

Type to search

Total OSCP Guide

Introduction

The Basics

Linux

Basics of Linux

Bash-scripting

Vim

Windows

Basics of Windows

PowerShell

PowerShell Scripting

CMD

Scripting With Python

Python Fundamentals

Useful Scripts

Transferring Files


Transferring Files on Linux






Transferring files on Windows

Firewalls

General tips and tricks

Recon and Information Gathering Phase

 Powered by **GitBook**



Privilege Escalation Windows

We now have a low-privileges shell that we want to escalate into a privileged shell.

Basic Enumeration of the System

Before we start looking for privilege escalation opportunities we need to understand a bit about the machine. We need to know what users have privileges. What patches/hotfixes the system has.

```
# Basics
systeminfo
hostname

# Who am I?
whoami
echo %username%

# What users/localgroups are on the machine?
net users
net localgroups

# More info about a specific user. Check if user has priv:
net user user1

# View Domain Groups
net group /domain
```