HACK LIKE A PRO

How to Scan the Globe for Vulnerable Ports & Services

BY OCCUPYTHEWEB 8/6/13 8:45 AM HACK LIKE A PRO NMAP

Welcome back, my hacker novitiates!

Finding vulnerabilities in systems can be one of the most time-consuming tasks for a hacker. There will be times, though, when you'll find yourself in a position that you know that a particular port represents a vulnerable application or service.

The Story of Max Vision

For example, the gray-hat hacker, Max Bulter, aka Max Vision, the founder of arachNIDS who's now serving 9 years in federal prison, found that the Aloha Point-of-Sale (POS) system had installed a remote backdoor to all their systems in order to provide technical assistance purposes to their customers.

Santa Clara County Sheriff

These Aloha systems are used by small-to-medium sized restaurants that take thousands of credit card numbers each year. Knowing this, Max set a computer program to constantly scan the U.S. for systems that had port 5505 open. This would indicate that the computer was running Alaho's POS system, as port 5505 is not used by any other common service, and that the vulnerable service was open and available.

When he found the port open, he would then execute an exploit against that port and service and scavenge all the credit card numbers he could. He then sold them for $5 to $50 each bringing him a tidy return for each hack.

How to Scan for Vulnerable Ports

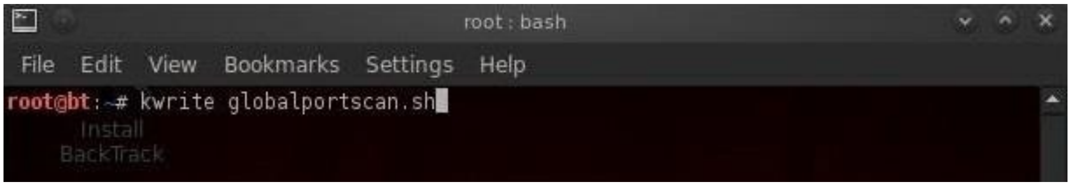
In this tutorial, we'll write a short script that does exactly what Max Vision was doing and send a report with every IP address of the vulnerable system.

Step 1: Open a Text Editor

To create our script, we need to open a text editor. Any of the Linux text editors will work; **vi**, **emacs**, **gedit** (in the GNOME), **Kate**, or **KWrite**. In this guide, we'll use the KWrite editor built into BackTrack5v3 KDE. We simply type in a terminal:

- **kwrite globalportscan.sh**

We can name our script anything, but I have chosen to call it **globalportscan.sh**.



```
root@bt:~# kwrite globalportscan.sh
```

This will open a blank file editor for our script.

Step 2: Create the Script

Now we need to type the following lines in our script file.

- **#!/bin/bash**

The required opening of all BASH scripts.

- **nmap -sT 74.125.225.0/24 -p 5505 -oG aloha**

Does an nmap connect scan (-sT) to the subnet of google.com and looks for the port 5505 open and sends the output (-oG) to a file called aloha.

- **cat aloha | grep open > alohaopen**

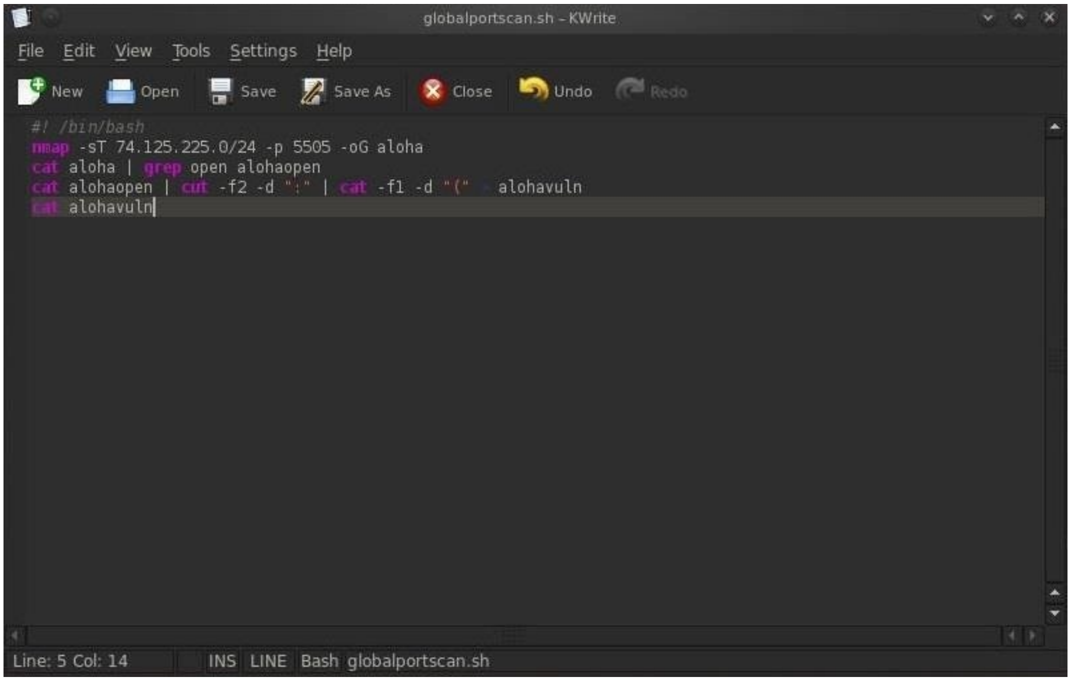
Opens the file aloha and filters (grep) for lines that say open, and stores those lines in a file called alohaopen.

- **cat alohaopen | cut -f2 -d ":" | cut -f1 -d "(" > alohavuln**

Opens the file alohaopen and cuts it at the second field (-f2) defined by the delimiter (-d) semicolon (":"), then pipes that to a second cut command that cuts the file at the first field (-f1) defined by the delimiter (-d) paren ("(") and saves it into a file named alohavuln.

- **cat alohavuln**

Finally, we open and display the file that contains all the IP addresses of systems with port 5505 open.


globalportscan.sh – KWrite
File Edit View Tools Settings Help
New Open Save Save As Close Undo Redo
Line: 5 Col: 14 INS LINE Bash globalportscan.sh

```
#! /bin/bash
nmap -sT 74.125.225.0/24 -p 5505 -oG aloha
cat aloha | grep open alohaopen
cat alohaopen | cut -f2 -d ":" | cat -f1 -d "(" > alohavuln
cat alohavuln
```

Step 3: Run the Script

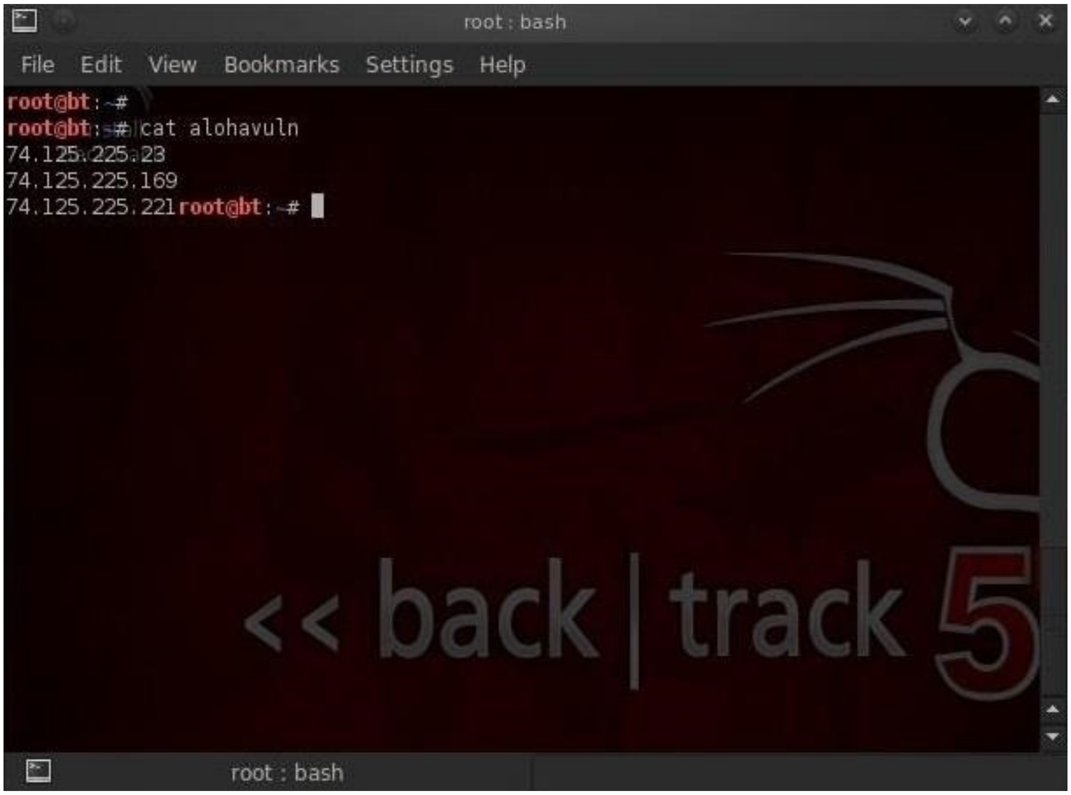
Now that you have saved the script, it's time to run it.

- **sh globalportscan.sh**

Now, sit back and wait for your results. It could take a while depending upon how many IP addresses you're scanning. In our example, we're only scanning 255 addresses, so it only takes a few minutes, but you could very well set this up to scan millions of addresses, in which you might wait days for results.

Step 4: Final Results

We can run this script on any IP address or network. I just used google.com as an example (you're not likely to find port 5505 open at google.com). You should see results that look something like this:



```
root@bt:~#
root@bt:~# cat alohavuln
74.125.225.23
74.125.225.169
74.125.225.221root@bt:~#
```

Of course, this vulnerability is likely closed in nearly all systems now, but this script can easily be edited to scan for other ports and other IP addresses depending upon your needs.

POS system and World images via Shutterstock, Max photos via WIRED and Santa Clara County Sheriff

WonderHowTo.com About Us Terms of Use Privacy Policy