Final Project Part 2 Template

(Note: the points for each row are given on an all-or-nothing basis. You must properly fill out each column in the row to receive all of the points. Correctly filling out ⅔ of the information earns zero points. Every answer must be adequate to receive full credit for the given row.)

Exploiting three machines (8.3 points per row; 25 **total points**)

Host Machines	**How did you gain access?**	**What specific harm could be done?**	**How can you remediate it?**
Reception Desktop	After scanning the ports and services, I decided on using Metasploit. To be more exact, I used the windows/smb/ms08_067_netapi exploit, since ports 139 and 445 were open and ended up getting root access.	Using this exploit, I was able to get root access, which is the highest privileged account. This means that I could do things like install malware, steal data, manipulate files, spread to other machines in the network, potentially compromising the entire network. Since I also had the possibility to see the hashes for all the users, I could use those to crack the password and try credential stuffing on various systems and even on other desktops, infecting the entire network. Additionally, thanks to my root rights, I could also do things like delete everything on the desktop, this however would be quickly noticeable,	The first step would be to disable the SMBv1 protocol. Patch and update the entire system including getting the latest security updates. Only give users the minimum amount of privileges, so that in case of being exploited, the damage can be minimized. Use different VLANs or subnets for the devices, in order to hinder/slow down the attacker from being able to find other devices one exploited. Configure the Firewall in order not to allow inbound access to ports like 139, 445 or 3389. Only allow the ports

		so another thing that could be done would be to stay hidden as long as possible and steal as much sensitive information as possible. Also could create a backdoor.	that actually needed and use authorized Ips. Use an antivirus. Monitor the logs.
Clinician Desktop	I used the same Metasploit exploit as in the previous Desktop (windows/smb/ms08_067_netapi). Again the Ports 139 and 445 were open, ADDITIONALLY, the desktop was running Windows XP. I ended up getting root access using this exploit.	Using this exploit, I was able to get root access, which is the highest privileged account. This means that I could do things like install malware, steal data, manipulate files, spread to other machines in the network, potentially compromising the entire network. Since I also had the possibility to see the hashes for all the users, I could use those to crack the password and try credential stuffing on various systems and even on other desktops, infecting the entire network. Additionally, thanks to my root rights, I could also do things like delete everything on the desktop, this however would be quickly noticeable, so another thing that	Disable SMBv1. UPDATE THE OS TO WINDOWS 10/11! Windows XP is not safe! Configure the firewall inbound rules to block the ports 139 and 445. Monitor logs. Only give Users the necessary right, nothing more, in order to minimize damage in case of being exploited. Use an Antivirus. Use different VLANs or subnets to hinder/slow down attackers when it comes to lateral moving/exploiting other devices in the same network. Patch and update the device including security updates, bring everything up to

		could be done would be to stay hidden as long as possible and steal as much sensitive information as possible. Also could create a backdoor.	date. (First update to Windows 10/11)
Tom's Project	I was able to login into the website and the desktop using the information Rachel gave me. She mentioned that her cat was named after her favorite ice cream, hence I simply logged in using that information. Next I tried entering various different things in the chat boxes after logging into the website and realized that executing things with <script> worked. How I ultimately got in however, is by carefully looking at the open ports and services again and doing an ftp. I chose anonymous as name and there was no password. Then I had a look at the directories and files and realized that the system already had been compromised. After carefully went through the directories I found a passwd and shadow file, downloaded both and cracked them using john. After that I found a user called "backdoor" who didn't have a password, hence I tried login in with him and it worked. The backdoor also has root rights.	The database can be accessed and the information leaked/stolen and used for things like credential stuffing on other devices in the network or other services. Since I had root rights, I could do whatever I wanted. Modify, delete, add files, add malware, add spyware, create a backdoor etc. I could simply delete everything and all the data in the db would be gone and the webserver/website gone aswell. Hack other devices in the network. Destroy reputation/ modify website to give people visiting it malware	Update and patch everything. Deactivate FTP. Don't give users more rights than they need to minimize damage. From what Ive seen on the database and the information I received from Rachel, USE STRONGER PASSWORD! AND PLEASE NO PET NAMES AS PASSWORD! Monitor the logs, someone already had a backdoor and the ftp I entered was full of sensible files the hacker added. Block unused ports or atleast change the inbound rules! Deactivate Telnet. DELETE THE BACKDOOR AND THE EXPOSED FILES!

Sensitive information (8.3 points per row; **25 total points**)

Host Machines	**What information I found, and why it's bad that I can see it.**
Reception Desktop	- Was able to find some patient reports as well as the report template itself. → Can have consequences for the company, since this can result in privacy lawsuits. Can also result in impersonating, data being sold, leaked, patients losing trust in the company resulting in less patients - Was able to find Toms password → Someone could take this password and do credential stuffing on different services or devices on the network and end up getting access to Toms account - Get Users hashes → Using the hashes, an attacker can crack users passwords and end up being able to log into their accounts and do credential stuffing on other devices - Logs → Can show things like misconfiguration and system errors. Basically reveals the weak points of the system, making the job easier for hackers. - System files and configs → Can give attacker access to things like service configurations, SSH keys, cron jobs etc. This might result in the hacker getting access to even more services, gain more information and make his job easier - Backups → Find unencrypted data, giving the hacker more sensitive information
Clinician Desktop	- Get Users hashes → Using the hashes, an attacker can crack users passwords and end up being able to log into their accounts and do credential stuffing on other devices - Was able to find a lot of patient data, these show information like name, gender, birthdate, emergency contact number, allergies, current medications etc, → Can have consequences for the company, since this can result in privacy lawsuits. Can also result in impersonating, data being sold,

	leaked, patients losing trust in the company resulting in less patients - A file saying “don’t forget password” from scrat → Is hinting that scrat is forgetting his password, which might tell the attacker either that his user does not have a password at all, an easy password or that his password is hidden and accessible somewhere in the device - Logs → Can show things like misconfiguration and system errors. Basically reveals the weak points of the system, making the job easier for hackers. - System files and configs → Can give attacker access to things like service configurations, SSH keys, cron jobs etc. This might result in the hacker getting access to even more services, gain more information and make his job easier - Backups → Find unencrypted data, giving the hacker more sensitive information
Tom’s Project	- Could access the entire database and get information like Username and passwords → Could also result in a privacy lawsuit, patients losing trust and hence less patients, the attacker can also manipulate anything on the database, can delete or crash the entire system if he feels like it or request a ransom. Can be used for credential stuffing again. - Get all users passwords and usernames (not from db, users on the device aswell) → Credential stuffing again, on online services and devices in network - Logs → Can show things like misconfiguration and system errors. Basically reveals the weak points of the system, making the job easier for hackers. - System files and configs → Can give attacker access to things like service configurations, SSH keys, cron jobs etc. This might result in the hacker getting access to even more services, gain more information and make his job easier - Backups → Find unencrypted data, giving the hacker more sensitive information

Remediation (8.3 points per row; **25 total points**)

Host Machines	**Vulnerabilities, misconfigurations, sensitive information disclosures, malpractices**	**Does the issue need to be fixed? Why, or why not?**	**If actions were taken, how did you remediate it**
Reception Desktop	- Patient reports and template exposed - Toms password is saved in plaintext - User hashes accessible → hash cracking and attacker gets passwords - Sensitive logs exposed - Weak passwords - Open SMB ports (139, 445) and hence vulnerable to m08_067 - System and applications might be outdated	YES!!!!!! The data leaks might result in lawsuits and most likely will damage your reputation. Plaintext, weak and reused passwords can lead to successful credential stuffing and brute force attacks. The password hashes make it easy for attackers to get all users login credentials and perform credential stuffing. The Logs as well as open ports and out of date system/applications make it easier for hackers to get into your system.	- Disable SMB - Update and patch softwares/system - Configure firewall to block ports 149, 445 and 3389 - Implement least privilege principle - School workers on how to create strong passwords, not to reuse and not use things like animal names - Use antivirus and monitor logs
Clinician Desktop	- Patient reports exposed - User hashes accessible → hash cracking and attacker gets passwords - Sensitive logs exposed - Weak passwords - Open SMB ports (139, 445) and hence vulnerable to m08_067 - DESKTOP IS USING	YES!!! Windows XP is outdated and insecure, can be exploited easily. The data leaks might result in lawsuits and most likely will damage your reputation. Weak and reused passwords can lead to successful credential stuffing and brute force attacks.	- Disable SMB - Replace Windows XP with Windows 10/11 - Update and patch softwares/system - Configure firewall to block ports 149 and 445 - Implement least privilege principle - School workers on how to create strong passwords, not to reuse and not use things like animal names

	WINDOWS XP!!!!!! - Entire system not up to date	The password hashes make it easy for attackers to get all users login credentials and perform credential stuffing. The Logs as well as open ports and out of date system/applications make it easier for hackers to get into your system.	- Use antivirus and monitor logs
Tom's Project	- Database with information like usernames and passwords Is exposed (file in the webserver contains login information to db) - FTP open and easily accessible using anonymous login without password (Received access to EXTREMLY sensitive files like paswords hashes, vulnerabilities and backdoor) - Telnet is enabled - User called backdoor exist, has root access and no password - JavaScript injection is possible using the chat in the website (after login)	YES!!!!! There is a possibility of the entire system being compromised. FTP and Telnet are major security risks. Currently, in order to get access to the entire system is by using FTP and login in as anonymous and you will be bombarded by EXTREMLY sensitive files which will make it easy to exploit the system. There is a backdoor in the system and as mentioned previously a lot of sensitive information available like the password hashes, vulnerabilities and even the hacker making fun of the system. The Backdoor is a literal user called backdoor with no password and hence easily accessible. Exposed credentials lead to the database being accessed.	- Deactivate FTP and Telnet - Remove backdoor user - Remove all the leaked files which can be accessed easily by FTP - Patch all vulnerabilities - Update system if possible - Implement least privilege principle - School workers on how to create strong passwords, not to reuse and not use things like animal names - Use antivirus and monitor logs - Sanitize inputs in order to prevent JavaScript Injection - Move the db credentials out of the public directory - Add firewall restrictions

	- Sensitive logs exposed - Credentials for db login easily accessible	JavaScript injection on the website will lead to big issues.	

Incident Response Table (8.3 points per row; **25 total points**)

Some potential hints of things that might be good to look for include:

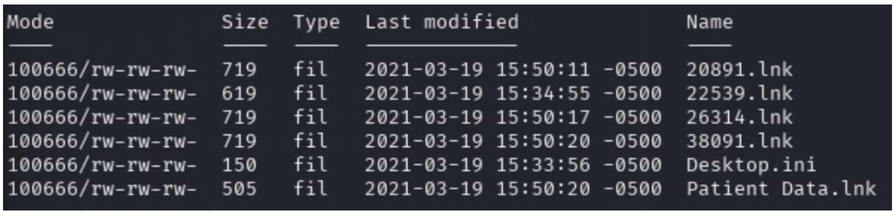
- .158 (ems_laptop), do you notice any new users / files?
- .154 (clinician desktop), same as 158, but also look through logs for suspicious connections.
- .150 (www) Look for signs of bruteforcing

Be specific in what you find, being vague will get you 0 points.

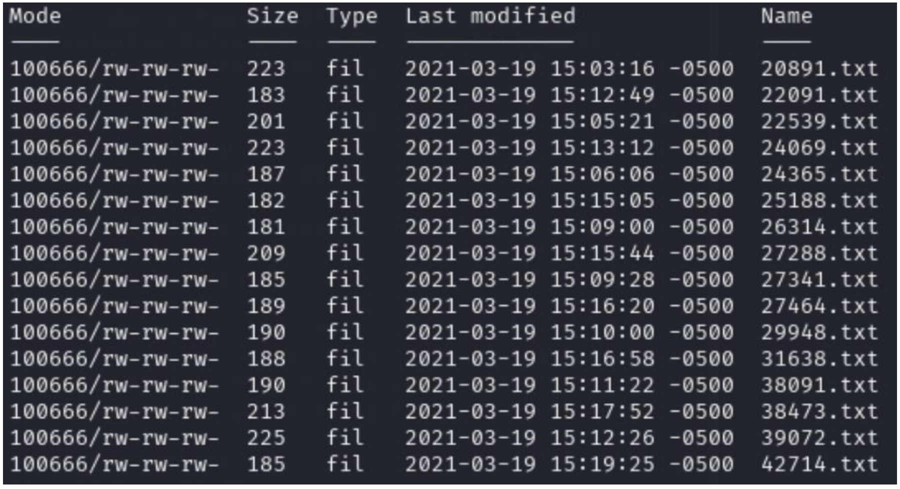
Host IP	1. **What was accessed?** 2. **How was it accessed?** 3. **What was the impact of the incident?** 4. **How did you respond to the incident?** 5. **Screenshot of what was accessed**
Receptions Dektop	1. The patients data was accessed 2. Working on it 3. Sensitive data was stolen 4. Deactivating SMB and updating the firewalls rules in order to protect other ports

Clinician Desktop

1. The attacker accessed the Patient Data

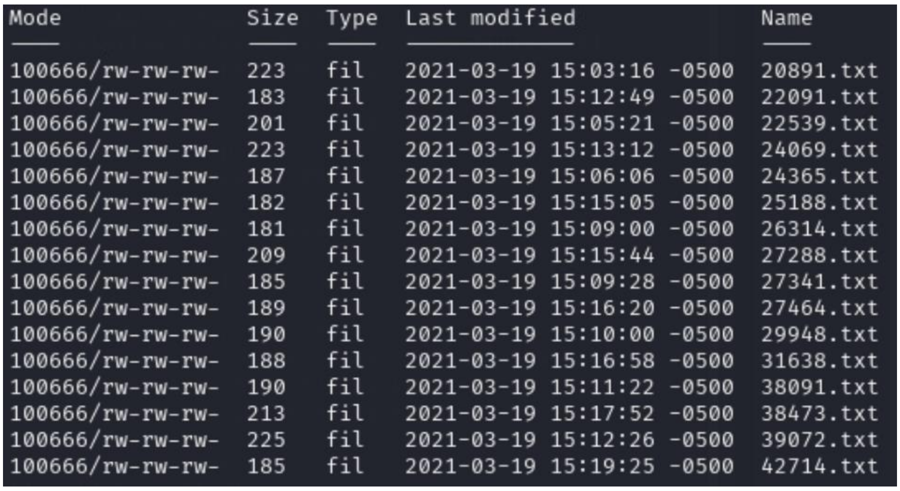


```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----

100666/rw-rw-rw-  719   fil   2021-03-19 15:50:11 -0500  20891.lnk
100666/rw-rw-rw-  619   fil   2021-03-19 15:34:55 -0500  22539.lnk
100666/rw-rw-rw-  719   fil   2021-03-19 15:50:17 -0500  26314.lnk
100666/rw-rw-rw-  719   fil   2021-03-19 15:50:20 -0500  38091.lnk
100666/rw-rw-rw-  150   fil   2021-03-19 15:33:56 -0500  Desktop.ini
100666/rw-rw-rw-  505   fil   2021-03-19 15:50:20 -0500  Patient Data.lnk
```



```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----

100666/rw-rw-rw-  223   fil   2021-03-19 15:03:16 -0500  20891.txt
100666/rw-rw-rw-  183   fil   2021-03-19 15:12:49 -0500  22091.txt
100666/rw-rw-rw-  201   fil   2021-03-19 15:05:21 -0500  22539.txt
100666/rw-rw-rw-  223   fil   2021-03-19 15:13:12 -0500  24069.txt
100666/rw-rw-rw-  187   fil   2021-03-19 15:06:06 -0500  24365.txt
100666/rw-rw-rw-  182   fil   2021-03-19 15:15:05 -0500  25188.txt
100666/rw-rw-rw-  181   fil   2021-03-19 15:09:00 -0500  26314.txt
100666/rw-rw-rw-  209   fil   2021-03-19 15:15:44 -0500  27288.txt
100666/rw-rw-rw-  185   fil   2021-03-19 15:09:28 -0500  27341.txt
100666/rw-rw-rw-  189   fil   2021-03-19 15:16:20 -0500  27464.txt
100666/rw-rw-rw-  190   fil   2021-03-19 15:10:00 -0500  29948.txt
100666/rw-rw-rw-  188   fil   2021-03-19 15:16:58 -0500  31638.txt
100666/rw-rw-rw-  190   fil   2021-03-19 15:11:22 -0500  38091.txt
100666/rw-rw-rw-  213   fil   2021-03-19 15:17:52 -0500  38473.txt
100666/rw-rw-rw-  225   fil   2021-03-19 15:12:26 -0500  39072.txt
100666/rw-rw-rw-  185   fil   2021-03-19 15:19:25 -0500  42714.txt
```

2. Working on it
3. Sensitive data was stolen
4. Deactivating SMB and updating the firewalls rules in order to protect other ports



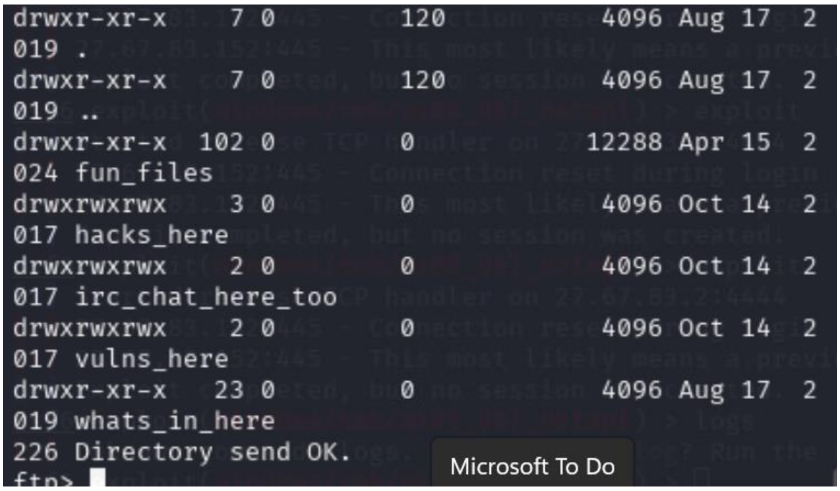
```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----

100666/rw-rw-rw-  223   fil   2021-03-19 15:03:16 -0500  20891.txt
100666/rw-rw-rw-  183   fil   2021-03-19 15:12:49 -0500  22091.txt
100666/rw-rw-rw-  201   fil   2021-03-19 15:05:21 -0500  22539.txt
100666/rw-rw-rw-  223   fil   2021-03-19 15:13:12 -0500  24069.txt
100666/rw-rw-rw-  187   fil   2021-03-19 15:06:06 -0500  24365.txt
100666/rw-rw-rw-  182   fil   2021-03-19 15:15:05 -0500  25188.txt
100666/rw-rw-rw-  181   fil   2021-03-19 15:09:00 -0500  26314.txt
100666/rw-rw-rw-  209   fil   2021-03-19 15:15:44 -0500  27288.txt
100666/rw-rw-rw-  185   fil   2021-03-19 15:09:28 -0500  27341.txt
100666/rw-rw-rw-  189   fil   2021-03-19 15:16:20 -0500  27464.txt
100666/rw-rw-rw-  190   fil   2021-03-19 15:10:00 -0500  29948.txt
100666/rw-rw-rw-  188   fil   2021-03-19 15:16:58 -0500  31638.txt
100666/rw-rw-rw-  190   fil   2021-03-19 15:11:22 -0500  38091.txt
100666/rw-rw-rw-  213   fil   2021-03-19 15:17:52 -0500  38473.txt
100666/rw-rw-rw-  225   fil   2021-03-19 15:12:26 -0500  39072.txt
100666/rw-rw-rw-  185   fil   2021-03-19 15:19:25 -0500  42714.txt
```

5.

Toms Project

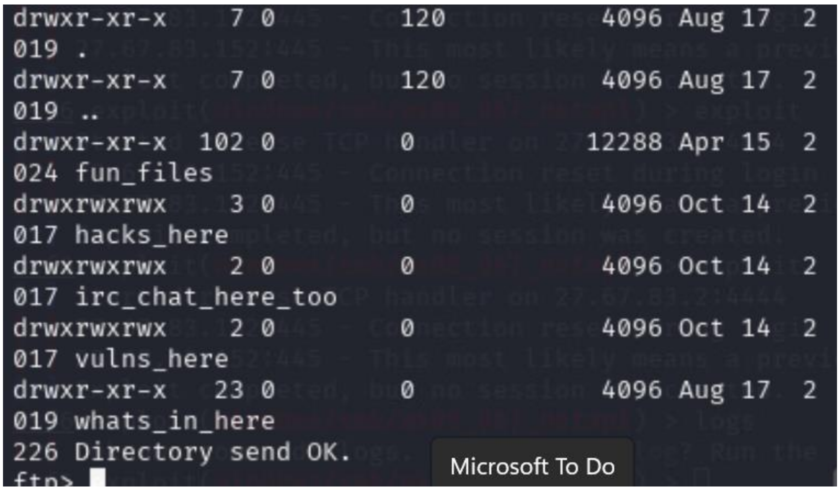
1. The entire device was compromised, the person who exploited the device has root rights and a backdoor. He has access to the server, webserver, database, everything on the machine. These are the folders

with all the files in the FTP



```
drwxr-xr-x    7 0        120          4096 Aug 17  2
019 .
drwxr-xr-x    7 0        120          4096 Aug 17  2
019 ..
drwxr-xr-x  102 0        0           12288 Apr 15  2
024 fun_files
drwxrwxrwx    3 0        0            4096 Oct 14  2
017 hacks_here
drwxrwxrwx    2 0        0            4096 Oct 14  2
017 irc_chat_here_too
drwxrwxrwx    2 0        0            4096 Oct 14  2
017 vulns_here
drwxr-xr-x   23 0        0            4096 Aug 17  2
019 whats_in_here
226 Directory send OK.
ftp> 
```

2. Working on it
3. The attacker was successfully able to create a backdoor user with root rights who doesn’t have a password. Plus the person can access a lot of the important files only using FTP
4. Deactivating FTP and telnet, deleting the backdoor user and telling everyone to change their passwords.
5.



```
drwxr-xr-x    7 0        120          4096 Aug 17  2
019 .
drwxr-xr-x    7 0        120          4096 Aug 17  2
019 ..
drwxr-xr-x  102 0        0           12288 Apr 15  2
024 fun_files
drwxrwxrwx    3 0        0            4096 Oct 14  2
017 hacks_here
drwxrwxrwx    2 0        0            4096 Oct 14  2
017 irc_chat_here_too
drwxrwxrwx    2 0        0            4096 Oct 14  2
017 vulns_here
drwxr-xr-x   23 0        0            4096 Aug 17  2
019 whats_in_here
226 Directory send OK.
ftp> 
```