

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

Passive Information Gatherig

Identify IP-addresses and Subdo...

Identify IP-addresses

Find Subdomains

DNS Basics

Finding subdomains

DNS Zone Transfer Attack

Identifying People

Search Engine Discovery

Identifying Technology Stack

Active Information Gathering

Port Scanning

Vulnerability analysis

Server-side Vulnerabilities

Common ports/services and how...

Port Knocking



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 privileges.

net user user1


# View Domain Groups

net group /domain


# View Members of Domain Group

net group /domain <Group Name>


# Firewall

netsh firewall show state

netsh firewall show config


# Network

ipconfig /all

route print

arp -A


# How well patched is the system?

wmic qfe get Caption,Description,HotFixID,InstalledOn
```

Cleartext Passwords

Search for them

```
findstr /si password *.txt

findstr /si password *.xml
```