# Secure Computer Systems I: Lab 3

Ren Li Tianyao Ma Samuel Pettersson

March 4, 2014

## Host 1: 192.168.233.20

## Host 2: 192.168.233.110

The second host to which root access was gained is 192.168.233.110. The instructions said that access to host 192.168.233.20 was required to access this machine.

Running nmap showed that two services were running on the target machine: Microsoft Windows RPC on port 135 and Microsoft Terminal Service on port 3389, the latter being used for serving remote desktop clients.

With no obvious vulnerabilities being present in the RPC service, attention was turned to the remote desktop service. The RDP client of our choice was (initially) rdesktop, which is available in the software package repository and was installed by issuing the command sudo apt-get install rdesktop.

Connecting to the other machine was as simple as running the command rdesktop 192.168.233.110. Upon doing so, we were presented with the Modern UI login screen. Authentication as the administrator appeared to require a smart card, whereas password authentication was an option for other users.

After some tinkering with a remote desktop connection on host 192.168.233.20, we found out that password authentication as the administrator on 192.168.233.110 was possible by starting a remote desktop session from 192.168.233.20 to 192.168.233.110. One could suspect that the administrator password for the two machines were the same, but despite having root access to 192.168.233.20, we were unaware of what the password to the administrator account was.

The immediate thought was to dump the password hashes on host 192.168.233.20 and have them cracked either by brute force or with a dictionary. Dumping the hashes is simple enough with a meterpreter shell: issuing the command run hashdump does the trick. For each user, two hashes were stored: an unused LM hash of the empty string and an NT hash. Unfortunately, the version of John the Ripper available on the BackBox machine did not have support for breaking NT hashes. The source code of the latest "jumbo" version of John the Ripper (version 1.7.9-7) with support for NT hashes was downloaded from `http://www.openwall.com/john/`. Building the application was a matter of running two make commands: make and make clean linux-x86-mmx as per the README and the installation instructions. After having run the jumbo version of John the Ripper for several hours without finding a password matching any of the dumped NT hashes, let alone the hash for the administrator account, the trail grew colder and we gave up on retrieving the password.

After having received a hint from Sofia, we decided to look into the possibility of passing the hash of the administrator on 192.168.233.20 (CL3\Administrator). That is, instead of authenticating with a password, we hoped to be able to authenticate with the hash of the password. Some research showed that Microsoft's Remote Desktop Protocol version 8.1 from last year introduced a Restricted Admin mode, in which credentials in the form of passwords are not sent to the remote server; instead, password hashes are sent. This mode was introduced in an effort to improve security in that authentication to a compromised server does not reveal the password in cleartext, but unfortunately, it comes at the expense of allowing pass the hash attacks[?]. Further research showed that an RDP client by the name FreeRDP with support for passing hashes was available in the form of a Git repository at GitHub[?][?].

The repository was cloned and the application was built by following the installation instructions available at GitHub[?]. The necessary packages were installed, cmake was used to generate Makefiles, and make was used to build and install the application. After having completed the installation, the client was available under the name xfreerdp.

The following command was executed to attempt to log on as the administrator with the hash retrieved from host 192.168.233.20: xfreerdp /u:Administrator /pth:fabc417905666832e4b4ba57711a4171 /v:192.168.233.110. Passing the hash turned out to work! A text file containing the secret code without any encryption was easily spotted on the desktop. The code read: vZxkRvEICzhNQ.

## Host 3: 192.168.233.106

## Host 4: 192.168.233.30