SysSec Final Project!

Here is the situation...

James (@james) and Aaron (@aaron) are two entrepreneurs with a bold idea. They want to deploy “Catflix” a website that streams thousands of 4k quality cat videos. They have purchased your services, and want you to build them a network for their start-up. They need a database for their cat videos. A webserver to run their new and cool website. A Windows client to talk to customers and Windows Server with Active Directory to manage the client. They also will need a router to setup a Furwall, I mean Firewall. And lastly they will need a Linux client to SSH into the database and webserver and well Linux is cool. And you have been HIRED! However you only have to do some of this network, the rest they hired RIT to make.

Part I - Topology (10 pts)

Just like the previous assignments, we need a topology, below is an example. Depending on the route you take your topology won't be very big. Be creative!

Part II - Windows + Linux (60 pts)

Here is the overview of Windows(30 pts), Linux(30 pts) and Firewall setup that you will need to perform:

Windows (Active Directory)

- 1 Windows client (10 ONLY)
- Windows Server (2016 or 2019), this will be your Domain Controller
    - follow the Windows homework, set up the same stuff (users, groups, GPO)
- Creds: Username - Admin/Administrator, Password: - Change.me!

Linux (LAMP Stack)

- Set up MediaWiki using the same workflow as the Services homework.
- Hosts (3, all on the DMZ):
    - Linux Desktop Client with GUI (so you can check your website)
    - CentOS Database supporting MariaDB hosting data for MediaWiki
    - Linux (Web) Webserver: Apache, PHP, MediaWiki
- Credentials: Reflect all machine UIDs AND the resulting MediaWiki site.
    - Username - sysadmin, Password: - changeme
- Evaluation: A SecDev grader will use the above credentials to create their own page on your

device.
    - If your installation is successful, the grader's created page will persist on your MediaWiki.

pfSense vs Palo Alto pfSense as router OR Palo Alto, if you choose Palo Alto you get 20 pts of extra credit on the assignment. Please let @aibek know if you would like Palo Alto. By default, you will get pfSense

Part III - Risk (30 pts)

Use what you learned in the Risk Management lecture and Choose 5 Technical controls you learned in the Risk Management lecture and implement these into your environment. These controls must come from the CIS top 20 control list: https://www.cisecurity.org/controls/cis-controls-list/

You must submit proof of your Implementation (Screenshot is fine). In a two to three page paper summarize the 5 controls that you have implemented. In this paper please summarize the specific control, what risk(s) is being mitigated (for each control implemented), and why CatFlix will benefit from this implementation.

If you decide to implement any sort of inventory list please submit this as an excel sheet/word document with a table in it.

Examples of technical controls to implement [Controls - Evidence]:

- **Hardware Inventory list** - You can just submit your **topology** for this. Normally this is done with a Table (Columns for the table: Asset Name, Asset Category, IP-Address, MAC Address, Operating System) (Also include NMAP output as proof)
- **Software Inventory List** - Table (Columns for the table: Software Name, Software Category, Main Use, List of assets where software was implemented) - Just list any software that you installed on the system. Just list anything that is not a default app. (Example: do not list internet explorer, but list Google Chrome)
- **Controlled use of Admin Privileges**- Screenshot what admins are on a particular system.
- **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** - provide proof that you hardened a certain aspect of your system (example: SSH config file set to reject logins after X failed attempts)
- **Maintenance, Monitoring, and Analysis of Audit Logs** - Provide a screenshot of 3 log files (Actually open the files)
- etc... Reach out to Jay if you are unsure about anything!

Part IV - Deliverable

Submit one PDF on homework.ubnetdef.org. If you have multiple PDFs you can use https://combinepdf.com/

Important:

Do not create a whole report for Part II, all we need is screenshots of...

- the static IP on all VMs

- LAN/WAN and DMZ configuration in pfSense or Palo Alto
- service working and running as you did in the previous assignment, each route will be about 10 screenshots in total for all of this
- **ENSURE TO ADD ALL CREDENTIALS INTO THE SUBMISSIONS, SO THAT SECDEV IS ABLE TO CHECK YOUR WORK**

As usual, if you have any questions please ask in the `System Security` channel!