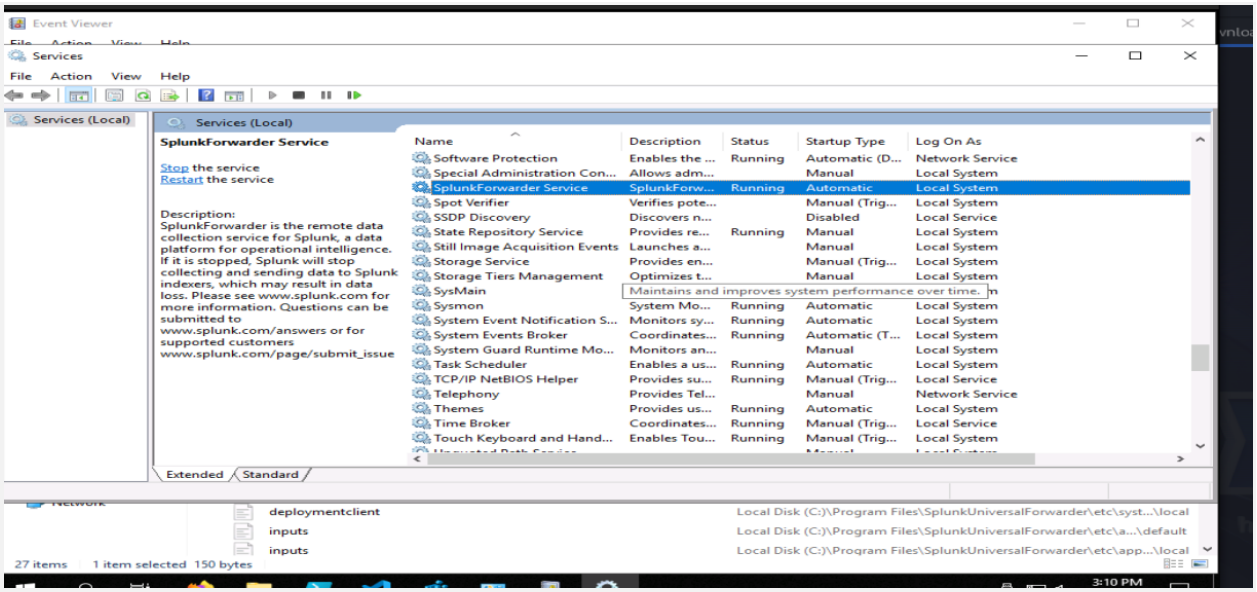


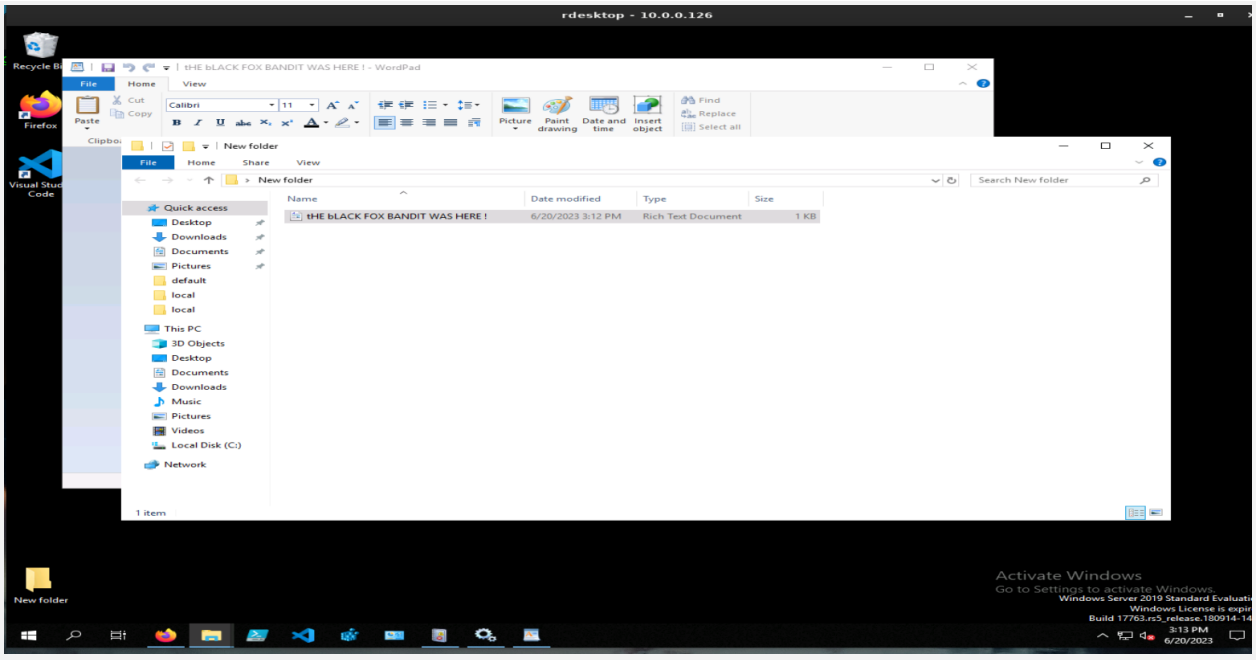
https://www.helpwire.app/blog/remote-access-kali-linux/

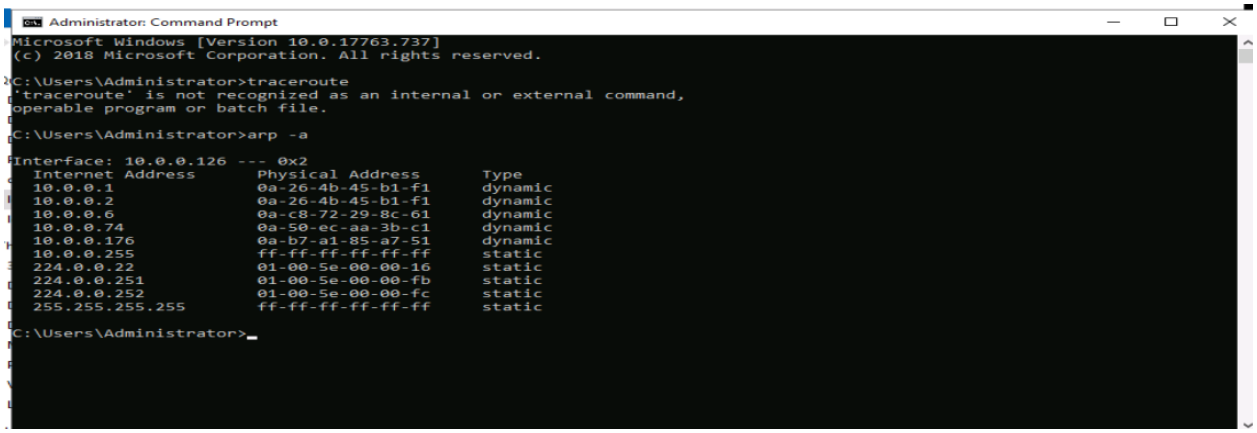


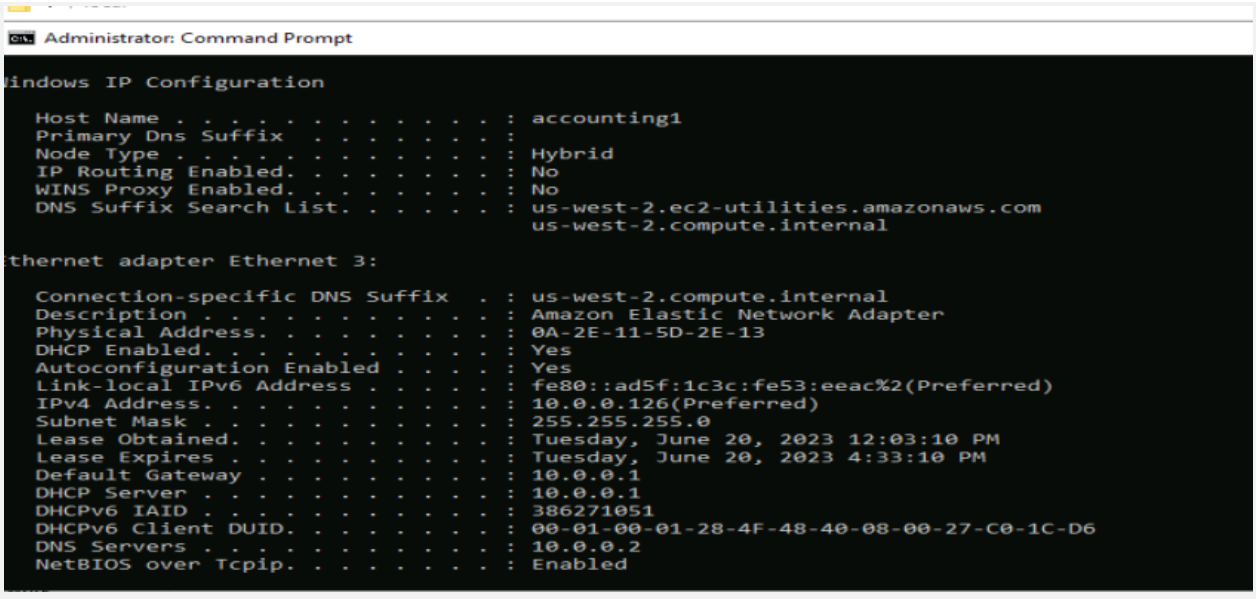
I was then able to gain access through port 3389 RDP from a Kali Linux machine into the windows using the discovered login credentials during the brute force attack. Once inside I began using ransomware, a malicious software (malware) that encrypts a victim's files or entire system, making them inaccessible until a ransom is paid. I also created an account and began escalating privileges for that user to make changes and have access to the operating system.

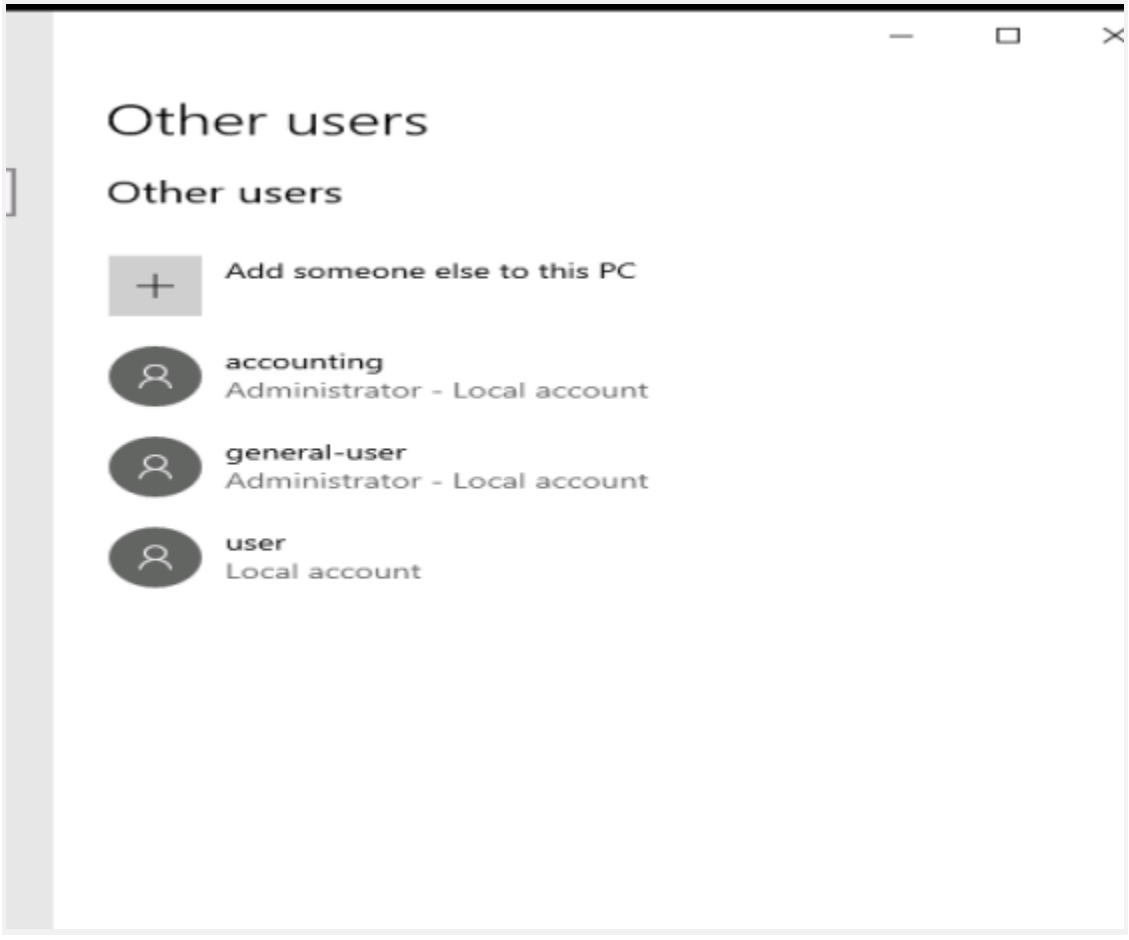


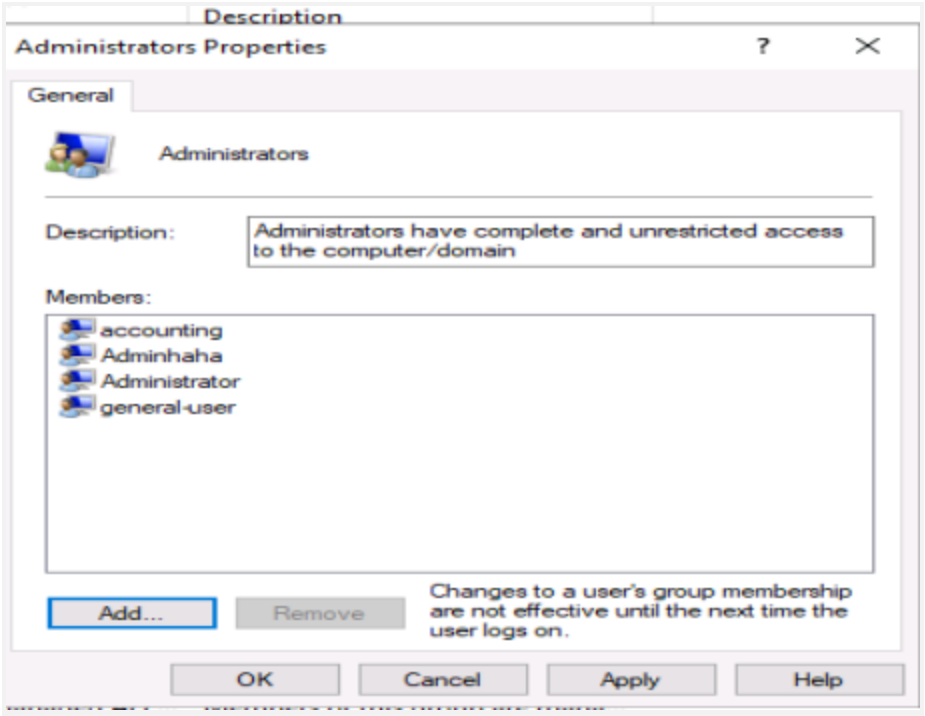

Event Viewer
Services
File Action View Help
Services (Local)
SplunkForwarder Service
Stop the service
Restart the service
Description:
SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue
Name
Description
Status
Startup Type
Log On As
Software Protection
Special Administration Con...
SplunkForwarder Service
Spot Verifier
SSDP Discovery
State Repository Service
Still Image Acquisition Events
Storage Service
Storage Tiers Management
SysMain
Sysmon
System Event Notification S...
System Events Broker
System Guard Runtime Mo...
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Themes
Time Broker
Touch Keyboard and Hand...
Maintains and improves system performance over time.
Extended
Standard
deploymentclient
inputs
inputs
27 items
1 item selected 150 bytes
3:10 PM


rdesktop - 10.0.0.126
tHE bLACK FOX BANDIT WAS HERE ! - WordPad
New folder
tHE bLACK FOX BANDIT WAS HERE !
6/20/2023 3:12 PM
Rich Text Document
1 KB
1 item
Activate Windows
Go to Settings to activate Windows.
3:13 PM
6/20/2023


Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>traceroute
'traceroute' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>arp -a
Interface: 10.0.0.126 --- 0x2
Internet Address Physical Address Type
10.0.0.1 0a-26-4b-45-b1-f1 dynamic
10.0.0.2 0a-26-4b-45-b1-f1 dynamic
10.0.0.6 0a-c8-72-29-8c-61 dynamic
10.0.0.74 0a-50-ec-aa-3b-c1 dynamic
10.0.0.176 0a-b7-a1-85-a7-51 dynamic
10.0.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\Administrator>

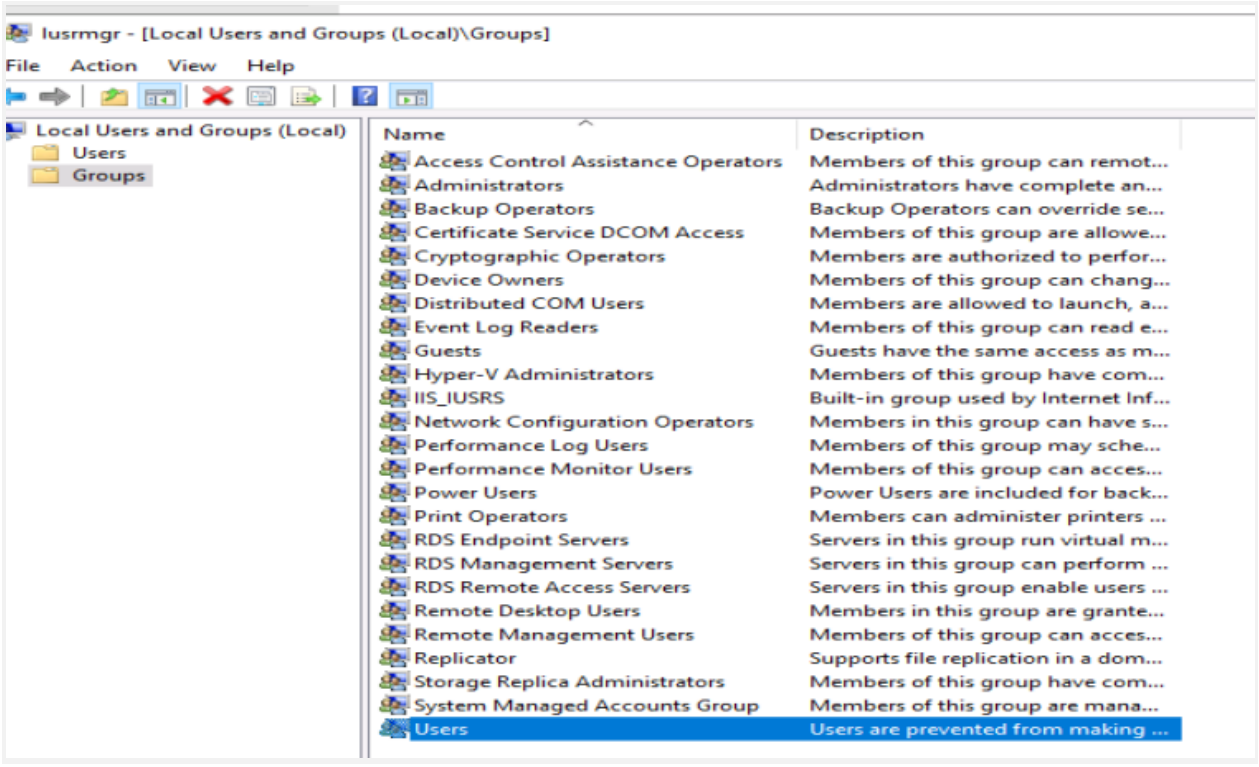

Administrator: Command Prompt
indows IP Configuration
Host Name . . . . . : accounting1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : us-west-2.ec2-utilities.amazonaws.com
us-west-2.compute.internal
thernet adapter Ethernet 3:
Connection-specific DNS Suffix . : us-west-2.compute.internal
Description . . . . . : Amazon Elastic Network Adapter
Physical Address. . . . . : 0A-2E-11-5D-2E-13
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ad5f:1c3c:fe53:eeac%2(Preferred)
IPv4 Address. . . . . : 10.0.0.126(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, June 20, 2023 12:03:10 PM
Lease Expires . . . . . : Tuesday, June 20, 2023 4:33:10 PM
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 10.0.0.1
DHCPv6 IAID . . . . . : 386271051
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-4F-48-40-08-00-27-C0-1C-D6
DNS Servers . . . . . : 10.0.0.2
NetBIOS over Tcpip. . . . . : Enabled

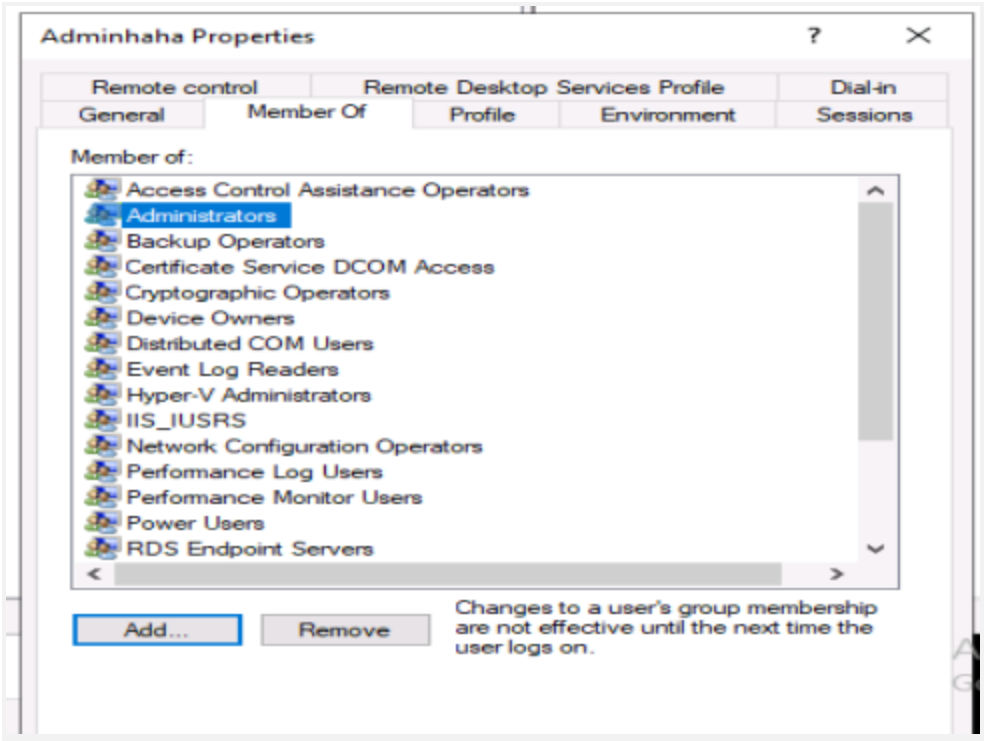

Other users
Other users
Add someone else to this PC
accounting
Administrator - Local account
general-user
Administrator - Local account
user
Local account



Blackfox123

Added to all groups at 1600 hours




Adminhaha Properties
Remote control
Remote Desktop Services Profile
Dial-in
General
Member Of
Profile
Environment
Sessions
Member of:
Access Control Assistance Operators
Administrators
Backup Operators
Certificate Service DCOM Access
Cryptographic Operators
Device Owners
Distributed COM Users
Event Log Readers
Hyper-V Administrators
IIS_IUSRS
Network Configuration Operators
Performance Log Users
Performance Monitor Users
Power Users
RDS Endpoint Servers
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.