Lab 10

Host discovery (3 points per row; **15 total points**)

Host Machines	IP Address	Open Ports/Services	Operating System
Ambulance Laptop	42.49.30.158	135: msrpc 139: netbios-ssn 445: microsoft-ds 3389: ms-wbt-server 49664: unknown 49665: unknown 49666: unknown 49667: unknown 49671: unknown 49672: unknown 49674: unknown	Windows 10
Reception Desktop	42.49.30.152	135: msrpc 139: netbios-ssn 445: microsoft-ds 3389: ms-wbt-server 49668: unknown	Windows 10
Clinician Desktop	42.49.30.154	135: msrpc 139: netbios-ssn 445: microsoft-ds	Windows XP
Web Server	42.49.30.150	22: ssh 8000: http-alt 44245: telnet	Ubuntu 18
Database	42.49.30.156	None	Ubuntu 20

Exploiting the machines (9 points per row; **45 total points**

Host Machines	**How did you gain access?**	**What specific harm could be done?**	**How can you remediate it?**
Ambulance Laptop	I was able to dump the hashes of user credentials on the reception desktop. This allowed me to gain access to the Ambulance laptop by sending Tom's hashed password to login through SMB, called passing the hash.	I was able to view a list of reports containing information about paramedics responding to incidents. This information could be used to blackmail patients if tracked back to them.	Since I was able to dump hashes on the reception desktop, one fix would be to reduce admin privileges on that device to only needed users. As well, utilizing NTLMv2 instead of LM/NTLM will prevent passing the hash from working. Finally, if Windows SMB service is not needed on the Ambulance laptop, it could be disabled.
Reception Desktop	I was able to gain access through remote desktop on the reception desktop, because the user Rachel's password was weak and easily guessable.	I was able to gain access to a list of HR records that contained employee addresses, emails, and phones. Using this information, I could phish these internal workers, among other crimes.	Since the user's password was simple and easy to guess, it should be set so that passwords must meet complexity requirements by editing the group policy in Windows.
Clinician Desktop	I was able to gain admin privileges and shell access to the clinician desktop by exploiting a remote code execution labeled as MS08-067. It affects Windows RPC on Windows 2000 through 2008.	I was able to gain access to a list of patient data that includes their smoking habits, used medicine, and phone numbers. This information can be used against the patients by vishing them or other crimes.	Since the clinician desktop is running Windows XP with an unpatched RPC service, I was able to exploit the RPC. To remediate this, installing the patch Windows put for the RPC service would prevent this. As well, another option is to update the machine to the latest version of Windows as XP is EoL.
Web Server	I was able to gain root access to the web server by connecting to the through SSH. It automatically logged me in as root with no password prompt. As well, hidden within the main page and going /llehs to the url there is a root access web shell within the application.	I was able to access a json file that would contain a list of user credentials and a file showing a database at 42.49.30.202 with an admin username that has no password. I could login as any after decrypting the passwords using the available python script. As well, I could compromise the database storing the logins.	Since I am able to gain root access through ssh and hidden webshells, modifying the sshd configuration to prevent root login and empty passwords would prevent this. Then, the root user & all users should be given strong passwords. As well, clearing out the web shells from the web page will prevent remote access through the web service.
Database	With physical access to the database, I booted a live Kali image and mounted the database's hard drive. Then, I could read and modify all information on the drive.	With physical access, I was able to gain access to a file userdata.ibd in the database that contained a list of people's names, attached to SSNs and card numbers. I could sell this information or commit credit card fraud and identity theft against these users.	Since I had physical access to the database and was able to mount the hard drive on a live image, a remediation for this would be full disk encryption on the hard drive. This would prevent me from mounting the drive without knowing its key/password. As well, since I could read the database's data, its information should be encrypted as well.

Sensitive information (8 points per row; **40 total points**)

Host Machines	**What information I found, and why it's bad that I can see it.**
Ambulance Laptop	On this ambulance laptop, I was able to view a list of paramedic reports that contain information like location, time, and a written report of the incident. Since I can access this information, the confidentiality of both the patient and paramedics is violated.
Reception Desktop	On the reception desktop, a list of HR data files containing information like an employee's residence, phone, title, name, birthday, and email are accessible. Since I have access to email and their work titles, I can now target certain users and send phishing attacks against them. Other information like their residence allows a viewer to know where they live. This violates the confidentiality of employees information that they trust with HR to know.
Clinician Desktop	On the clinician desktop, in a common "All Users" directory, there was a series of patient data files that contained information like someone's blood type, smoking status, name and their numerical identifier. This could be seen as a HIPAA violation as anyone accessing the device can view these records. This information should be made confidential between only the doctor and patient or anyone else who needs access to it.
Web Server	I was able to view a list where user login credentials would be stored and the admin credentials to a database on the 42.49.30.202 ip address. By learning this information, I would be able to login and impersonate any user and/or compromise the other database storing user logins for the website. In this way, I could invalidate the integrity of user actions of the web page and confidentiality of logins users trust the web page to store.
Database	On this database, I was able to view unencrypted sets of first and last names, SSNs and card numbers. This is both in violation of PCI and HIPAA as SSNs and any card information must not be stored where it could be viewed by anyone like I have with physical access. This invalidates the confidentiality patients expect with the hospital to store their card and health information.