



- & &



1-

systeminfo

net start

tasklist

schtasks

2-

ipconfig /all -dns

net view /domain

net time /domain

netstat -ano

nslookup

3-

Domain Admins

Domain Computers

Domain Controllers

Domain Guest

Domain Users

Enterprise Admins

whoami /all

net config workstation

net user

net localgroup

net user /domain

net group /domain

wmic useraccount get /all

net group "Domain Admins" /domain

net group "Enterprise Admins" /domain

net group "Domain Controllers" /domain

4-

HASH -mimikatz(win) mimipenguin(linux)
-LaZagne(all) XenArmor(win)

Netsh WLAN show profiles

Netsh WLAN show profile name=" " key=clear

1.

2. Web PHPMyAdmin

3. Cookies

4. 3389 ipc\$
- 5.Windows WIFI
6. Email VPN FTP OA

5-

net time /domain nslookup ping

nbtscan 192.168.3.0/24

for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.3.%I | findstr "TTL="

nmap masscan PowerShell nishang empire

nishang

Import-Module .\nishang.psm1

#

Set-ExecutionPolicy RemoteSigned

nishang

Get-Command -Module nishang

#

Get-Information

#

Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress 192.168.3.100 -ResolveHost -ScanPort

Shell

:

1. / /
- 2.
- 3.
- 4.
5. SVN GIT
- 6.
- 7.
- 8.
- 9.
- 10.



<http://unixwiz.net/tools/nbtscan.html>

<https://github.com/samratashok/nishang>