# PWN Challenge #1

Read this entire document carefully as it contains important details about the challenge.

The objective of this challenge is to utilize the tools and techniques you have been taught to discover and exploit discovered hosts within the authorized scope.

To get credit for the assignment you will be required to create an assessment report. The report should contain your findings along with their associated impact. It should also create context for your customer (your instructors) so that informed decisions can be made for remediation. Your report should contain any hash values and include enough detail that your results could be reproduced by your instructors.

Anti-cheating – Screenshots of key steps should include:

- your name
- date and time

The following commands will print the required information into the command prompt and should be performed before or after the successful attack step

Windows Command Line:

```
> echo Mike Cook %date% %time%
```

Linux Terminal:

```
# echo Mike Cook; date
```

The scope listed in your ROE is: **10.20.160.10-150**
**10.20.170.20-100**

To access this assignment:

1. Login to STEPfwd
2. Click on the "EPT Penetration Testing (EPT)" course link.
3. Expand Week 3 and click on the "EPT-PWN Challenge 1" link.

Each machine within the authorized scope has proof documents containing hash values. The "proof.txt" documents are typically located on the desktop of the vulnerable machine.

It is recommended that you take thorough notes and screenshots of all your activities. This will assist you in creating a top notch report (and a good grade).