Unix for Telecommunications

Portfolio Task – P-Lab-07-NMap

Pass Level Task

I. Introduction

In this lab you will use the program NMap to discover a range of network services running on remote machines and perform some simple network auditing tasks.

WARNING: Although port scanning is not illegal, it is considered bad practice and may be viewed as a prelude to an attack by the operators of those hosts. Do not scan hosts and ports outside of the ones defined in this lab handout using your RULE host. Note that if you do, your actions can be traced and you may face consequences. Remember that you are bound by Swinburne's IT policies and procedures while using Swinburne's IT infrastructure.

II. Purpose

To gain and/or enhance the following practical skills:

- Using NMap to discover a range of network services running and simple network auditing tasks
- Understand concepts and processes in determining which services are running on a remote system

III. Preparation

You can prepare for this lab by reading some of the NMap documentation available at https://nmap.org/.

IV. Methodology

A. Special Note

All commands in this lab should be run as user **`student`** rather than as **`root`**. Running NMap as **`root`** on the RULE host does not work properly due to limitations imposed by the virtualisation system deployed using BSD jails. If you are exploring NMap beyond the commands described in this lab you may receive messages such as "Operation not permitted". If this occurs it is because you have entered a command that required low-level **`root`** access to the underlying hardware. Using NMap at home on a real host will allow you to fully explore NMap. Again, it is considered poor practice to run NMap against hosts that you do not manage and may be considered as a prelude to an attack by the operators of those hosts. Please consider this when you run NMap from home.

B. NMap Exploration

1) NMap has already been installed on your rule host. If it would not be installed already, how could you install NMap under FreeBSD?
2) Read the NMap documentation, what is the purpose of running NMap in verbose mode? Why should you do this during the lab exercises?
3) Perform a "Host Discovery" on the subnet `136.186.230.0/24`. What does the result show?
4) What ports are included in a default port scan? Why?
5) Scan the following hosts and comment on what ports are open:
   - `jbut.caia.swin.edu.au`
   - Your other Rule host(s)
6) Repeat the scan on the above hosts but this time scan **all** ports rather than just the default ports.
7) Comment on why you think some machines might take longer to scan than others.

C. Probing a hosts network services in more detail

We will now explore the host `rule21.caia.swin.edu.au`

1) What network applications/services are running on this host?
2) What versions of these applications are running on this host?
3) How might this information be used for:
   - A hacker attempting to compromise the system
   - A network administrator attempting to protect the system
   - The server administrator

V. Assessment

The due date for completion of practical work is **11:00pm**, exactly **six** days after your scheduled class.

Note: *The nominated submission day/time holds regardless of whether that day is a non-teaching day or public holiday*

To complete this lab you need to submit (to Doubtfire) a simple (unformatted) PDF document containing a list of all services running on `rule21.caia.swin.edu.au`

Note: *A PDF upload is required as Doubtfire cannot currently accept uploads of text files*

A. Completion of task in Doubtfire

You will need to upload your PDF file containing the list of running services to your Doubtfire portfolio before the due date

B. Tutor Discussion

In order for the submission to be marked as complete, you must discuss your work with the tutor