Global Information Assurance Certification Paper

The State of Intrusion Detection

Intrusion Detection in a Wireless LAN Environment: There's Something in the Air

Gary Smith

GCIA Practical Assignment

Version 3.1

The State of Intrusion Detection

Intrusion Detection in a Wireless LAN Environment: There’s Something in the Air

Introduction

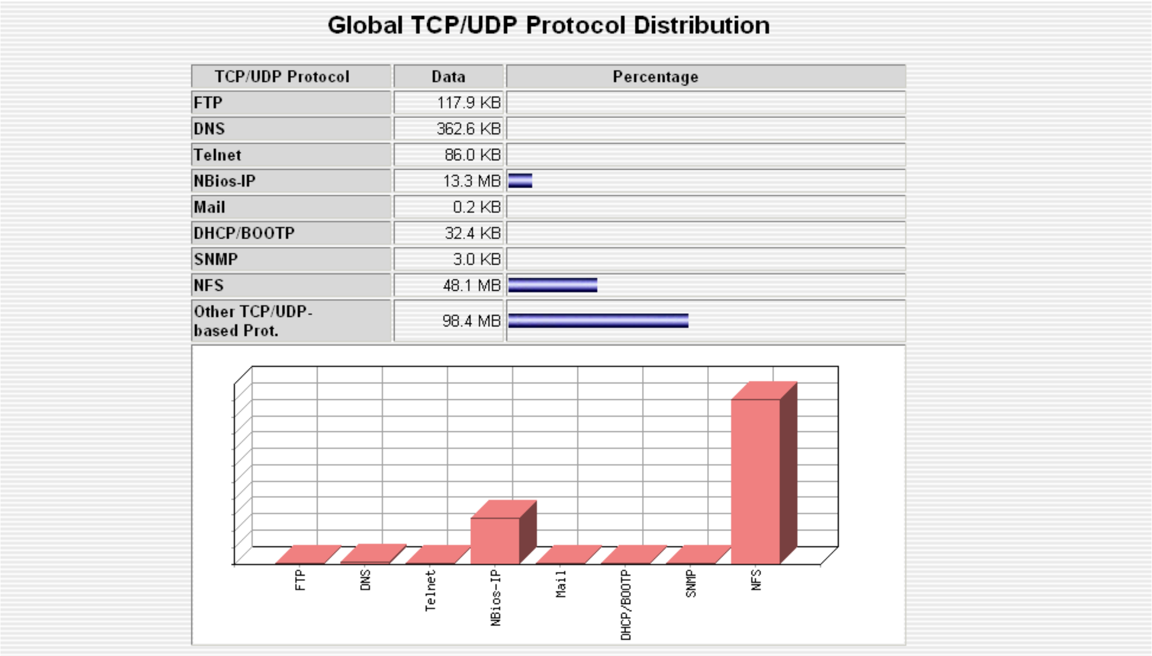
When I was charged with setting up and securing the wireless LAN at my site, I saw this as an opportunity to set up a network with intrusion detection as far of its initial infrastructure and explore the new frontier of intrusion detection on a wireless LAN.

Initial Traffic Characterization

Before the installation of the wireless LAN, I characterized the traffic on the existing wired LAN the wireless LAN was to replace. To characterize the wired LAN, I used the open source program, *ntop* by Luca Deri. Ntop is to networks what top is to Unix systems, but more. Ntop can

- Sort network traffic according to protocols
- Show network traffic sorted by various criteria
- Display traffic statistics
- Show IP traffic distribution among the various protocols
- Analyze IP traffic and sort it according to the source/destination
- Display IP Traffic Subnet matrix, i.e., who's talking to whom
- Report IP protocol usage sorted by protocol type
- Perform light-weight intrusion detection

Some examples of ntop’s output are shown below.



Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Percentage
FTP	117.9 KB	
DNS	362.6 KB	
Telnet	86.0 KB	
NBios-IP	13.3 MB	
Mail	0.2 KB	
DHCP/BOOTP	32.4 KB	
SNMP	3.0 KB	
NFS	48.1 MB	
Other TCP/UDP-based Prot.	98.4 MB	

Figure 1 – Global TCP/UDP Protocol Distribution

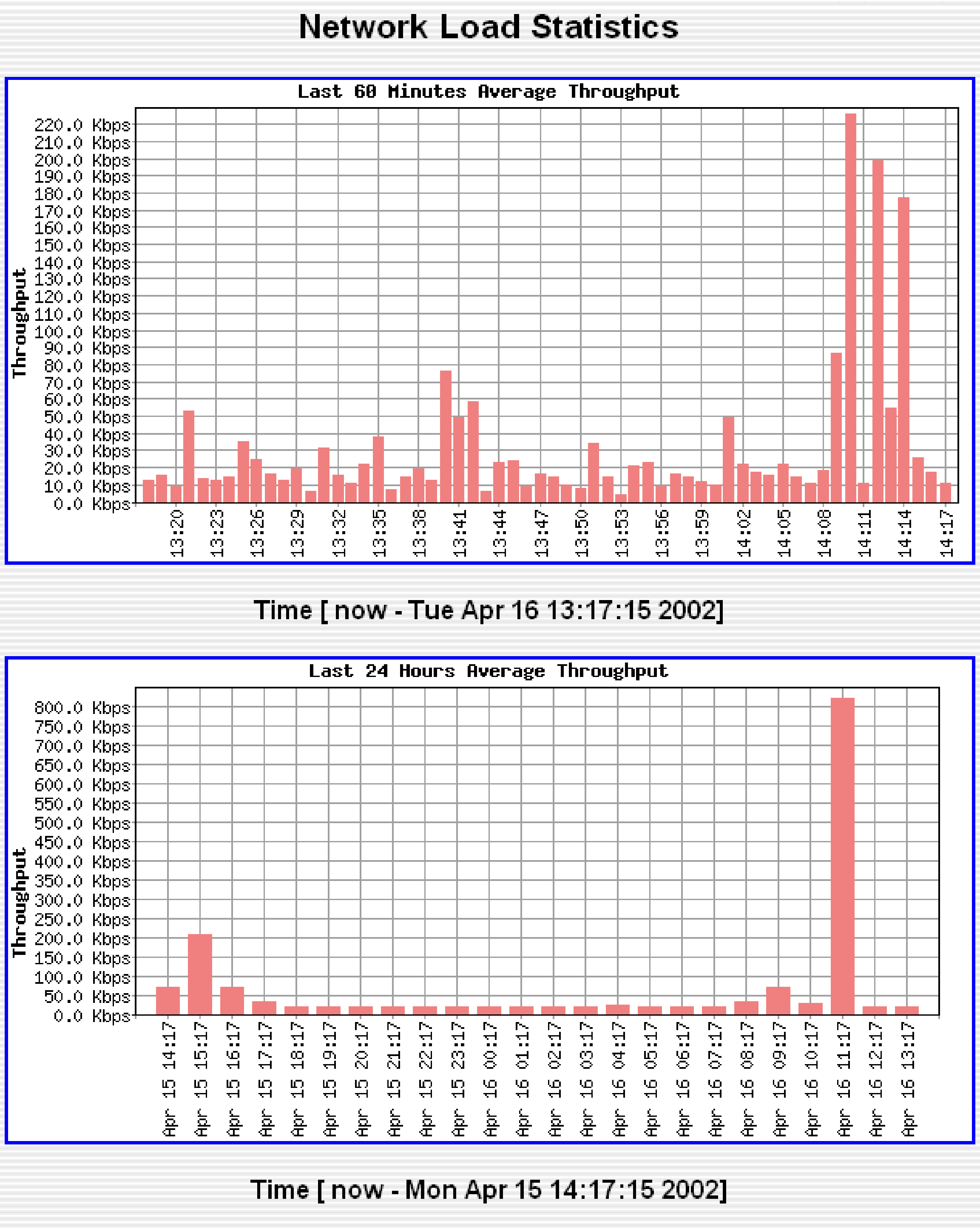


Figure 2 – Network Load Statistics

From information produced by ntop, I was able to characterize the traffic types and patterns of use on the wired LAN. Given that the types of systems are a mixture of Unix/Linux workstations and servers doing design and simulation and PC's running

Windows XP and Microsoft Office applications, there were no surprises about unusual services being used or peculiar usage patterns. This is shown in Table 1.

Protocol Name	*Port Number*	*Transport*
DNS	53	UDP
HTTP	80	TCP
HTTPS	443	TCP
Lpr/Lpd	515	TCP
Microsoft Windows	137,138,139,445	UDP
NFS	2049	UDP
SMTP	25	TCP
Sun RPC	111	UDP
Telnet	23	TCP
X windows	6000-6100	TCP

Table 1 – Protocols in Use on the Wired LAN

A second type of characterization of the wired LAN involves using nmap. Nmap is a utility for network exploration or security auditing. It supports ping scanning to determine which hosts are up, many port scanning techniques to determine what services the hosts are offering, and TCP/IP fingerprinting to determine remote host operating systems With an nmap scan, I compiled a baseline of IP addresses and the OS associated the address.

Installation

The topic of installing a wireless LAN is deserving of a paper unto itself. However, I want to briefly address some aspects of the installation that relate to intrusion detection.

- Know where the Wireless Access Points (WAPs) are physically located. Armed with this knowledge, you can identify an authorized WAP from a renegade WAP.
- Know the IP addresses of all authorized WAPs. If your detection mechanisms detect an unauthorized IP address, you can identify an authorized WAP's IP address from a renegade WAP's IP address.
- Most WAPs are manageable via SNMP. At the very least, change the default community string to something other than "public". Treat this information as if it were the password to "root" on Unix or the domain administrator on Windows by limiting its knowledge.

- Know the limits of your wireless perimeter. Take a laptop with a wireless Ethernet card and walk around your work area. By watching the “link light”, you can determine the perimeter of your network. If possible, do the same in the floor above and below your area. Also, check across the street in restaurants and coffee shops. Something to keep in mind while establishing the perimeter is a connection to a WAP at a lower speed of 1 or 2 Mb is still a connection.

- Set up the WAPs to log events to a central log server.

- Select your security software. I selected the following open source software tools for intrusion detection:

    - Ntop. As mentioned previously, ntop is to networks what top is to Unix systems.

    - Snort. Snort, written by Martin Roesch, is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

    - ACID. ACID stands for Analysis Console for Intrusion Databases. ACID is a PHP-based analysis engine to search and process a database of incidents generated by security-related software such as IDSes and firewalls e.g., Snort or iptables. It provides a search interface for finding alerts matching practically any criteria.

    - EtherApe. EtherApe is a GNOME/pcap-based etherman, interman, and "tcpman" clone. It displays network activity graphically. Active hosts are shown as circles of varying size, and traffic among them is shown as lines of varying width. It supports Ethernet, FDDI, Token Ring, ISDN, PPP, and SLIP. Additional statistics windows will let you concentrate on protocols or nodes.

- As a result of redeployments, we had extra low-end Pentium 3 class PC’s available for use. I converted some of the desktop units to be a dedicated intrusion detection sensors and a dedicated log server. A laptop was converted into a mobile wireless tester.

Detection

The Usual Suspects

The manufacturers of wireless LAN equipment have gone to great lengths to insure that wireless LANs appear to operate like their wired brothers only without wires. This also insures that they are subject to any form of attack a wired LAN is capable of sustaining such as SYN/FIN, Smurf, or Loki. So, the same set of principles for intrusion detection on a wired LAN also applies to a wireless LAN: multiple intrusion detection sensors: update the intrusion signatures as soon as new ones become available, log information from multiple sources, and review logs often and regularly.

Odd Traffic

One of indicators of an intrusion is the appearance of odd traffic. Having characterized what was "normal and expected" traffic and utilization patterns before the implementation of the wireless LAN, something new might indicate an intrusion. For instance, the sudden appearance of IRC, Gnutella, or Morpheus in an ntop display might indicate the presence of a Freddy Freeloader on your network. Similarly, a sudden increase in a known activity such as FTP, mail, or HTTP might indicate a Freddy Freeloader or a malicious intruder thieving company information.

Odd MAC Addresses

If you're lucky enough to have purchased all the wireless equipment from a single vendor, the vendor portion, i.e., the first 6 hex digits of the MAC address for all the wireless clients will be the same. If a MAC address pops up in an ntop report/display, or EtherApe display, or Snort alert that does not have a similar vendor portion, an intrusion may be occurring. This is not a 100% indicator of an intrusion because some wireless LAN cards will allow you to change the MAC address under program control.

Slow Response

Users are always complaining of about slow response of the network. Complaints about slow response should be taken seriously and may indicate an intrusion-in-progress. An EtherApe display will show which systems are instantaneously getting the lion's share of the bandwidth.

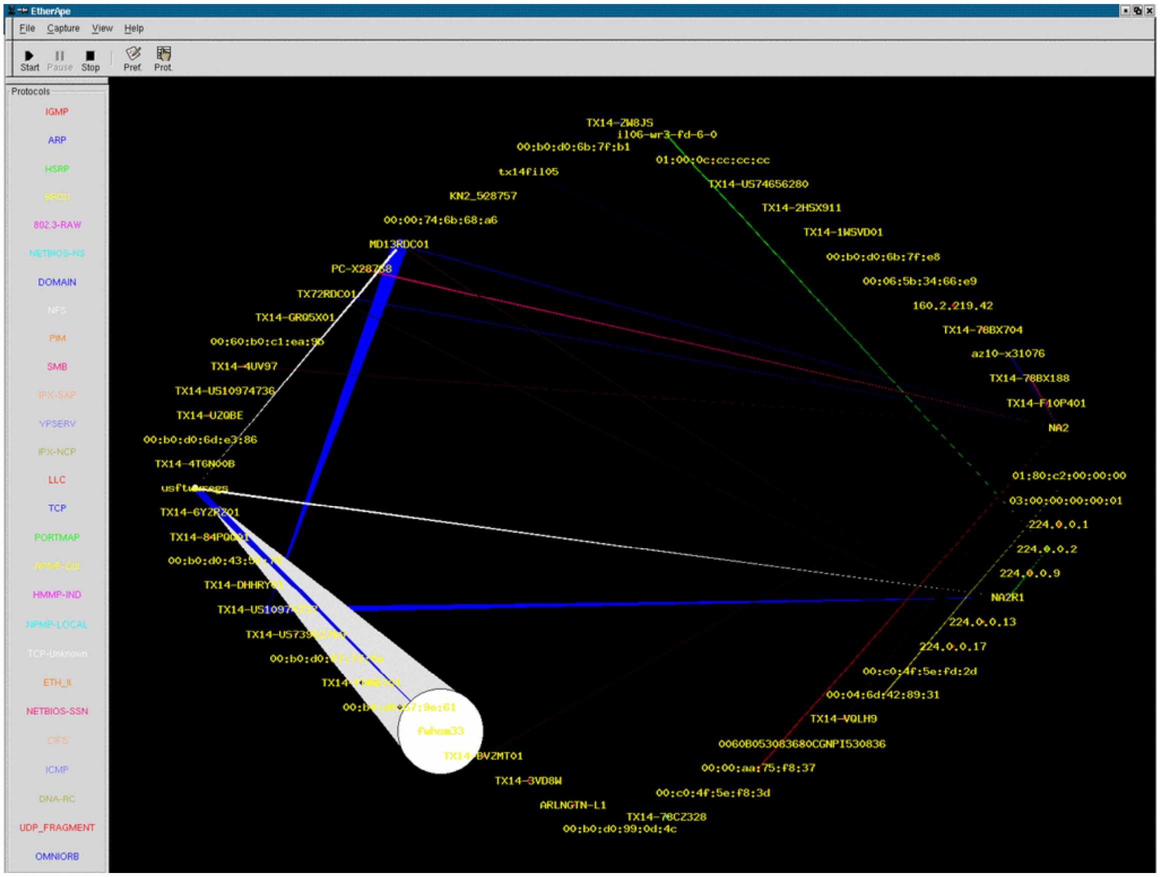


Figure 3 – EtherApe in Operation

The wireless LAN should be periodically nmap-ed. This will yield what IP addresses are extant at the time of the scan. Next, fingerprint the OS of the extant systems on the wireless LAN. Compare this against the characterization done in pre-wireless LAN times. The presence odd OSes, for instance Windows 95, Windows 98, or Windows ME in an all Windows XP environment, indicates some type of intrusion has taken place

Renegade WAPs.

Renegade WAPs are a large cause of intrusions in a wireless LAN. Renegade WAPs are due to two factors: well meaning individuals and individuals with malicious intent. A well-meaning individual might install a WAP himself. Wireless LAN cards and WAPs have gotten inexpensive and are readily available at CompUSA, Best Buy, and Fry’s. The renegade WAP in this case is probably set up without any encryption and the default SNMP community set to “public” as it comes out of the box. Set up this way, anyone with a wireless LAN card could connect to the renegade WAP and consequently, your network. This is why it is important to know where each WAP is physically located and know its IP address. Renegade WAPs will show up in nmap sweeps, ntop reports/displays, and EtherApe displays. Periodically physically sweeping the work areas can turn up a renegade WAP. Also, walk around with a laptop and a wireless card and a program such as Netstumbler or Kismet to map WAPs. Finding a renegade WAP is not a good time make network policy decisions. Before the wireless network is in place, policy and procedure for dealing with renegade WAPs need to be in place. These will guide you if someone will ‘fess up to putting in the renegade WAP or if they don’t.

Denial of Service/Man-In-The-Middle

Wireless LANs by their very open nature are subject to denial of service intrusions. The intruder doesn’t have to be located on your premises to attack; they could be across the street in a coffee bar. Neither does the intruder need wireless LAN equipment to cause a crude denial of service. All the intruder needs is some device that operates at 2.4 GHz just as wireless LAN equipment does. At the next level up, there is the unconnected WAP intrusion. In this scenario, the intruder puts a powered-up WAP in the vicinity of the users. Since wireless LAN cards are designed to connect with the strongest signal in their area, it is as if they are connected to a black hole. Man-in-the-middle intrusions are possible with wireless networks. The intruder sets up a WAP to mimic the configuration of a bona fide WAP on your network and inserts it in the general area of the user base. Users’ systems connect to the intruder’s WAP if its signal strength is sufficient to overwhelm a real WAP in the same area. The intruder can copy, record, modify, and reinsert packets back into the data stream. This is why it is vitally important to know where your WAPs are physically located, and their IP addresses. In addition, frequently conduct regular sweeps for signal strengths with a mobile device such as a laptop and Netstumbler or similar program.

False Positives

Wireless LANs are subject to intrusion false positives just as wired LANs but some are unique to the radio frequency nature of wireless LANs. For instance, some of the users on the wireless LAN would experience an outage between 11:30am and 12:00am. It turned out the culprit was a microwave oven with a leaky door seal and not some nefarious intruder trying to take out our wireless LAN. The short-term fix was to reposition the microwave oven so that it pointed away from the users’ offices. The long-term fix was to have facilities replace the microwave oven. Another instance of a false positive was harder to track down. Users in one area would aperiodically loose connection to the WAP in their area. The random nature in which they would loose connection seemed to suggest it was not an attack against the wireless LAN. After some investigation, it was determined the area above the affected users was the computer room for another business. The computer room had a wireless telephone in it so the administrator would not be tied down to the length of a telephone cord while troubleshooting a problem. This model of telephone operated at 2.4 GHz as do wireless LAN devices. When outage times were compared with times the system administrator was on the phone, the mystery was solved. The lesson to learn from these two examples is a lesson from wired LANs: Don’t Panic! Consider the medium first before jumping to conclusions.

Summary

Wireless LANs present many new possibilities for the intrusion analyst. Intrusion analysts can make the most of these possibilities by taking these steps:

- Characterize the traffic and bandwidth utilization on the wired LAN before the wireless LAN is implemented. Having done this, the intrusion analyst will know what is "normal and expected".
- Know where the WAPs are physically located in the network and their IP addresses.
- Determine the perimeter of the network.
- Select, install, and configure intrusion detection tools as part of an overall intrusion detection framework.
- Look for activities that do not conform to the "normal and expected" seen in the characterization, e.g., the sudden appearance of applications like IRC or Gnutella, odd IP or MAC addresses, slow response, and unusually high traffic.
- Make frequent and regular sweeps for renegade WAPs. Unsecured, renegade WAPs are an open invitation to intrusion.
- Make frequent and regular sweeps using nmap for unaccountable IP addresses or operating systems.

References

Cowell, Ruth, War Dialing and War Driving: An Overview, http://rr.sans.org/wireless/war.php, June, 2001

Danyliw, Roman, "Analysis Console for Intrusion Databases (ACID)", http://acidlab.sourceforge.net/, July, 2001

Deri, Luca, "ntop – network top", http://www.ntop.org/ntop.html, February, 2002
Ellison, Craig, "Wireless LANs at Risk", http://www.pcmag.com/article/0,2997,apn=2&s=1482&a=23839&ap=1,00.asp, April 2002

Fyodor, "Nmap", http://www.insecure.org/nmap, March 2002

Kershaw, Martin, "Linux 802.11b and wireless (in)security", http://www.linuxsecurity.com/feature_stories/wireless-kismet.html, March, 2002

Meredith, Gail, "Securing the Wireless LAN", http://www.cisco.com/warp/public/784/packet/jul01/p74-cover.html, July, 2001

O'Farrell, Neal, Bautts, Tony, Ouellet, Eric, Hack Proofing Your Wireless Network, Rockland, MA, Syngress Publishing, March, 2002

Owen, Daniel, "Wireless Networking Security: As Part of Your Perimeter Defense Strategy", http://rr.sans.org/wireless/netsec.php, January, 2002

Roesch, Martin, "Snort Users Manual", http://www.snort.org/docs/writing_rules/, March, 2002

Toledo, Juan, "EtherApe, A Graphical Network Monitor", http://etherape.sourceforge.net, April, 2001

Zhang, Yongguang and Lee, Wenke, "Intrusion Detection in Wireless Ad-Hoc Networks", The Sixth Annual International Conference on Mobile Computing and Networking, Aug 2000