**Windows firewall:**

Netsh.exe advfirewall firewall add rule name="<Rule Name>" program="<FilePath>" protocol=tcp dir=in enable=yes action=allow profile=Private

Parameter Description:

· Name=<Name of the rule you want >

· program=<”Path of the executable”>

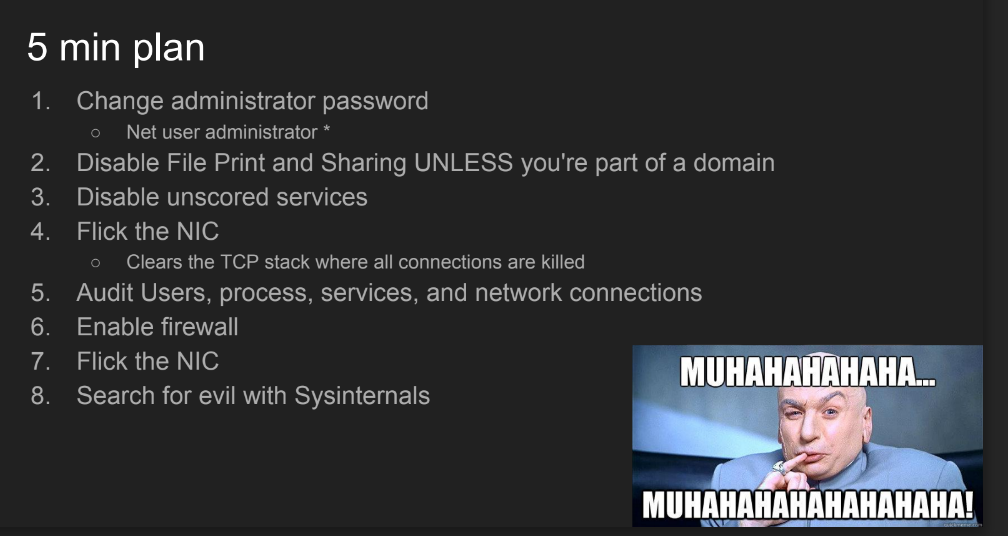
· protocol=tcp or udp

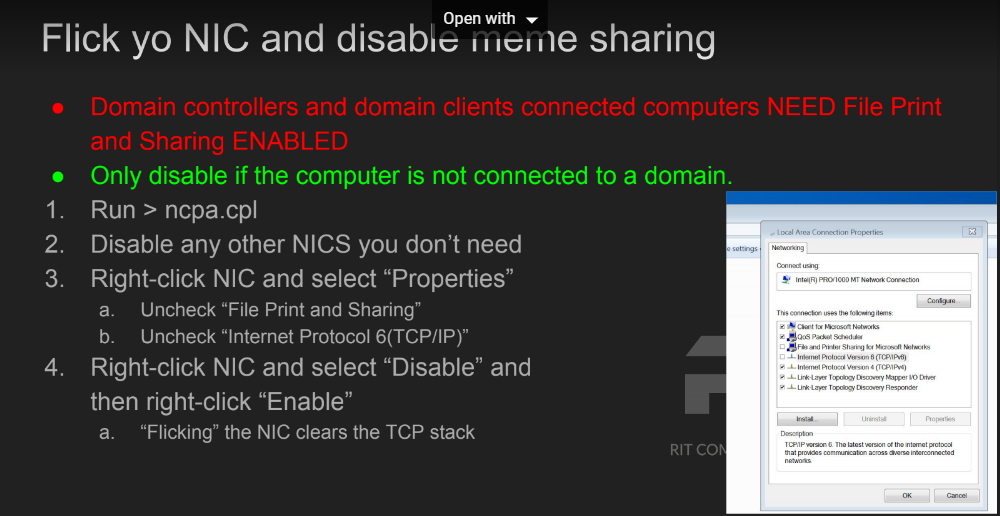
· dir=Inbound(in) or outbound(out) rule

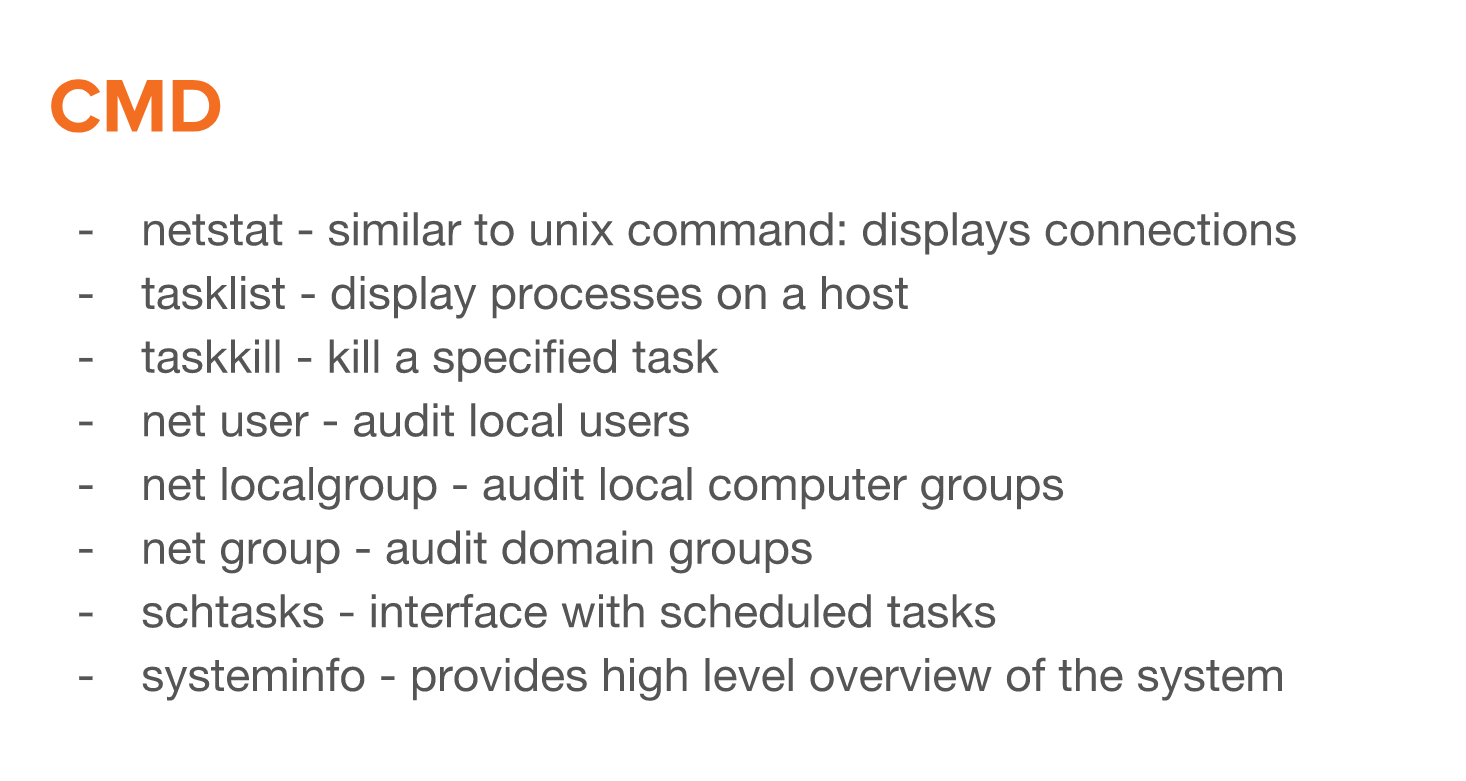
· enable=yes or no

· action=allow or block or custom

· profile=Private and/or public and/or domain (To add rule in more than one profile use “,” E.g.: profile=private, domain )







**Defense strategies:**

-Backdoored Service Files

-Disable Unneccessary

-Services Harden Service Files

-Web shells

-Audit Web Directory

-Harden PHP config?

-Backdoored Binaries

-Reinstall Packages

-Malicious Cron Jobs

-Stop and Disable Cron

-Bind Shells

-Audit listening ports

-Firewalls (iptables)

-Default Creds

-Change Passwords

-Aliased Commands

-Unalias or prepend a \

-Install and use a different shell

-Reverse Shells

-Firewalls (iptables)

-Rootik?

-Disable unsigned modules

Linux

* Make a file immutable, must have root, chattr +i file.txt
* Make a file mutable, must have root, chattr -i file.txt
* 