

## **I-1. Abstract**

The design of the small secure network comprising our senior design was completed last semester, while this semester our senior design has focused on implementing the network and security. The steps taken to implement the network consisted basically of installing the hardware, connecting it to the network we built last semester, loading applications, and configuration of the network and applications. The firewall and server have also both been installed and configured, though at the time of this report the firewall has been removed for the replacement of a faulty network card. We are now in the third and final phase of our senior design plan, testing.

## **I-2. Acknowledgement**

We would like to acknowledge our sponsor, Dunn's Financial Review, Inc., for the opportunity to implement our senior design. We are also grateful to our technical advisor, Mrs. Christine Hromnak, for her willingness to make time for us in her busy schedule to answer our questions and discuss the project. Our gratitude also extends to Professor Bruno, our faculty advisor and course coordinator, for his advice, guidance, and patience.

## **II. Project Progress**

The network architecture had been designed and the hardware was purchased last semester, therefore the installation and configuration of the base network architecture was relatively straightforward this term.

Upon completion of the initial network configuration a common operating system (Windows 2000) was rolled out across the network to allow uniform traffic of background protocols. Once uniformity was achieved the Verizon DSL connection to the internet was tested and troubleshooted. The configuration of the Windows 2000 operating system across the network was somewhat tedious. Constant changes had to be implemented as the new platform was rolled out, tested and customized to the clients needs, as well as overcoming numerous Windows 2000 foibles.

The approach taken to develop our prototype firewall is extremely meticulous and detailed. We have chosen to approach the implementation gradually, to allow enough time for precise documentation of every step taken during installation. Our reasons to slow down the implementation process are as follow:

- ◆ Compile documentation for a precise mirrored installation to be undertaken by anyone following our directions.
- ◆ Document configuration changes to trace possible problems with the prototype to their root without having to guess on steps previously taken.

The functionality of our prototype secure network has proven to be superior to what we expected. The secure beacon to the internet has provided much easier access to the World Wide Web that has not only sped up existing digital interactions but also created new ways of doing business. We have customized the network to our client's needs helping Dunn's Financial Review, Inc. move into the digital age with much of their old manual transactions.

The performance of our prototype has been as expected up to this point. The expected speed of 10 Mbps has been retained; however, the changes being implemented over the next few weeks will allow us to test in depth the performance of the network. Over the next weeks the Unix based operating system will be stressed by constant queries originating from our testing facility at Stevens.

ADSL line provided by Verizon Wireless				
Throughput (ADSL Line)		Max IP Packet		packets/sec
640000	Kbs	12000	bits (1500 bytes)	53.3333
1600000	Mbs	12000	bits (1500 bytes)	133.3333
7100000	Mbs	12000	bits (1500 bytes)	591.6667

The following critical components were acquired for implementation:

- Complete Tool Kit
- 500' White Cat 5 Enhanced Plenum
- Jacks and cover plates
- 3 Com Switch
- Dell Poweredge 300 Firewall without Operating System
- Dell Pentium IV Server 1400
- Dell tape backup 650
- UPS

Phase III of our senior design is our testing and security assessment phase, and it is broken into phases as well.

#### **Sub-phase 0: Tool Selection & Documentation**

We will be using several tools throughout the course of Phase III. The tools we will be using range from small utilities, such as ping, traceroute, and netstat, to scanners such as nmap and nessus to full-blown network monitoring software from Solar Winds.

#### **PING:**

- A utility that sends a series or continuous stream of icmp echo requests and waits for an icmp echo reply. After words the program the returns pertinent statistics such as, the round trip time and the number of messages that made it through.

#### **TRACEROUTE:**

- A program which provides the major routes between yourself and the destination host

#### **NETSTAT:**

- A program that will output to the screen (or file) the number of open sockets (connections) on the local host.

#### **NMAP:**

- "Nmap is a utility for port scanning large networks, although it works fine for single hosts. The guiding philosophy for the creation of nmap was TMTOWTDI (There's More Than One Way To Do It). This is the Perl slogan, but it is equally applicable to scanners. Sometimes you need speed, other times you may need stealth. In some cases, bypassing firewalls may be required. Not to mention the fact that you may want to scan different protocols (UDP, TCP, ICMP, etc.). You just can't do all this with one scanning mode. And you don't want to have 10 different scanners around, all with different interfaces and capabilities. Thus we incorporated virtually every scanning technique we know into nmap specifically, nmap supports:
  - Vanilla TCP connect() scanning,
  - TCP SYN (half open) scanning,
  - TCP FIN, Xmas, or NULL (stealth) scanning,

- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses some packet filters),
- TCP ACK and Window scanning,
- UDP raw ICMP port unreachable scanning,
- ICMP scanning (ping-sweep)
- TCP Ping scanning
- Direct (non portmapper) RPC scanning
- Remote OS Identification by TCP/IP Fingerprinting, and
- Reverse-ident scanning.

nmap also supports a number of performance and reliability features such as dynamic delay time calculations, packet timeout and retransmission, parallel port scanning, detection of down hosts via parallel pings. Nmap also offers flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, and output to machine parseable or human readable log files.” This description along with the scanner can be found at

[www.insecure.org/Nmap](http://www.insecure.org/Nmap).

#### **NESSUS:**

- The "Nessus" Project aims to provide to the Internet community a free, powerful, up-to-date and easy to use remote security scanner. A security scanner is software, which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way. Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability. Nessus is very fast, reliable and has a modular architecture that allows you to fit it to your needs.” This description along with the scanner can be found at [www.nessus.org](http://www.nessus.org).

#### **SOLARWINDS Network Management Toolset:**

- “The SolarWinds Network Management Toolset is a collection of popular Network Management, Network Monitoring and Network Discovery Tools. SolarWinds utilizes SNMP and ICMP in the discovery and monitoring of many networking devices and MIBs (management information base). Designed to work with not only Cisco routers, Cisco bridges, and Cisco switches but also routers, bridges and switches, hubs and servers from other companies like Bay Networks, Novell, HP, Dell and more.” A trial version of this software can be found [www.solarwinds.net](http://www.solarwinds.net).

#### **Sub-phase 1: Testing**

During this phase the firewall will be tested both internally and externally. When conducting internal testing we will be looking for conformation that our network applications are able to work seamlessly with the firewall. Applications such as web browsers, instant messenger clients, and ftp clients, just to name a few, must be able to access the internet without the possibility of being blocked. During external testing we will be testing the firewall software itself. Tests will be performed against the rule set to make sure that the firewall is working properly. We will also be conducting OS specific

tests to make sure that the operating system that our firewall is running on is up to date. We will conclude by conducting denial of service tests to see how reliable the firewall is. This last test will give us an accurate indication of the maximum load that the firewall can handle before failure.

### **Sub-phase 2: Analysis, Documentation & Recommendation**

Data that we collect from our testing phase will then be analyzed from which we will produce our documentation and recommendations. Copies of our documentation, recommendations, and data collected throughout our review will be distributed to Dunn's Financial Review as well as included in our final report.

As of this moment we are currently finalizing our installation and will begin serious testing within the next two weeks. Testing to date has been ad hoc in order to make sure that our hardware and software is working so that the client can utilize the network even though it has not been fully upgraded.

The risks of our design are limited to the stress applied by potential attackers on the system. The firewall's main memory is limited to 128 Megabytes. The simultaneous processes that can be started by such a system are limited compared to the amount of queries that can be opened per second by a potential attacker. We believe that the risk of a buffer overflow has been mitigated by our use of Stateful inspection on originated packets. Our firewall will only allow traffic to pass if it was originated on the inside network. Only traffic that has been registered on the internal Stateful inspection table will be routed and all the rest will be dropped. Due to the limited number of employees having access to the server at any given time we believe the risk of a crash has been minimized.

A further risk remains that the intrusion detection system if not actively monitored may not only be useless in preventing attacks, but may be used to overload a system buffer. Long running logs may be overwhelming for the system after a long period of time. Upon discussing the issue with the client we have decided to omit the Intrusion Detection System and simply utilize the firewall to monitor the incoming packets.

The largest problem we have encountered is the probability of having to provide support to the client for the hardware installed on the network. We believe that a thorough professional job requires us to install a network solution that can be maintained functional at any point in time by the client. We have assessed our point of failure to be the BSD firewall. Scarce technical support exists for this operating system and all hardware purchased by our client was required to be under a Dell support contract. Therefore we have decided to change the operating system of our firewall from BSD to Linux. Utilizing the Linux operating system we have been able to obtain a support agreement from Dell, as Dell supports Red Hat Linux 7.0

A revised and updated budget for Team Seventeen is shown below.

<b>Team 17 Expenses (revised)</b>	<b>EM/EE/CpE 416</b>
Phone charges	\$56.00
Fuel expenses	\$236.00
Meal expenditures	\$0.00
Printing costs	\$40.00
<b>Total</b>	<b>\$332.00</b>

- ◆ Phone charges are estimated as a group total, including each members hard-wired and cellular phone charges, as ten minutes of toll usage per week per member regarding Network Design & Innovation at a rate of \$.10 per minute for a fourteen week semester.
- ◆ Fuel expenses were calculated using a cost of \$.32 per mile, 9 trips this semester of one vehicle per group trip of 82 miles per round trip.
- ◆ There have not been any meal expenditures this semester that Team Seventeen has had to pay for.
- ◆ Printing costs are an estimation of the sum of individual group members printing costs in regards to Network Design & Innovation.

These numbers may be compared to the estimated budget included in the Final Design Report, below.

<b>Team 17 Expenses (estimated)</b>	<b>EM/EE/CpE 416</b>
Phone charges	\$40.00
Fuel expenses	\$50.00
Meal expenditures	\$120.00
Printing costs	\$40.00
<b>Total</b>	<b>\$250.00</b>

A Gantt chart is attached relating the Team Seventeen project schedule.

### **I. Conclusion**

Based on the information we have, we can expect that this senior design, as specified in the Final Design Report with the stated modifications, will be successfully completed and tested by the end of the Spring 2001 term.