** DO NOT USE THE SKILLS/TOOLS COVERED IN THIS LECTURE/HW FOR ANY UNAUTHORIZED ACTIVITY. These skills/tools should only be used on environments/systems that you own or have explicit permission to do so. **

HW12 - Penetration Testing and Ethical Hacking

Objectives

This exercise provides experience on:

- Scanning a server endpoint
- Exploiting common system vulnerabilities
- Performing tasks yielding privilege escalation

Prerequisites

- Attend the Week 12 lecture and participate in corresponding in-class activities.

Deliverables

- PDF report (**100 points**): Provide a “high-resolution,” “sparse-segment” **instructional report** on how you were able to gain access to the server. (For future reference, note that this approach is similar to a NetSec style report)
    - High-resolution: Each “step” consists of **one** committal action. e.g.,
        - Opening a file or clicking ‘`OK`’ or `Next`
        - Populating and saving configuration file changes
        - Typing a CLI command and pressing enter
    - Sparse-segment: Per each step:
        - *One* 1-2 sentence description of the step.
        - An **In-report** (typed out) copy of CLI command or configuration language used where applicable (so your audience can cut/paste).
        - *One* **well-cropped, bordered** screenshot matching the description (and showing typed commands where applicable)
            - Do not provide the entire screen in screenshots.

    - Provide well-written step-by-step instructions (**60 points**)
        - Flags for `root` and `user` (in the respective home directories) (**10 points** each)
        - Instructions leading to achieving `user` login (**20 points**)
        - Instructions leading to achieving `root` login (**20 points**)
    - Provide clear screenshots on each step you took to exploit the server (**40 points**)
        - Screenshots for achieving `user` login (**20 points**)
        - Screenshots for achieving `root` login (**20 points**)

** DO NOT USE THE SKILLS/TOOLS COVERED IN THIS LECTURE/HW FOR ANY UNAUTHORIZED ACTIVITY. These skills/tools should only be used on environments/systems that you own or have explicit permission to do so. **

Task Details

Kali device credentials: `kali:toor`
Target server IP: `10.43.X.253`

Report Instructions

- There is a webserver running on a common port, you must chain together a couple of vulnerabilities to gain user access to the server.
- Once you have user access you must escalate your privileges to `root`.
- There will be two `flag.txt` files, each containing a hash, please find and include these in your report.
- Please refer to slides 23, 34, and 35.

Populate a step-by-step report explaining how you were able to gain access to the server. The report must be detailed enough so a person with basic computer skills can reproduce what you did *exactly*. You don't have to describe your thought process; just explain what you did to gain access.

- *Don't* include what you had to google or other external research you may have done.

- *Don't* include figure numbers or captions for this style of report. The description is sufficient.

- *Do* follow **UBNetDef Instructional Report Style Guide** instructions on formatting for readability (e.g., use alternate fonts to distinguish `commands` from instructions).

- *Do* use high-contrast

  shapes

  …to highlight CLI command entries or mouse-click targets per-step.

- *Do* include the process of doing a `nmap` scan and running other recon tools on the server.

- You do *not* have to include every recon tool you run; only include tools that lead to exploitation.
  - E.g., if `nikto` didn't return anything useful for exploitation of the server, you may omit `nikto`. However if `sqlmap` did give you important information on exploiting the server, include `sqlmap` in your report.

- Make sure you include a screenshot for each step you took for the exploitation! Include only relevant steps that lead to exploitation.

Assignment continues on next page

Example Report Content

The report should look similar to example contents below:

First, run `nmap` against the target system:
`nmap -sV -sC -oN test.txt -p- 192.168.1.1`
[Screenshot with shape highlighting command and command output]
--

Open a browser (FireFox (FF) is used for this example)
[Screenshot of opening FF browser]
--

Next, notice that a webserver is running on port 8080. Navigate to port 8080 in the browser.
`http://192.168.1.1:8080`
[Screenshot of webpage with shape highlighting URL]
--

Note that the home URL was vulnerable to an `lfi` injection.
[Type out command executing `lfi` injection]
[Screenshot showing the `lfi` injection vulnerability with shape highlighting the command]
--

Leverage this vulnerability to read a file from user `shrek`'s desktop.
`http://homepage/../../../../../home/shrek/password.txt`
[Screenshot of the password file with shape highlighting the URL]
--

… and so on