# Information

You have the following tools at your disposal to complete the exercises.

* A PCW (Pretty Crappy Web) server (10.1.12.220)
* A CTF (Capture the Flag) server (10.1.12.221)
* Wi-Fi network: ssid=ASU-CTF; password=challenge2016
* Kali Linux Toolkit (10.1.12.2##) – Where # is your team number.
* VNC Viewer to connect to your Kali Linux host. The password is “challenge” (without quotation marks). You will connect to display #1.  
  (e.g. 10.1.12.2xx:1)

Terra Verde personnel are available if you get stuck. They can provide hints, but the first FOUR hints will cost you 20% of the total possible points for that exercise!

Thank you for participating and good luck!

# PCW Exercise 1: Brute Force Score \_\_\_\_/20 Points

## Background

You have been tasked with performing a Brute Force attack against the Web Server (10.1.12.220). Your mission, should you choose to accept it, is to do as many of the items listed below as possible.

* You will log into the PCW server
  + server: **10.1.12.220**
  + user: **ctf**
  + password: **challenge**
* Set your difficulty level.
* Navigate to the “Brute Force” page of the Web Server

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* PCW server (10.1.12.220)
* Your Kali Linux toolkit (10.1.12.2##) where ## is your team number

|  |  |
| --- | --- |
| 1) Find a valid user/password combination.  Smitty / password | Score \_\_\_\_/10 Points |
|  |  |
| 2) Log in to the password protected are of the web server.  “Welcome to the password protected area, Smithy” | Score \_\_\_\_/10 Points |

# PCW Exercise 2: Command Injection Score \_\_\_\_/30 Points

## Background

You have been tasked with attempting a command injection into a form that was designed to execute the ping command. Your mission, should you choose to accept it, is to do as many of the items listed below as possible.

* You will log into the PCW server
  + server: **10.1.12.220**
  + user: **ctf**
  + password: **challenge**
* Set your difficulty level
* Navigate to the “Command Injection” page of the Web Server

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* PCW server (10.1.12.220)
* Kali Linux Toolkit

|  |  |
| --- | --- |
| 1. List the contents of the /etc/passwd file. | Score \_\_\_\_/10 Points |
|  |  |
| 2) Copy the /etc/passwd file to the tmp directory and name the file with your team number and name (e.g. 1-team-awesome-PCW-2).  VIEW FILE IN /TMP | Score \_\_\_\_/10 Points |
|  |  |
| 3) Start a netcat listener on port 88XX on the PCW server (where XX is your team number) and connect to it from your Kali box .  netcat -l 88xx netcat IP 88xx  send test msg. | Score \_\_\_\_/10 Points |

# PCW Exercise 3: File Inclusion Score \_\_\_\_/10 Points

## Background

File inclusion is the “art” of viewing file contents on a server. Your mission, should you choose to accept it, is to list the contents of /etc/passwd using the technique of File Inclusion

* You will log into the PCW server
  + server: **10.1.12.220**
  + user: **ctf**
  + password: **challenge**
* Set your difficulty level.
* Navigate to the “File Inclusion” page of the Web Server.

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* PCW server (10.1.12.220)
* Ssh/putty

|  |  |
| --- | --- |
| 1) Output the contents of /etc/passwd. | Score \_\_\_\_/10 Points |
|  |  |

# PCW Exercise 4: File Upload Score \_\_\_\_/20 Points

## Background

Your task is to upload a payload you can then execute on the server. Your mission, should you choose to accept it, is to do as many of the items listed below as possible.

* You will log into the PCW server
  + server: **10.1.12.220**
  + user: **ctf**
  + password: **challenge**
* Set your difficulty level.
* Navigate to the “File Upload” page of the Web Server

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* PCW server (10.1.12.220)

|  |  |
| --- | --- |
| 1) Upload a file (use your team # and name) that will output the contents of /etc/group. Determine the location of the file. Record your answer below  \_\_\_\_\_\_/dvwa/hackable/uploads/\_\_\_\_\_\_\_\_\_\_\_ | Score \_\_\_\_/10 Points |
|  |  |
| 2) Execute the file and show your output to a Terra Verde helper for scoring. | Score \_\_\_\_/10 Points |
| Depends on script uploaded |  |
|  |  |

# PCW Exercise 5: SQL Injection Score \_\_\_\_/20 Points

## Background

SQL injection is a very real problem in online databases. Your mission, should you choose to accept it, is to do as many of the items listed below as possible.

* You will log into the PCW server
  + server: **10.1.12.220**
  + user: **ctf**
  + password: **challenge**
* Set your difficulty level.
* Navigate to the “SQL Injection” page of the Web Server

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* PCW server (10.1.12.220)
* Kali Linux toolkit

|  |  |
| --- | --- |
| 1) Determine the name in record #1 of the database.  Admin/admin | Score \_\_\_\_/10 Points |
|  |  |
| 2) Determine the type of database system Installed on this host.  Mysql (verify output, not just their word/guess) | Score \_\_\_\_/10 Points |
| **UNION ALL SELECT @@datadir, 1 --** |  |
|  |  |

# CTF Exercise 1 – Don’t be DATED! Score \_\_\_\_/50 Points

## Background

The SSH password for the level2 user is located in /home/level2/.password. Figure out what you have to do to read that file. There's a scratch directory for you in /tmp

* You will log into the CTF server
  + server: **10.1.12.221**
  + user: **level1**
  + password: **iStP1w1jkGou**
* Follow the directions on the screen.

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* CTF server (10.1.12.221)
* Kali Linux toolkit

|  |  |
| --- | --- |
| 2) What is the password for level2?  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_nNP0nBOwFtja\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Score \_\_\_\_/50 Points |
|  |  |

# CTF Exercise 2: Cookie Monster! Score \_\_\_\_/100 Points

## Background

Log onto the server with level 2 username and the password to get started. Same deal here as in the previous level, the password is in /home/level3/.password, for the next one. This time you're faced with a web-based vulnerability, you'll need to direct your browser to /level2.php on this server. You'll need to provide the password

for level2 using HTTP digest authentication.

* You will log into the CTF server
  + server: **10.1.12.221**
  + user: **level2**
  + password: **flag obtained in CTF Exercise 1**
* Follow the directions on the screen.

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* CTF server (10.1.12.221)

|  |  |
| --- | --- |
| 1) Obtain the password of the flag3 user.  1kAcQgwR2E6P | Score \_\_\_\_/100 Points |
|  |  |

# CTF Exercise 3: Overflow! Score \_\_\_\_/200 Points

## Background

The password for the next level is in /home/level4/.password. As before, you may find /levels/level3 and /levels/level3.c useful. While the supplied binary mostly just does mundane tasks, we trust you'll find a way of making it do something much more interesting.

* You will log into the CTF server
  + server: **10.1.12.221**
  + user: **level3**
  + password: **Flag obtained by completing level2**
* Follow the directions on the screen.

When you have completed your exercise, provide the results to one of the Terra Verde helpers for scoring.

## Components

* CTF server (10.1.12.221)
* SSH/putty
* gdb
* Text viewer (optional)

|  |  |
| --- | --- |
| 1) Obtain the flag password:  pECROq065B52 or theflagIEfcD2a5ByzBy1d4qUFi? | Score \_\_\_\_/200 Points |