CERIAS

the center for education and research in information assurance and security

Network Security Support

Problem:

Many network scanning tools provide a snapshot of a network at a given time. However, they do not allow a way to compare two reports.

Why this is a problem:

With no way of comparing two reports, a new machine may be present and the administrator will have no knowledge of that. Said machine could be malicious.

Benefits:

- Provides administrator with useful information
- Makes viewing reports quicker
- Possibility of a configuration file for administrators to compare data in specified intervals

Solution:

Nmap is one of these network scanning tools. An extension of nmap, ndiff, compares the outputs of two nmap files and prints the results in a format similar to that of the Unix command diff. The purpose of this project is to improve on this output so that administrators can get more information out of the results of the ndiff program.

Before

```
-Nmap 5.00 at 2010-03-01 13:00
+Nmap 5.00 at 2010-02-28 13:00

+sheol.cerias.purdue.edu (128.10.247.57, 00:30:65:4D:C9:BA):
+Host is up.
+Not shown: 999 closed ports
+PORT   STATE SERVICE VERSION
+22/tcp open  ssh

-golgafrincham.cerias.purdue.edu (128.10.247.62, 00:16:CB:D1:4D:49):
-Host is up.
-Not shown: 1000 filtered ports

-dhcp-254-1.cerias.purdue.edu (128.10.254.64):
-Host is up.
-Not shown: 999 closed ports
-PORT     STATE SERVICE    VERSION
-3689/tcp open  rendezvous

-dhcp-254-2.cerias.purdue.edu (128.10.254.65):
-Host is up.
-Not shown: 997 closed ports
-PORT    STATE SERVICE      VERSION
-135/tcp open  msrpc
-139/tcp open  netbios-ssn
-445/tcp open  microsoft-ds
```

After

```
Found 44 Services and 24 Hosts Today
Difference of 3 Services and 2 Hosts from Yesterday
Difference of -7 Services and -2 Hosts from a week ago
Difference of 10 Services and 11 Hosts from a month ago
```

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center