Jon schnell
Cpr E 231
Lab 11
Part 1

Host	Open Ports	Services	OS guess
111.76.65.151	22 8000	SSH(open SSH 7.6p1) HTTP(nginx 1.14)	Linux (no fingerprint match) Ubuntu or BSD 7.6
111.76.65.152	135 139 445 3389	MSRPC Netbios-ssn Microsoft-ds SSL/ms-wbt-server	Microsoft windows 10 DESKTOP-XXXXX
111.76.65.153	21 22 139 445 5901 6001	FTP(vsftp) SSH(open SSH 7.2p2) Netbios-ssn(samba 3 or 4 smbd) Microsoft-ds(samba 3 or 4 smbd) VNC 3.8 x11	Linux 3.2 - 4.9 ubuntu 16 UBUNGUGANO
111.76.65.154	22 80 4567 8080	SSH(open SSH 7.2p2) HTTP (apache 2.4.18) tcpwrapped HTTP alt or proxy	Linux 3.2 - 4.9 Ubuntu CPE
111.76.65.155	22 79 139 445	SSH(open SSH 7.2p2) Finger(debian finger) Netbios-ssn(samba 3 or 4 smbd) Microsoft-d(samba 3 or 4 smbd)	Linux 3.2 - 4.9 Ubuntu WEBCAM

Host	What I tried	What I found	How I could use it
111.76.65.151	Poked around the web interface	Bulletin board has some valuable information available to the public	Holiday dinner might be a good opportunity to compromise the physical security of the company. Company shutdown dates and times that no one will be in the office.

Jon schnell
Cpr E 231
Lab 11
Part 1

			W2's are being handed out by an intern that doesn't know the staff. This is a good opportunity for social engineering. llehs took down the site they may have left a backdoor. Due to c-19 all orders are to be picked up in person and the purchaser should call upon arrival. This is a good opportunity for social engineering.
111.76.65.152	Nessus scan	Screenshot of the login screen	This could be used to spy on a user or determine valid usernames to bruteforce with
111.76.65.153	Banner grab	Reveals the os version as well as an error message from the probe of the FTP client	This can be used to look for known vulnerabilities
111.76.65.154	Poke around the web interface	Looks like its still under development	Could be an experimental or test server and likely to have bugs or misconfigurations. Broken links reveal the version of apache being used.
111.76.65.155	Probe finger	A username and personal details for the user	This would be valuable for social engineering

Jon schnell
Cpr E 231
Lab 11
Part 1

	Ssh into root	The hashes are printed before asking a user for a password	because you know a name and phone number but also for brute forcing because the username is already known. The hashes can be cracked to reveal the password for users

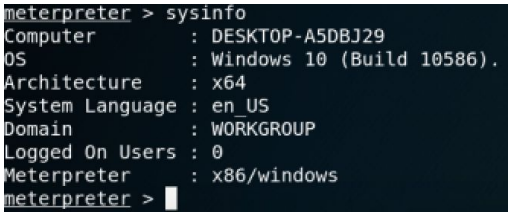
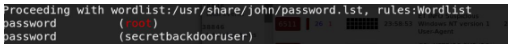
Source IP	Source Port	Destination IP	Destination Port	Useful cleartext captured/recorded
111.76.65.151	8000	111.76.65.2	41340	Nginx v1.14
111.76.65.151	22	111.76.65.2	34794	Open ssh v7.6p1
111.76.65.151	22	111.76.65.2	34794	diffie-helmen key exchange information 
111.76.65.154	80	111.76.65.2	34640	apache 2.4.18 A user making a purchase on this site will expose banking details because http is plaintext

Jon schnell
Cpr E 231
Lab 11
Part 1

Host	Vulnerability	Why it is a threat
111.76.65.152	Ms17-010 (eternal blue)	eternal blue allows a remote use to connect to the machine and drop to a shell. From there information could be extracted, malware installed, or a backdoor put in place.
111.76.65.152	Ms16-047 (badlock)	This vulnerability allows an attacker to man in the middle the client and server and change the authentication rules and hijack another user's session
111.76.65.152 111.76.65.153 111.76.65.155	SMB signature not required	This allows an attacker to man in the middle the client and server
111.76.65.153	VNC server using default password 'password'	This would allow an attacker to gain a shell remotely
111.76.65.153	X11 server unprotected	This allows an attacker to
111.76.65.155	Finger service running	Allows an attacker to see what users are logged on and when they last logged on

Host	Exploit	Countermeasure to suggest to the CIO
111.76.65.151	Ssh root@111.76.65.151 No password on root account	Add a strong password for root. Don't allow password authentication for ssh sessions.
111.76.65.152	Ms17-010	Update windows or filter port 445

Jon schnell
Cpr E 231
Lab 11
Part 1

		
111.76.65.153	VNC password is ‘password’ 	Set a strong password for VNC or filter port 5901
111.76.65.155	Attempting to ssh into root dumps the etc/shadow file. I used John the Ripper to crack the passwords and found that multiple users have a password of ‘password’ (including root) and there is a backdoor on the box (maybe put there by llehs) 	Don’t expose etc/shadow because weak passwords can easily be cracked. Force password complexity and change passwords quartley.