# UCOL BICT Network Internship

*Rupert Woodroffe*
UCOL Intern
*1491769@studentmail.ucol.ac.nz*

*Sandra Cleland*
UCOL (Internship Sponsor)
*s.cleland@ucol.ac.nz*

*Graeme Richards*
UCOL (Internship Sponsor)
*g.richards@ucol.ac.nz*

## ABSTRACT

Having a student intern within the School of Business and ICT served two purposes: it helped alleviate some of the pressure on the internship sponsors to complete infrastructure tasks alongside their full-time lecturing roles, and it provided the Intern with experience working within a live environment. The Intern helped with: imaging of lab computers, deploying Endpoint Antivirus, completing a penetration test on the BICT network, investigating software deployment using System Center Configuration Manager, troubleshooting infrastructure issues, writing PowerShell scripts and group policies, creating a vulnerable network for a network penetration exercise, installing new Cisco network devices.

**Keywords**: Infrastructure Internship, Windows 10 Imaging, Network Penetration Testing

## 1. INTRODUCTION

The UCOL BICT programme has had its own dedicated network since 2008. The Sponsors for this internship are fulltime lecturers on the programme who also maintain the network. They are responsible for: software selection and testing, PC imaging, server installation and maintenance, purchasing equipment for BICT infrastructure and Cisco Networking Academy upgrades, creating student and staff user accounts. The BICT network has 75 client PCs and a number of virtual servers hosted on two physical servers. PCs used in the Software Lab are part of UCOLs leased PC fleet, PCs in the Hardware Lab and BICT project room are School owned and maintained. The internship sponsors were approached by a third year BICT student in Semester One, 2016 to see if they would consider having an intern. The student had approached many local businesses looking for an infrastructure related internship to meet the requirements of their semester two capstone course but had not been successful in securing one. The student began interning with the sponsors during the mid-semester break in July 2016.


This poster appeared at the 8th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2017) and the 30h Annual Conference of the National Advisory Committee on Computing Qualifications, Napier, New Zealand, October 2-4, 2017.

## 2. INTERNSHIP SCOPE

The initial Internship Scope was set as: Assisting with the PC imaging process prior to semester two start; writing of PowerShell scripts to automate common tasks; troubleshooting of infrastructure issues; deployment of Endpoint anti-virus via System Center Configuration Manager (SCCM); further investigation into Windows 10 image deployment via SCCM. As well as these technical skills the Intern was looking to further develop their interpersonal skills through communication and interaction with Internship sponsors and end users and improve their time management. During the Internship the Intern was also involved with: Penetration testing of the BICT network, Installation of new Cisco switches and routers, creating a vulnerable network for simulated penetration testing, and various active directory and group policy tasks.

## 3. EVIDENCE OF SKILL DEVELOPMENT

The intern assisted in the imaging of the lab pcs by helping document the new imaging process for the Windows 10 environment and assisting with troubleshooting errors when Sysprep of the build pc failed. Microsoft Sysprep is run to 'generalize' the image, removing any unique installation information from the build PC such as the Security Identifier (Microsoft, 2003). The build pc image is then captured using Deployment Image Servicing Management (Microsoft, 2014). The captured image is then deployed over the network to other PCs through the use of Microsoft Deployment Toolkit and Windows Deployment Services (Microsoft, 2016)

Once the labs were ready for semester the Intern then began looking into deployment of Endpoint Antivirus via SSCM (ESET, 2016). Deploying Endpoint Antivirus involved first adding a WSUS role to the SCCM server and then installing the SSCM client to PCs over the network using SSCM. There was some troubleshooting of the client installation as it failed on some PCs. The intern worked around this issue by using a GPO (Group Policy Objects) to deploy the client software on some machines. The intern then used SSCM to deploy Endpoint and set the rules for how it operated.

With Endpoint operational the Intern began to investigate the use of SSCM to create and deploy PC images in the future (O'Meally, 2015). The internship sponsors requested this

investigation to ensure that the imaging process that was being used was the most efficient way to work with Windows 10 PCs. The intern had a certain amount of success with creating and deploying a software image to the Hardware Lab PCs where the amount of applications in use was minimal but found that the process could not be applied to the Software Lab PCs where the many development environments in use added extra complexity.

Penetration testing of the BICT network involved first gathering as much information about the network as possible. This was achieved through existing diagrams, scans with Nmap, scans with Nessus, inspection of equipment, Wireshark and Ettercap captures as well as connecting to each device and checking operating system/software versions. Then with the use of Armitage, Metasploit, and accessing the Exploit Database the Intern checked to see if any of the infrastructure was susceptible to attack. The Intern found the Exploit Database was found to be particularly useful, this site has an archive of over 30,000 exploits and vulnerabilities (Exploit Database, 2016).

The scans identified information leakage about the services and protocols running on the machines. A lot of this information could be masked with properly configured firewalls, however the servers are accessible internally and was therefore not seen as a huge risk. The Intern also found many remote code execution and denial of service vulnerabilities in some of the key infrastructure. The reason behind these was outdated software and operating systems. The Intern was able to fix some of these issues straight away i.e. re-enabling automatic updates on the domain controller, however the rest would involve downtime to infrastructure so were logged as issues to fix over semester breaks.

Creating the vulnerable network for the simulated penetration testing began with working with one of the Internship sponsors to design a layout for the network and the components that would be operating on it, A MySQL environment was created by installing MySQL on a Debian server and creating accounts, databases, populating tables with dummy data, disabling direct SSH access and only allowing tunnels by preventing the use of a shell prompt. Then a vulnerable webserver component was constructed to connect to and query the MySQL database from a PHP site. Also residing on the webserver was a simulated SQL injection attack. Only basic Apache authentication was enabled on these sites, allowing for the clear text login information to be captured. Asterisk, a software based private branch exchange, was set up on another Debian server and configured to call a VOIP phone through the use of call files (Digium Inc, 2016). The phone would play a conversation generated from an online text to speech resource. The phone was configured to provision using TFTP, allowing for the capture of this information. A machine running Metasploitable was configured with an iptables firewall rule to only allow access from only one client based on its MAC address (Netfilter, 2016). Metasploitable is an intentionally vulnerable linux virtual machine (Rapid7, 2016). An unpatched version of Windows XP was set up to connect to an iSCSI server and provide remote storage with sensitive info. A mobile phone simulating a security camera was also set up to connect to the XP machine and send photos via FTP. All of these servers were virtual machines running on a single ESXi box, they were connected to the other devices via a switch that was vulnerable to MAC flooding and ARP poisoning. An access point running WEP with a hidden SSID was also connected. To allow for the cracking of this WEP key a raspberry pi was used to generate traffic when needed.


**Figure 1: Vulnerable network setup (left) and attack machine (right)**

## 4. INTERNSHIP SUMMARY

Overall the Internship went well. The Internship sponsors got valuable assistance and the Intern gained experience in a variety of areas to do with server and network administration and maintenance. As the Intern was well known to the Sponsors there was no hesitation in letting the Intern work with the live infrastructure, something that would have been less likely in an external organisation. The Intern was constantly facing new challenges and in turn honed their problem solving, researching, and decision-making skills. The Intern identified their greatest achievements during the internship as: writing PowerShell scripts to change BIOS settings remotely, deploying Endpoint Antivirus and other software to a blank machine using System Center Configuration Manager, penetration testing the BICT network and writing recommendations for fixes, creating a vulnerable network for network penetration testing, and varied tasks using group policies and active directory.

## 5. REFERENCES

Digium Inc. (2016). Retrieved from http://www.asterisk.org/

ESET. (2016). Retrieved from https://www.eset.com/int/business/endpoint-security/windows-antivirus/

Exploit Database. (2016). Retrieved from https://www.exploit-db.com/

Microsoft. (2003). *What is Syspep?* Retrieved from TechNet: https://technet.microsoft.com/en-us/library/cc783215(v=ws.10).aspx

Microsoft. (2014, April 18). *What is DISM?* Retrieved from TechNet: https://technet.microsoft.com/en-us/library/hh825236.aspx

Microsoft. (2016). *Microsoft Deployment Toolkit*. Retrieved from TechNet: https://technet.microsoft.com/en-us/windows/dn475741.aspx

Netfilter. 2016). Retrieved from http://ipset.netfilter.org/iptables.man.html

O'Meally, Y. (2015). *System Center Configuration Manager: for Windows 10 and Microsoft Intune*. Retrieved from: https://blogs.technet.microsoft.com/enterprisemobility/2015/10/27/system-center-configuration-manager-support-for-windows-10-and-microsoft-intune/

Rapid7. (2016). Retrieved from https://www.metasploit.com/