# Network Diagram

Phyllis

192.168.224.127

Administrator

192.168.224.1

Keith

192.168.224.128

Remote Desktop Protocol enabled

OpenSSH Service Running at port 22

Windows 2019 Server

192.168.224.137

Gerald

192.168.224.129

# Attack Timeline 2

1530 to 1608

|  |  |  |
| --- | --- | --- |
| Datetime | Description | Command |
| ~1530 -1534 10/2/23 | User Gerald logins via rdp to edit some files.  Mallory happens to see gerald’s rdp password |  |
| ~1536 | Gerald goes out to buy starbucks  Mallory tries her luck by accessing into gerald’s account via rdp  Mallory does a quick search on gerald’s files and finds something interesting.  Being fearful of getting caught, she immediately logs out of the rdp session afterwards.  Mallory then tries her luck again to ssh in as Gerald with the same credentials. However, she is denied access as gerald’s authoried\_keys do not contain her public key. |  |
| ~ 1543 - 1545 | Keith logins via rdp to update some passwords before logging off. |  |
| ~ 1552 | Mallory login as Gerald via rdp and edits gerald’s .ssh/authorized keys by appending her own public key.  Mallory logins via ssh  Mallory closes her rdp session.  Mallory checks for files again |  |
| ~1556 | Mallory scp gerald’s project folders | scp -r gerald@192.168.224.137:C:/Users/gerald/Desktop/Projects . |
| ~1559 | Mallory decides to try privilege escalation | scp -r Privesc gerald@192.168.224.137:AppData/Local/Temp |
| ~1602 - 1608 | Mallory imports the privesc module and runs Invoke-AllChecks and found the administrator password  Mallory rdps back in as Gerald and edits the administrator .ssh/authorized\_keys file to gain ssh access as admin  Mallory changes the file permissions of authorized\_keys and adds her own keys inside the authorized\_keys file  Mallory then changes back the permissions to avoid suspicion  Mallory ssh in as admin  Mallory steals keith’s important password file. |  |
|  |  |  |



