System Information

Since we will be working with many different Linux systems, we need to learn the structure and the information about the system, its processes, network configurations, users, directories, user settings, and the corresponding parameters. Here is a list of the necessary tools that will help us get the above information. Most of them are installed by default.

Command	Description
`whoami`	Displays current username.
`id`	Returns users identity
`hostname`	Sets or prints the name of current host system.
`uname`	Prints basic information about the operating system name and system hardware.
`pwd`	Returns working directory name.
`ifconfig`	The ifconfig utility is used to assign or to view an address to a network interface and/or configure network interface parameters.
`ip`	Ip is a utility to show or manipulate routing, network devices, interfaces and tunnels.
`netstat`	Shows network status.
`ss`	Another utility to investigate sockets.
`ps`	Shows process status.
`who`	Displays who is logged in.
`env`	Prints environment or sets and executes command.
`lsblk`	Lists block devices.
`lsusb`	Lists USB devices
`lsof`	Lists opened files.
`lspci`	Lists PCI devices.

Let us look at a few examples.

Hostname

The `hostname` command is pretty self-explanatory and will just print the name of the computer that we are logged into

Hostname

```
amit8986@htb[/htb]$ hostname

nixfund
```

Whoami

This quick and easy command can be used on both Windows and Linux systems to get our current username. During a security assessment, we obtain reverse shell access on a host, and one of the first bits of situational awareness we should do is figuring out what user we are running as. From there, we can figure out if the user has any special privileges/access.

Whoami

```
cry0l1t3@htb[/htb]$ whoami

cry0l1t3
```

Id

The `id` command expands on the `whoami` command and prints out our effective group membership and IDs. This can be of interest to penetration testers looking to see what access a user may have and sysadmins looking to audit account permissions and group membership. In this output, the `hackthebox` group is of interest because it is non-standard, the `adm` group means that the user can read log files in `/var/log` and could potentially gain access to sensitive information, membership in the `sudo` group is of particular interest as this means our user can run some or all commands as the all-powerful `root` user. Sudo rights could help us escalate privileges or could be a sign to a sysadmin that they may need to audit permissions and group memberships to remove any access that is not required for a given user to carry out their day-to-day tasks.

Id

```
cry0l1t3@htb[/htb]$ id

uid=1000(cry0l1t3) gid=1000(cry0l1t3) groups=1000(cry0l1t3),1337(hackthebox),4(adm),24(cdrom),27(sudo),30(dip),46(pl
```

Uname

Let's dig into the `uname` command a bit more. If we type `man uname` in our terminal, we will bring up the man page for the command, which will show the possible options we can run with the command and the results.

Uname

```
UNAME(1)                                User Commands                                UNAME(1)

NAME
       uname - print system information

SYNOPSIS
       uname [OPTION]...

DESCRIPTION
       Print certain system information.  With no OPTION, same as -s.

       -a, --all
              print all information, in the following order, except omit -p and -i if unknown:

       -s, --kernel-name
              print the kernel name

       -n, --nodename
              print the network node hostname

       -r, --kernel-release
              print the kernel release

       -v, --kernel-version
              print the kernel version

       -m, --machine
              print the machine hardware name

       -p, --processor
              print the processor type (non-portable)

       -i, --hardware-platform
              print the hardware platform (non-portable)

       -o, --operating-system
```

Running `uname -a` will print all information about the machine in a specific order: kernel name, hostname, the kernel release, kernel version, machine hardware name, and operating system. The `-a` flag will omit `-p` (processor type) and `-i` (hardware platform) if they are unknown.

Uname

```
cry0l1t3@htb[/htb]$ uname -a

Linux box 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

From the above command, we can see that the kernel name is `Linux`, the hostname is `box`, the kernel release is `4.15.0-99-generic`, the kernel version is `#100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020`, and so on. Running any of these options on their own will give us the specific bit output we are interested in.

Uname to Obtain Kernel Release

Suppose we want to print out the kernel release to search for potential kernel exploits quickly. We can type `uname -r` to obtain this information.

Uname to Obtain Kernel Release

```
cry0l1t3@htb[/htb]$ uname -r

4.15.0-99-generic
```

With this info, we could go and search for "4.15.0-99-generic exploit," and the first result immediately appears useful to us.

It is highly recommended to study the commands and understand what they are for and what information they can provide. Though a bit tedious, we can learn much from studying the manpages for common commands. We may even find out things that we did not even know were possible with a given command. This information is not only used for working with Linux. However, it will also be used later to discover vulnerabilities and misconfigurations on the Linux system that may contribute to privilege escalation. Here are a few optional exercises that we can solve for practice purposes, which will help us become familiar with some of the commands.

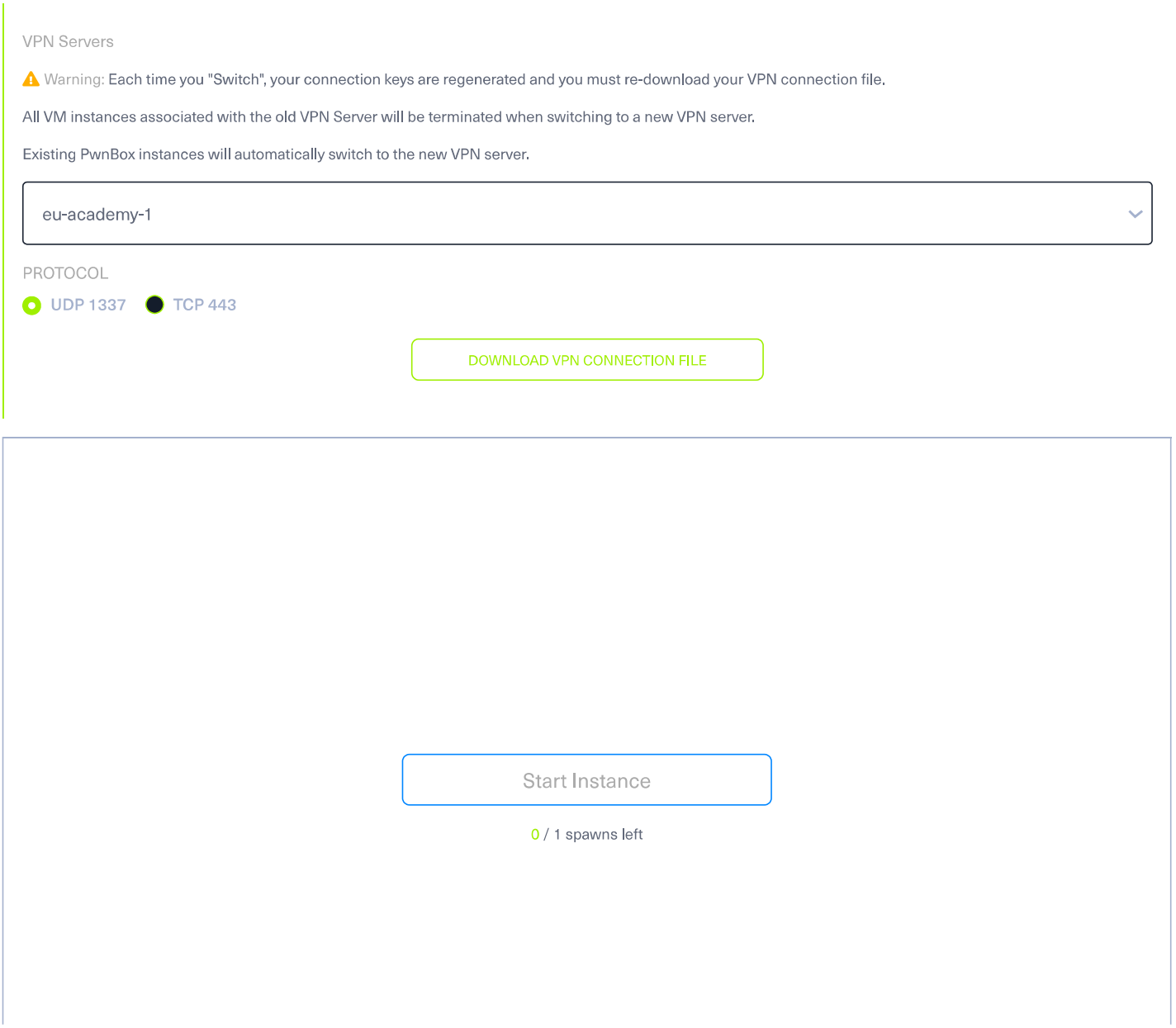
Logging In via SSH

`Secure Shell` (`SSH`) refers to a protocol that allows clients to access and execute commands or actions on remote computers. On Linux-based hosts and servers running or another Unix-like operating system, SSH is one of the permanently installed standard tools and is the preferred choice for many administrators to configure and maintain a computer through remote access. It is an older and very proven protocol that does not require or offer a graphical user interface (GUI). For this reason, it works very efficiently and occupies very few resources. We use this type of connection in the following sections and in most of the other modules to offer the possibility to try out the learned commands and actions in a safe environment. We can connect to our targets with the following command:

SSH Login

SSH Login

```
amit8986@htb[/htb]$ ssh [username]@[IP address]
```



Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

Cheat Sheet

Download VPN Connection File

SSH to with user "htb-student" and password "HTB_@cademy_stdnt!"

+ 0 Find out the machine hardware name and submit it as the answer.

Submit your answer here...

Submit Hint

+ 1 What is the path to htb-student's home directory?

Submit your answer here...

Submit

+ 0 What is the path to the htb-student's mail?

Submit your answer here...

Submit

+ 0 Which shell is specified for the htb-student user?

Submit your answer here...

Submit

+ 0 Which kernel version is installed on the system? (Format: 1.22.3)

Submit your answer here...

Submit

+ 1 What is the name of the network interface that MTU is set to 1500?

Submit your answer here...

Submit