**Security Blue Team – Introduction to Vulnerability Management**

### METASPLOITABLE 2 SETUP

You’ll be setting up the intentionally vulnerable virtual machine Metasploitable 2, created by security firm Rapid7. This will be your test environment where you can practice vulnerability scanning, collecting results, and analysing them to produce vulnerability reports.

### NESSUS SETUP

You’ll install and explore the Nessus Essentials vulnerability scanner created by Tenable, in preparation for the final course challenge.​ You’ll be walked through the GUI and conduct a scan against your own system, so that you’re familiar with how to use this powerful tool, and understandscan results.​

### WPSCAN ANALYSIS

You’ll be analysing real-world WPScan results to make sure you’re familiar with the tool’s output. and the security flaws that it can detect. In the future we will release a public lab where you can conduct your own scans.​

### COURSE CHALLENGE: VULNERABILITY ASSESSMENT

For the final challenge you’ll be conducting a short and simple vulnerability assessment of the Metasploitable 2 system, by launching your own vulnerability scans using Nessus, and reporting on the vulnerabilities and flaws that are discovered.​

### **Metasploitable 2**

**Some of the questions in the course**

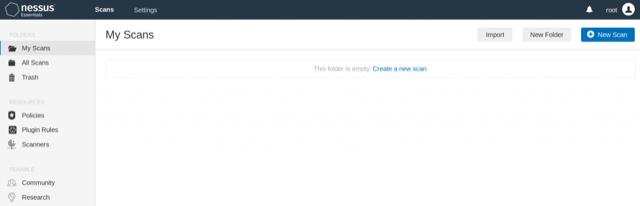
How many TCP ports are OPEN on MS2? (Use the -sT flag in Nmap).

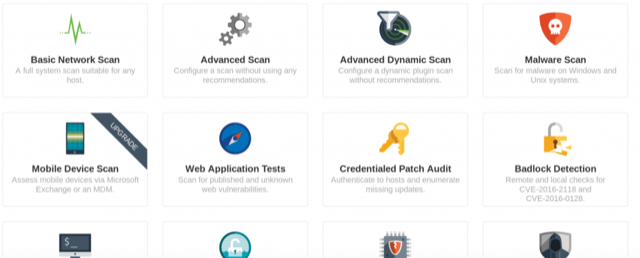
How many UDP ports are OPEN on MS2? (Use the -sU flag in Nmap – this may take a while).

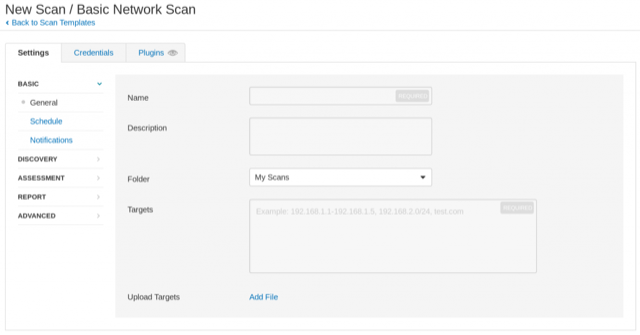
What port is running a Metasploitable Root Shell? (Use the -sV flag in Nmap).  
What non-standard port is FTP running on? (NOT p21) (Use the -sT flag in Nmap)

What version of FTP is running on the non-standard port? (Use the -sV flag in Nmap).

**Nessus**







The course also included OpenVAS and WPScan with activities…

**Completion Certificate**

