

Penetration Testing on a Switched LAN

By,

Brian Wilson

CCNA, CSE, CCAI, MCP, Network+

Slimjim100@gmail.com

www.middlegeorgia.org

www.middlegeorgia.info

In this article we will explore the presence of known vulnerabilities in switched LAN's. I hope to open your eyes on some of the techniques & tools that can be freely downloaded and used to test your network. Let's start out with some of the basics we see in most small to medium networks. Now we need to start assessing the network and gathering information on it. We need to look at a few things first to better understand the obstacles we might face on a pen test. Start with these basic questions as a foundation to gathering information.

Where are the switches located?

Can you gain access to the equipment?

What kind & type of switches or hubs are in the network?

Are the switch's manageable and do they have a web interface?

What is the physical topology or design of the network?

Do the switches have security features (IDS) and are there VLAN's being used?

Once we have the basic information on the network design and the equipment used in the network we need to research the vendor's security bulletins to see if there are any known exploits to test. If this network has wireless there are a lot of other techniques we can deploy to find vulnerable points. At this point we should also look at what Physical media is used to move data on the network (CAT5, Fiber, or Wireless). Once you know what the network media is you can figure out the best way to tap into it. Below are some ideas on tapping into the network and tools used.

Ethernet (CAT3, CAT5, or CAT6):

To tap Ethernet it's normally done by using a protocol sniffer like Ethereal. To sniff on an Ethernet LAN you need to have access to the network via switch port or other network connection.

Fiber (Gig-e or FDDI):

To tap a fiber network you need an optical splitter like "netoptics". To tap with a splitter you will have to have access to the fiber lines. Once you have the splitter installed you can run ethereal or any other network sniffer.

Wireless (802.11 A, B, & G):

To tap wireless you need to first identify what kind of signal the network is using. Most common networks will be using 802.11 B or G but there are some networks that have an 802.11 A. To find out what the type of wireless is you can run software like Network Stumbler. Network Stumbler will allow you to see the access points and all the need info about them like the channel, signal, encryption used. Once you know what if the AP is open or encrypted you can plan your path to accessing the network. If you find the wireless network is encrypted you will have to find tools to crack the encryption. For WEP encryption you can use tools like AirCrack to break the encryption. Once you have gained access to the wireless network you will use a network sniffer like ethereal to capture packets.

Sniffing/ Tapping the Network

As I have stated above Ethereal is a very good (and free) network sniffer but there are many other protocol Sniffing tools on the internet many are free but some vendors charge for their tools. The idea behind sniffing is that you can see all the packets on the network. With the ability to see

the packets and capture them you can reconstruct the data that flows over the network and gain access to passwords and password hashes. Other useful data you can collect is e-mails, website data, database info, & a lot of other sensitive info. Some obstacles you may face sniffing is that if the network is switched you will only see broadcast traffic and traffic directed to your IP. To solve this problem you will have to sniff on a trunk port, mirror port, or spoof the network traffic to pass through your port. One good tool to sniff and spoof is Cain & Able, with Cain you can also sniff for VoIP calls and many other passwords.

Port Scanning

Port scanning is a way of testing network devices to see what communication ports might be open. This can be done from a LAN, WAN, MAN, or the internet. Port scanners are some of the most used tools by pen tester to see what is open and how to best identify devices and services running on network devices. For example if you port scan an IP and you see port 25 open then there is a possibility that a mail service is running. Next step to test port 25 might be to telnet to the port and see if the reply is a banner. If the device is a mail server it will normally report back to your telnet session with a service banner. Microsoft Exchange server will report its SMTP name and the version of Exchange running on the server. Other interesting ports are 23 Telnet, 21 FTP, 23 SSH, 80 HTTP, 443 HTTPS, and 3389 Terminal servers (RDP). Some good programs for port scanning are SuperScan (from foundstone), Nmap (from insecure.org) and X-scan (from xfocuse.com). There are hundreds of scanners on the internet and many are specialized for scanning for certain services or exploits. If you want more information on port scanning just Google it and you will be busy for months.

Password Recovery

Password recovery can be done remotely or physically with software. On windows PC's you can run programs remotely like PWDump and if you have access you can run many different kinds of bootable disk to change and recover passwords. Other password recovery methods include running Hash or Sam files recover tools from the PC on a users account. With the SAM file of Hashes you can then proceed to crack the hash to gain the password.

Password Cracking

Password cracking is done by taking an encrypted value (Hash) and using a technique to crack or reverse engineer it. A few common type of cracking is running deanery, Burteforce, or Cryptanalysis attacks on the hash. There are many programs on the internet to run dictionary & Burteforce attacks but the fastest way to crack passwords is to use rainbow Tables on them. There are a few rainbow tables cracking sites online and the program rcrack.exe is a free download with source code from "antsight.com/zsl/rainbowcrack" The most popular site to crack hashes online is plain-text.info and they allow 2 hashes free per hour to crack. With rainbow tables a pen tester's life has gotten a lot easier. Older methods of cracking like "Burteforce" can take months to crack a password and dictionary attacks only work if the password is a common word.

So far we have discussed how to analyze a network and then profile it for a pen test. We have also covered ways to tap/sniff the network for data. With the little info we have discussed it should prove as a good primer session to show you where to start with pen testing. All the tools mentioned in this article are easily found on the internet and all the tools talked about in this article are free for download. If you need any help with pen testing just use the internet as there are many guides around that cover specialized areas of pen testing. Remember that the whole idea behind pen testing is to learn and secure your network.