Linux gerelateerde Groups/commando’s

|  |  |
| --- | --- |
|  | Description |
| /Bin | Bin staat voor binary daar staan alle user binaries dus alle programma’s die ik als user kan gebruiken staan hierin. |
| / etc | Bevat de configuratiebestanden zoals SSH |
| / home | De homedirectory's bevatten de gebruikers en hun directory's |
| / sbin | Bevat de binaire bestanden van het systeem, bijvoorbeeld als je het systeem opnieuw wilt configureren |
| / tmp | Map is als u iets tijdelijk wilt gebruiken en als je bestanden wilt dumpen |
| / root | Dit is de basismap van de gebruiker, deze map is niet toegankelijk voor andere gebruikers alleen als ze root-toegang hebben. |

|  |  |
| --- | --- |
| Command | Description |
| Ctrl + r | Search command history |
| Ctrl + a | Move cursor to beginning |
| Ctrl + e | Move cursor to end |
| Ctrl + k | Kill = Cut (from where the cursor is) |
| Ctrl + y | Yank = Paste |
| Ctrl + l | Clear |
| Shift + Ctrl + O | Close al terminals |
| Shift + Ctrl +C | Copy |
| Shift + Ctrl + P | Paste |
| Passw | Veranderen Password (Root toegang vereist) |
| pwd | Print working directory |
| cd | change directory |
| mkdir | make/create directory |
| touch | Create file |
| ls | list directory content |
| cat | Concatenate and display files |
| less | show file content |
| head –[n] | Default displays the first 10 lines of a file |
| tail –[n] | Default displays the last 10 lines of a file   * *if you replace n with 50 it will show 50 lines* |
| tail -f | Follow the end of a changing file |
| cp | Copy file |
| mv | Move or rename file |
| Rm & rmdir | Remove file and/or directory |
| Cd ~ | returns to home |
| Ls -l | Shows a long list of the directory and permissions |
| Ls -a | list all files in the directory including the hidden files |
| Ls -r | List files/directories in reverse order |
| Ls -t | list new files first (sort by time and date) |
| Ls -rt | list old files reverse |
| cp [ files (s)] [destination]- | Copy files(s) |
| cp -r | Copy recursively (if you want to copy dirs.) |
| cp -I | Copy interactivily , |
| cp /file name /Directory | Copy file to different directory |
| Rm /tmp/testfile | Remove file |
| Rmdir /tmp/testdir | Remove **empty** testdir  The rm command you can remove files or directory notice the word empty if this directory is **not** empty you cannot use this command. |
| Rm -r /tmp/testdir | Remove directory and its content  This command will remove the file in tmp if it is not empty |
| Rm -r -i /tmp/testdir | Iteractive  This command will remove the file in tmp if it is not empty but will prompt u if you really want to remove this. |
| Rm -rf /tmp/testdir | Force remove  The command is used when the file/directory is used by a program and we can cannot delete it |
| tar c | Create archive |
| tar r | Append to archive (Add files to the archive) |
| tar t | list content of archive (List without extracting it) |
| tar v | * Verbose archive (This gives you information what is going on) |
| Tar f (file) | File to use (Specify the file that you want to archive) |
| Tar x | Extract archive |
| cd.. |  |
| whatis ping | Voor het ping programma vragen we de One line description op. |
| ping --help | We vragen de parameters van een commando/programma op. |
| sudo | Een commando wordt met root privilege uitgevoerd |
| sudo su | Change to root |
| cd / | We openen de root map |
| ls | We vragen de inhoud van een map op |
| ls –a | We vragen de inhoud van een map op ook de hidden files |
| cd <map-naam> | We openen een child map  (level down) |
| cd .. | We openen de parentmap (level up) |
| cd /<map-naam>/<map-naam> | We openen een map |
| cd ~ | We openen de home map |
| nano | We maken een tekstbestand aan of openen een tekstbestand |
| rm | We verwijderen een bestand |
| mkdir | We maken een map aan |
| rm –r | We verwijderen een map |
| passwd root | We configureren het root wachtwoord |
| adduser | We voegen een gebruiker toe |
| passwd | We passen het wachtwoord van een gebruiker aan |
| su - <user> | We loggen in met een ander gebruikersprofiel |
| deluser --remove-home <user> | We verwijderen een gebruikersprofiel |
| chmod -R 777 <map> | We configureren rechten op een map |
| history | We vragen de inhoud van de command history buffer op |
| lsb\_release –a | We vragen de Linux versie op |
| clear | We resetten de terminal |
| ifconfig | We vragen de IP configuratie op |
| Ps aux | We vragen een lijst op met lopende processen/programma’s |

Install commando’s

|  |  |
| --- | --- |
| apt-get update | Controleert of er updates zijn voor installed packages |
| apt-get upgrade | Upgrade installed packages |
| apt-get install | Install package |
| apt-get remove | Verwijderd installed package, maar niet de personal settings |
| apt-get purge | Verwijderd installed package en de personal settings |
| apt autoremove | Packages die niet meer nodig zijn worden verwijderd |
| Top | We vragen een lijst op met lopende processen (applicaties). De processen die de meeste resources gebruiken worden getoond |

Netwerk en proces commando’s

|  |  |
| --- | --- |
| ifconfig | We vragen de IP configuratie op |
| route –n | We vragen het IP adres van de default-gateway op |
| ping 8.8.8.8 | We pingen de Google DNS server |
| Ctrl+c of Ctrl+Z | We stoppen een programma |
| ping 8.8.8.8 -I eth0 | We pingen via een opgegeven interface |
| ps aux | We vragen een lijst op met lopende processen/programma’s |
| kill | We stoppen een proces/programma |
| top | We vragen een lijst op met lopende processen (applicaties). De processen die de meeste resources gebruiken worden getoond |
| netstat –a | We vragen de lijst met poorten op die door services worden gebruikt |
| ssh [student@10.0.0.4](about:blank) | We openen een SSH verbinding met een remote apparaat |
| echo $PATH | We vragen de PATH variabele op. |
| which ls | We vragen het pad naar een bin bestand op. |
| Cat | Cat gebruiken we, wanneer we tekstbestanden alleen willen lezen |
| Less | Wanneer de output te groot is om te kunnen worden gedisplayed in de terminal, dan kunnen we het less commando gebruiken. |
| Find | Find zoekt standaard in de huidige map en onderliggende mappen (relative path). |

Project 1

Websites

|  |  |
| --- | --- |
| Portal.azure.com | Website azure platform |
| Github.com | Website github platform |
| Dev.azure.com | Website Devops |
| https://www.microsoft.com/nl-nl/microsoft-365/microsoft-teams/group-chat-software | Aanmaken Teams account |
| https://www.keybr.com/ | Blind typen |

Commando’s and ports

|  |  |
| --- | --- |
| RDP (shortcut mstsc port 3389) | Remote desktop in windows |
| Ssh (port 22) | The **ssh** command provides a secure encrypted connection between two hosts over an insecure network  **(**ssh <username>@<ip of domeinnaam>**)** |
| ssh [student@160.10.2.1](about:blank) | We maken een connectie met een remote apparaat |
| Telnet(23) | **Telnet** is an application protocol **used** on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. |
| sftp(port 22) | SH Secure File Transfer Protocol. **SFTP** (SSH File Transfer Protocol) is a secure file transfer protocol. It runs over the SSH protocol. It supports the full security and authentication functionality of SSH. |
| taskkill /F /PID 5928 | Stop de taak met het process id 5988 |
| ipconfig | Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings |

Standaard CMD-commando’s

|  |  |
| --- | --- |
| help | We vragen de beschikbare OS commando’s op |
| Get-Help | Uitgebreide help functie |
| /? | We vragen de parameters van een commando/programma op |
| ver | We vragen de Windows versie op |
| dir | We vragen de inhoud van een map op |
| cd <map-naam> | We openen een map (level down) |
| cd .. | We open een parentmap (level up) |
| cd / | We openen de root (C:\) |
| cd \<map-naam>\<map-naam>\ | We openen een map |
| ping 8.8.8.8 | We pingen 8.8.8.8 |
| ping -t 8.8.8.8 | We pingen oneindig 8.8.8.8 |
| Ctrl+C | We stoppen een programma |
| tasklist | We vragen de lijst op van lopende programma’s |
| taskkill /F /PID <pid> | We stoppen een programma |
| ipconfig | We vragen de IP configuratie op |
| <naam programma> | We openen een programma |
| netstat -n | Met netstat -n vragen we de netwerksessies op |
| netstat –a | We vragen de poorten op, die gebruikt worden door services |
| exit | We verlaten de huidige sessie |
| cls | Clear screen |
| ssh [student@160.10.2.1](about:blank) | We maken een connectie met een remote apparaat |

Project 2

Websites

|  |  |
| --- | --- |
| https://www.whatismyip.com/ | Publieke ip addres opvragen |
| https://www.ssh.com/ssh/putty/download | Download Putty |
| https://winscp.net/eng/download.php | Download Winscp |

Commando’s and ports

|  |  |
| --- | --- |
| http (80) | Unencrypted webverkeer |
| https (443) | Encrypted webverkeer |
| Mstsc | Remote desktop windows |
| cmd | Openen dos box |
| Where notepad | We vragen de PATH van notepad op. |
| help | We vragen de beschikbare OS commando’s op |
| /? | We vragen de parameters van een commando/programma op |
| ver | We vragen de Windows versie op |
| dir | We vragen de inhoud van een map op |
| cd <map-naam> | We openen een map (level down) |
| cd .. | We open een parentmap (level up) |
| cd / | We openen de root (C:\) |
| cd \<map-naam>\<map-naam>\ | We openen een map |
| ping 8.8.8.8 | We pingen 8.8.8.8 |
| ping -t 8.8.8.8 | We pingen oneindig 8.8.8.8 |
| Ctrl+C | We stoppen een programma |
| tasklist | We vragen de lijst op van lopende programma’s |
| taskkill /F /PID <pid> | We stoppen een programma |
| ipconfig | We vragen de IP configuratie op |
| <naam programma> | We openen een programma |
| netstat -n | Met netstat -n vragen we de netwerksessies op |
| netstat –a | We vragen de poorten op, die gebruikt worden door services |
| exit | We verlaten de huidige sessie |
| cls | Clear screen |
| ssh [student@160.10.2.1](about:blank) | We maken een connectie met een remote apparaat |
| Title /? | Opvragen parameters title |
| Dir | Vraag de bestanden in een directory op |
| regedit | **Hiermee open je het Windows Register. Het bevat allerlei gegevens over instellingen van Windows** |

Project 3

Websites

|  |  |
| --- | --- |
| https://hub.docker.com/editions/community/docker-ce-desktop-windows/ | Download Docker |
| https://nodejs.org/en/ | Download Node.js |
| https://chocolatey.org/install | Download chocolatey |
| https://git-scm.com/download/win | Download Git |
| https://www.postman.com/downloads/ | Download Postman |
| https://www.python.org/downloads | Download Python |

|  |  |
| --- | --- |
| docker --version | Opvragen docker versie |
| git --version | Opvragen Git version |
| python -V | Huidige pythone versie |
| pip –version | Huidige Pip versie |
| Pip freeze | Installed Python libraries |
| pip install numpy | Install numpsy |
| pip uninstall numpy | Deinstall numpsy |

Powershell

|  |  |
| --- | --- |
| Get-ExecutionPolicy -list | Lijst rechten in powershell |
| Set-ExecutionPolicy Unrestricted | Rechten op onbeperkt zetten |

Project 4

Websites

|  |  |
| --- | --- |
| https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?view=azure-cli-latest&tabs=azure-clid | Azure CLI-installatie pagina. |
| https://code.visualstudio.com/download | Download Visual studio |
| https://www.microsoft.com/en-us/p/windows-terminal/9n0dx20hk701?activetab=pivot:overviewtab | Download windows terminal |
| https://notepad-plus-plus.org/downloads/ | Download notepad++ |

Powershell, Command Prompt, Azure Cloud Shell

|  |  |
| --- | --- |
| Az --version | In powershell CLI versie opvragen |
| Az login | Inloggen op azure omgeving |
| Az -h (--h ) | Alle az commando’s opvragen |
| Az network -h | We zoeken op network |
| --name pf -n |  |
| az network nsg create -n nsg01 -g test-student | Aan maken NSG |
| Get-AzVM -Name testpc01 | We vragen over onze VM basis informatie op |
| Remove-AzVM -ResourceGroupName test-student -Name pc02 | We verwijderen de VM |
| Install-Module -Name Az -AllowClobber | installeren de Azure Az module |
| import-Module Az | Importeren Module az |
| Connect-AzAccount | Inloggen Az account |
| **Get-Command** | Opvragen beschikbare cmdlets |
| Get-Command –Verb new | In dit voorbeeld vragen we de cmdlets op waarin het werkwoord (Verb) new is |
| Get-Command –Noun service | In dit voorbeeld vragen we de cmdlets op waarin het zelfstandig naamwoord (Noun) service is. |
| New-AzVM -ResourceGroupName test-student | Nieuwe resource group met naat test student |
| Get-AzVM -Name test-pc01 | We vragen over onze VM basis informatie op. |
| New-AzVM –ResourceGroupName test-student -Name pc02 –Location 'West Europe' –Image UbuntuLTS | Aanmaken nieuwe VM me loacatie en image (OS) |
| Start-AzVM -ResourceGroupName test-student -Name pc02 | Start de vm |
| Remove-AzVM -ResourceGroupName test-student -Name pc02 | Verwijder de VM |

Project 5

Powershell

|  |  |
| --- | --- |
| Get -Executionpolicy -list | We vragen de PowerShell rechten op |
| Set-executionPolicy unrestricted | Onbeperkte rechten configureren |
| Choco feature enable -n allowGlobbalConfirmation | Installleren Chocolatey doormiddel van script |
| Choco uninstall <app-naam> | We deïnstalleren een programma. |
| Choco upgrade <app-naam> | We upgraden een app |
| Pip install virtualenv | We installeren virtualenv |
| Enable-WindowsOptionalFeature-Online -FeatureName Containers -All -Verbose | We enable Windows Containers. |
| Enable-WindowsOptionalFeature-Online -FeatureName Microsoft-Windows-Subsystem-Linux | We enablen WSL 2. |
| $mylogin =Get-Credential | In dit voorbeeld slaan we onze gebruikersgegevens (username en password) op als variabele. |
| Get-Credential | Opent credentials windows |
| $mylogin | De credentials worden opgeslagen in $mylogin |
| New-AzVM | We maken een nieuwe VM aan |
| -Image | We geven de image op (e.g. Windows, Ubuntu, private image) |
| -Name | We geven de VM een naam |
| -DomainNameLabel | We geven de VM een DNS label |
| -ResourceGroupName | We plaatsen de VM in een Resource group |
| -Size | Hardware VM |
| -Credential | We geven de locatie van de credentials op |
| New-AzVM -Image <jouw image naam> -Name <jouw VM naam> -DomainNameLabel <jouw VM naam> -ResourceGroupName <jouw Resource group naam> -Size Standard\_D2\_v3 -Credential $mylogin | Aanmaken Vm met credentials |

Installeren apps met chocolatey

|  |  |
| --- | --- |
| Putty | choco install putty |
| WinSCP | choco install winscp |
| Docker | choco install docker-desktop |
| Node.js | choco install nodejs |
| Git | choco install git |
| Postman | choco install postman |
| Python | choco install python |
| Azure CLI | choco install azure-cli |
| Azure Az module | choco install az.powershell |
| Visual Studio Code | choco install vscode |
| Notepad++ | choco install notepadplusplus |

Project 6

Website

|  |  |
| --- | --- |
| https://www.paessler.com/howto-free-network-monitoring | PRTG |

Powershell

|  |  |
| --- | --- |
| Get-WindowsCapability –Online | ? Name –like 'OpenSSH\*' | Controleren of ssh op de machine staat |
| Add-WindowsCapability –Online –Name OpenSSH.Server~~~~0.0.1.0 | We installeren OpenSSH.Server 0.0.1.0. |
| start-service sshd | We starten de SSH service. |
| choco | Kijk of chocolatey is geinstalleerd |
| Get-AzResourceProvider -ListAvailable | Select-Object ProviderNamespace, RegistrationState | We vragen in PowerShell de lijst van Resource Providers op. |

Project 7

Zie voorgaande projecten

Project 8

Zie voorgaande projecten

Project 9

Websites

|  |  |
| --- | --- |
| https://www.eve-ng.net/index.php/download/#DL-WIN | Download wireshark paackage |
| lin-server01.westeurope.cloudapp.azure.com | Open eve-ng in een webbrowser |
| service ssh restart | Restart ssh service. |

Commando’s

|  |  |
| --- | --- |
| sed -i -e 's/GRUB\_CMDLINE\_LINUX\_DEFAULT=.\*/GRUB\_CMDLINE\_LINUX\_DEFAULT="net.ifnames=0 noquiet"/' /etc/default/grub | We configureren de boot loader (grub). |
| update-grub | Update grub. |
| Reboot | Reboot server. |
| get - http://www.eve-ng.net/repo/install-eve.sh | We downloaden het eve-ng installatiebestand. |
| ./install-eve.sh | We voeren het installatiebestand uit. |

Cisco commando’s

|  |  |
| --- | --- |
| Enable | Enter privilege mode. |
| Configure terminal | Enter configuration mode. |
| Crypto key generate rsa | Configureer SSH. |
| Write | Safe configuratie |
| int e0/0  shutdown | We deactiveren e0/0. |
| logging 10.0.0.6 | We configureren op de eve-ng devices. |
| Ip name-server 8.8.8.8 | we configureren de Google DNS server als onze DNS server. |
| Which sysctl | Note: sysctl wordt gebruikt voor kernel processen. Port forwarding is een kernel proces. |

Project 10

Zie voorgaande projecten

Project 11

Commando’s

|  |  |
| --- | --- |
| which rsyslogd | We vragen de PATH variabele van syslog op. |
| rsyslogd -v | We vragen de syslog versie op. |
| systemctl status rsyslog | We controleren de syslog status. |
| service rsyslog restart | We herstarten de syslog service. |
| netstat -tulnp4 | grep 514 | We vragen de lijst van actieve TCP en UDP poorten op en filteren op 514. |
| which iptables | Iptables welke ip’s hebben toegang |
| $rule1 = New-AzNetworkSecurityRuleConfig -Name ssh-rule -Description "Allow SSH"` -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix ` Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 22 |  |
| $rule2 = New-AzNetworkSecurityRuleConfig -Name web-rule -Description "Allow HTTP" ` -Access Allow -Protocol Tcp -Direction Inbound -Priority 101 -SourceAddressPrefix ` Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 80 |  |
| $rule3 = New-AzNetworkSecurityRuleConfig -Name telnet-rule -Description "Allow Telnet" ` -Access Allow -Protocol Tcp -Direction Inbound -Priority 102 -SourceAddressPrefix ` Internet -SourcePortRange \* -DestinationAddressPrefix \* -DestinationPortRange 32769-32869 |  |
| New-AzNetworkSecurityGroup -Name security-lin01 -ResourceGroupName test-student -Location 'West Europe' -SecurityRules $rule1, $rule2, $rule3 | We maken een NSG aan met de access-list regels die we hierboven hebben aangemaakt |
| New-AzVM -image lin-server01-image -Name eve-ng -DomainNameLabel lin-server01 -ResourceGroupName test-student -Size Standard\_D2s\_v3 -SecurityGroupName security-lin01 -Credential $mylogin | We maken een VM aan. In de string verwijzen we naar de variabelen die we hierboven hebben aangemaakt. We geven ook het subnet van de VM op. |

Hostfile

|  |
| --- |
| 10.0.0.100 R1 |
| 192.168.1.2 R2 |
| 192.168.3.2 R3 |

In rsyslog moeten we 4 regels enablen namelijk:

|  |  |
| --- | --- |
| module(load="imudp") | laad de UDP module |
| input(type="imudp" port="514") | enabled poort 514 voor UDP verkeer |
| module(load="imtcp") | laad de TCP module |
| input(type="imtcp" port="514") | enabled poort 514 voor TCP verkeer |

Project 12

Zie voorgaande projecten

Project 13

Zie voorgaande projecten

CMD

|  |  |
| --- | --- |
| ipconfig /all | We vragen het IP- en MAC adres op van de local host en het IP  adres van de local gateway. |
| arp /g 192.168.178.1 | We vragen op de local host de ARP cache op en achterhalen het  MAC adres van de local gateway. In mijn voorbeeld is het IP  adres van mijn local gateway 192.168.178.1. |
| Arp -n | We vragen het MAC adres op van de Azure gateway. We openen de  ARP cache van de Kali Linux server. |

Project 14

WireShark Commands

|  |  |
| --- | --- |
| Interface | Interfaces waarop we kunnen capturen |
| Traffic | Verkeers grafiek (activiteit) |
| (Data)Link-Layer Header | Laag 2 protocol (OSI) dat wordt gecaptured |
| Promiscuous | Al het verkeer dat arriveert op de interface (NIC) wordt gecaptured. Dit geldt ook voor verkeer dat niet voor de interface bestemd is. |
| Snaplen (B) | De maximale hoeveelheid data dat per frame wordt gecaptured uitgedrukt in Bytes |
| Buffer (MB) | Geheugenbuffer. Default is 2 MB |
| Monitor Mode | We capturen al het verkeer in de omgeving, niet alleen verkeer dat op de interface arriveert |
| Capture filter | Capture filter |
| host <IP>, <domain name> | source or destination |
| port <number> | source or destination |
| src <IP>, <domain name> | Source |
| dst <IP>, <domain name> | Destination |
| src port <Port> | Source |
| dst port <Port> | Destination |
| and | samenvoegen van filters |
| not | uitsluiten van verkeer |

|  |  |
| --- | --- |
| ip.addr == <IP> | source or destination |
| ip.src == <IP> | source |
| ip.dst == <IP> | destination |
| <protocol> | source or destination |
| tcp.port == <port> | source or destination |
| udp.port == <port> | source or destination |
| tcp.srcport == <port> | source |
| udp.srcport == <port> | source |
| tcp.dstport == <port> | destination |
| udp.dstport == <port> | destination |
| !() | source or destination |
| tcp contains <tekst> | source or destination |
| udp contains <tekst> | source or destination |
| or | n.v.t. |
| and | n.v.t. |

Project 15