Project X

CSC 790

Shuowen Wei

I. Reconnaissance

1. Yes, the kiosk system is connected to the network most of the day time, except it’s shut down during the nights. The IP address is 10.104.251.71

2. I ran nmap on the IP and found the following currently open ports:

PORT STATE SERVICE

22/tcp open ssh

111/tcp open rpcbind

5999/tcp open ncd-conf?

6002/tcp open X11

7007/tcp open utsessiond

The application normally associated with each port are listed below, cited from Wiki:

| **Port** | **TCP** | **UDP** | **Description** | **Status** |
| --- | --- | --- | --- | --- |
| 22 | TCP | UDP | [Secure Shell](http://en.wikipedia.org/wiki/Secure_Shell) (SSH) — used for secure logins, [file transfers](http://en.wikipedia.org/wiki/File_transfer) ([scp](http://en.wikipedia.org/wiki/Secure_copy" \o "Secure copy), [sftp](http://en.wikipedia.org/wiki/SSH_file_transfer_protocol" \o "SSH file transfer protocol)) and port forwarding | Official |
| 111 | TCP | UDP | [ONC RPC](http://en.wikipedia.org/wiki/Open_Network_Computing_Remote_Procedure_Call) ([Sun](http://en.wikipedia.org/wiki/Sun_Microsystems) [RPC](http://en.wikipedia.org/wiki/Remote_Procedure_Call)) | Official |
| 5999 | TCP |  | [CVSup](http://en.wikipedia.org/wiki/CVSup) file update tool[[99]](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers#cite_note-99) | Official |

Those two from not found on Wiki, they are from other web sources:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port(s)** | **Protocol** | **Service** | **Details** | **Source** |
| 6002 | tcp,udp | x11 | X Window System | SANS |
| 6002 | tcp | X11:2 | X Window server | Nmap |
| 6002 | udp | X11:2 | X11:2 | Nmap |
| 7007 | tcp,udp | applications | Port used by: Windows Media Player Encoder-to-Server Communication, Skype Session Manager, G3Torrent, X-Men Movieverse, Silent Spy, basic overseer process, City of Heroes, City of Villains, RealAudio. Trojans that use this port: W32.Spybot.Gen3, Silent Spy | SG |
| 7007 | tcp | trojan | Silent Spy | Trojans |
| 7007 | tcp,udp | afs3-bos | basic overseer process | IANA |
| 7007 | tcp,udp | threat | MSBD | Bekkoame |
| 7007 | tcp,udp | threat | Windows Media encoder | Bekkoame |

3. The operating system the kiosk system uses is Sun Solaris 9 or 10, or OpenSolaris 2009.06 snv\_111b

4. The kiosk system is just using a ppt-like software on Sun Solaris system playing pre-made slides iteratively.

5. Virtual access to the system is very difficult, basically because I not good at it, plus Dr. Pluf told us the wrong IP space 10.104.2.\*, while the true is 10.104.251.71 that we found it physically. I am guess there a machine in the IP space 10.104.2.\* remotely controlling ppt-playing the kiosk system with IP 10.104.251.71. But, physically access to the kiosk system is not a very hard thing, just stay until after every professor is gone (except Dr. Turkett but he is fine with it).

6. Well, the first and the only successful method is physically accessing to the system while there’s no professors around. Get everything done within 5 minutes.

The second method I was thinking was to find the machine and upload some vulnerable program, use commands like ‘strcpy’ and overflow the stack to spawn the shell, get the root and change the slides. But I can’t find the machines virtually and nor do I have this piece of shell code to use.

Can't think of any third method, to collate with other teams? ?

II. Kiosk Tag

1. Physically access to the kiosk system at 7:00 pm when Dr. Turkett is out for dinner and then …

2. Tuesday to Wednesday, trying the nmap the IP space given by Dr. Pluf, gave up since heard other team talking that IP info is useless since the real IP address is in the given IP space. On Thursday night, successfully get into the main office and physically accessed into kiosk system, and accomplished the mission.

3. Tried to get into the main office on Wednesday night after the “trivia night” event, but Dr. Pluf is around and we failed the first time. But we didn’t get caught! Succeed on the following night. I also tried nmap the kiosk IP but failed because the system was shut down, I tried later to get all the related info when the screen is on.