

# Obfuscation Assignment

OS: Windows

Tool: PowerShell

Command: net user username /delete

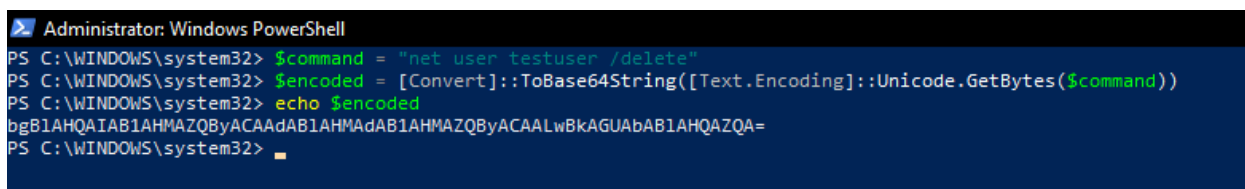
Encryption / Encoding: Base64

Encode the administrative command “net user” using Base64 to obscure its real purpose from the user.

Use PowerShell to encode the command by running the following commands:

1. `$command = "net user testuser /delete"`
2. `$encoded = [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($command))`
3. `echo $encoded`

The first command defines our command that we are trying to encode, second command defines the encoding command and the conversion of the command to be to Base64 string. Finally, we echo the encoded command to display the Base64 string of our delete user command.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> $command = "net user testuser /delete"
PS C:\WINDOWS\system32> $encoded = [Convert]::ToBase64String([Text.Encoding]::Unicode.GetBytes($command))
PS C:\WINDOWS\system32> echo $encoded
bgBIAHQAIAB1AHMAZQByACAAdABIAHMAAdAB1AHMAZQByACAALwBkAGUAbABIAHQAZQ
PS C:\WINDOWS\system32>
```

Base64 string Output:

bgBIAHQAIAB1AHMAZQByACAAdABIAHMAAdAB1AHMAZQByACAALwBkAGUAbABIAHQAZQ  
A=

Now we will attempt to execute the obfuscated command using the Encoded string:

1. `$encodedCommand = "bmV0IHVzZXIgbmV3dXNlciAvZGVsZXRI"`
2. `$decodedCommand = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($encodedCommand))`
3. `Invoke-Expression $decodedCommand`

This part of the process, we will begin by defining our encoded command, followed by the decoding command where we reverse the encoding command performed above. Finally, we will invoke the decoded command which contains the delete user command.

```
PS C:\WINDOWS\system32> $encodedCommand = "bgB1AHQAIAB1AHMAZQ8yACAAdAB1AHMAdAB1AHMAZQ8yACAALwBkAGUABAB1AHQAZQA="
PS C:\WINDOWS\system32> $decodedCommand = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($encodedCommand))
PS C:\WINDOWS\system32> Invoke-Expression $decodedCommand
The command completed successfully.
```

## Validation:

We can use CMD to verify that the user account is successfully deleted.

```
C:\WINDOWS\system32>net user

User accounts for \\MAR

-----
Name                Password               Last
-----                -
testuser            [REDACTED]             [REDACTED]
The command completed successfully.
```

Before

```
C:\WINDOWS\system32>net user

User accounts for \\MAR

-----
Name                Password               Last
-----                -
Ar[REDACTED]         Dr[REDACTED]           e[REDACTED]
Gr[REDACTED]         h[REDACTED]            ol[REDACTED]
WC[REDACTED]
The command completed successfully.
```

After

## Conclusion:

In this practice, we were obfuscating commands by encoding them in Base64, like in this example with the “net user testuser /delete” command, which offers us an effective way to mask our true intentions. The command was encoded, then decoded and executed to delete the user "testuser" without revealing the actual command in plaintext. This simple technique helps adversaries bypass detection, as security tools may overlook the obfuscated commands, making it harder for security teams to quickly identify and respond to potential threats.