Final Project Demo

Nina Gadelha

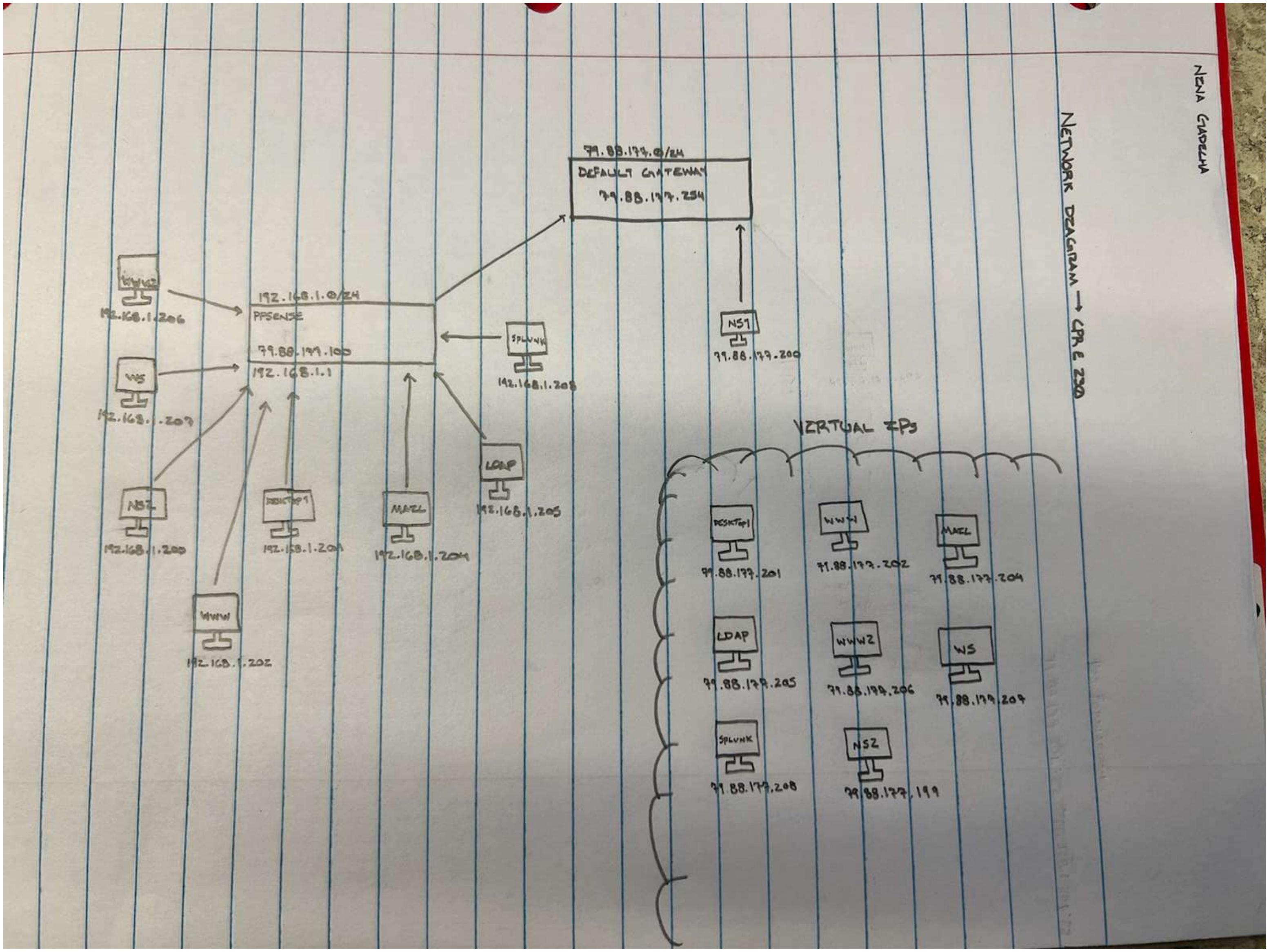
Identify the vulnerability	What harm could it do?	How to fix it
1. Users are able (when it comes to permissions of files), are able to read /etc/shadow (which contains sensitive information). No one should have access to this file!	Allowing others to have access to this file could allow the hacker to obtain sensitive information. If they are able to view this file (/etc/shadow), they can obtain the needed information to decrypt all user's passwords (which algorithm is used to encrypt their passwords, salt value, encrypted password).	In order to fix this, you run the command to restore the default permissions of the /etc/shadow file. *Chmod 000 'filename'* ^^ Owner, Group and Other can not read, write or execute
2. There is a user "backdoor" (shown in /etc/passwd file) that is listed as a root user (has sudo privileges). Logging into the 'backdoor' account, we can see they have access to information they should not.	A "root" user likely has access to anything and everything within this machine. This user has access to all commands and files (some like /etc/shadow, which have sensitive info). If an unknown/unwanted user has root permissions, they can obtain information to change, keep or sell. The root user should be 'the one in charge', someone who actually has authorization to see information.	One method to change this issue is through the /etc/shadow file. In that file, you can change the root user's shell. This can be achieved by changing *:/root:/bin/bash* to *:/root:/sbin/nologin*. After being saved, the next time the root user attempts to login, they will receive an error message.
3. Currently, the VM is open on port 21, which uses protocol FTP. FTP is an unsecure way of transferring files, it does not use encryption, leaving your data to be potentially exposed.	FTP does not use encryption when sending/receiving files. This means, a hacker could see all information in files being sent using FTP protocols. This is due to plaintxt (unencrypted text) being allowed under FTP. Wire-sharking into current transfers of files using FTP, we can see the plaintxt is exposed for other to obtain (passwords, bank info, company stats).	This issue can be solved by changing the use from FTP to FTPS (port 990). FTPS uses encryption, meaning the data in the files will no longer be displayed as plaintxt, rather an encryption of the raw data. This can be achieved by updating ufw rules or using pfsense to create new firewall rules.
4. CVE-2011-2767: This is an exploit that can be used by hackers to infiltrate and jeopardize the integrity of a webservice. Using this CVE, a hacker can write to a user's .htaccess file, causing them to compromise the integrity of certain webservice(s).	A user's .htaccess file can be accessed and changed by an attacker. A .htaccess file is a configuration file, used for configuration of website-access issues. If an attacker is allowed to change the contents of this file, they could possibly redirect any/all traffic (aimed to go to original website) to a malicious/harmful site (changing ip in .htaccess file). The hacker can then use some other tricks to obtain your information through their harmful website (could make the new webpage look exactly like the real one so user will trust it, ask them to enter personal info, steal info). Exploitability Score is rated anywhere between a 9.8 and 10.	Since the release of this bug, the only current solution is a patch. The patch contains the fix to only allow access to certain sections (such as the .htaccess file) to be obtained through the server configurations, rather than through directories (how hackers were able to access this file). This will stop attackers from being able to change the integrity of the file.

5. The capstone machine is currently using HTTP to transfer information. HTTP is not secure, so all the data being sent can be read by unwanted eyes.	HTTP does not use encryption when sending data. This means, any/all information that is sent through HTTP is at risk to being exposed. The attacker can simply read the text as it was typed, displayed to them in plaintxt. No encryption of data/protection of information is given when using HTTP.	Switching from HTTP to HTTPS will ensure the safety of transferred information. HTTPS uses encryption, this means any information exchanged is encrypted (not displayed in plaintxt). You can switch the protocols by adding ufw and/or pfsense rules.
6. When attempting to login to ip address website (through desktop), login/password can be ‘passed by’ by using SQL injection (password’ OR ‘1’ = ‘1).	SQL injection can be a serious security threat, as it can be used to obtain sensitive information. If a user is able to bypass the login (username and password) of a website, they are able to gain any/all access to any info that the real user has authorization to view. Bank numbers, sensitive work data, personal information can all be accessed when a website is susceptible to SQL injection.	One way to prevent it is to use parameterized queries instead of string concatenation. This way, the user input is not concatenated DIRECTLY, making it harder for the attacker to obtain sensitive info. The user must ensure they sanitize/filter data. (Sanitizing: removing data from device, ensuring it can’t be recovered).
7. Several of the listed users (tom, toor, jry, alice) have bad passwords. All of their passwords are short in length and not complex enough; some even have their username and password as the same thing!	Bad passwords make it easier for attackers to crack. The attackers would have an easier shot at decrypting your password due to its ease and/or lack of length/complexity (algorithm used to crack will run faster). Once they obtain your password, they would be able to login into your account and gain access to any/all information you have access to on the system.	One command to use is*: passwd –expire ‘username’*. This will force their current password to expire (at time of command run). This means, the next time the user attempts to answer, they will be faced with a prompt to enter a new password. You could also use the ‘chage’ command: *chage –lastday 0 usernam*’. This will do the same thing, force the user to change their password next time they attempt to login.

Please draw a network diagram illustrating the comprehensive network infrastructure established over the semester. This diagram should resemble Lab 4's layout but should provide a thorough depiction of the network, including each configured machine placed appropriately with their respective services, ports, and IP addresses indicated.

- All network resources must be assigned an IP address.
- Any necessary port forwarding should be annotated on the Firewall/NAT (excluding UFW firewall rules).
- The LDAP workstation and the Kali Box do not need to be included.
- Ensure the inclusion of virtual IP port forwarding within the diagram.

Network Diagram



Port Forwarding for Network Diagram

Pfsense NAT/Firewall Rules

79.88.177.201:22 → 192.168.1.201:22	(ssh)
79.88.177.199:53 → 192.168.1.199:53	(dns)
79.88.177.205:389 → 192.168.1.205:389	(ldap)
79.88.177.204:587 → 192.168.1.204:587	(smtp)
79.88.177.204:143 → 192.168.1.204:143	(imap)
79.88.177.204:993 → 192.168.1.204:993	(imap/s)
79.88.177.204:995 → 192.168.1.204:995	(pop3/s)
79.88.177.204:110 → 192.168.1.204:110	(pop3)
79.88.177.202:80 → 192.168.1.202:80	(http)
79.88.177.202:443 → 192.168.1.202:443	(https)
79.88.177.206:8000 → 192.168.1.206:8000	(http servers)
79.88.177.206:22 → 192.168.1.206:22	(ssh)
79.88.177.203:9997 → 192.168.1.208:9997	(slunk)

Virtual IPs

79.88.177.201 → desktop1
79.88.177.202 → www
79.88.177.204 → mail
79.88.177.205 → ldap
79.88.177.206 → www2
79.88.177.207 → ws
79.88.177.208 → splunk
79.88.177.199 → ns2