Cyber Security Applications: Freeware & Shareware

Gary Rogers
Professor
Palm Beach State College
4200 S Congress Ave
Lake Worth, FL 33461
rogersgs@palmbeachstate.edu

Tina Ashford
Professor of Information Technology
Middle Georgia State College
100 College Station Drive
Macon, GA 31206
tashford@mga.edu

Abstract:

This paper will discuss some assignments using freeware/shareware instructors can find on the Web to use to provide students with hands-on experience in this arena. Also, the college, Palm Beach State College, via a grant with the U.S. Department of Labor, has recently purchased a unique cyber security device that simulates cyber security attacks upon servers/hosts/devices. Information on this is also discussed and included herein.

Cyber Security Topic Area: Firewalls

ASSIGNMENT: Run Shields UP! save this analysis (you can print screen it or save it; your call). see https://www.grc.com/shieldsup. Also, run the LeakTest test as well at https://www.grc.com/lt/howtouse.htm.

ZoneAlarm is one of the most secure and proven personal firewall products you can purchase. Zone-Alarm protects over 80 million PCs from viruses, spyware, hackers and identity theft. The award-winning Internet security product line is installed in consumer PCs and small businesses, protecting them from Internet threats. I use it at home myself for additional protection.
Download the free version at their website at
http://www.zonealarm.com/security/en-us/trial-download-zap.htm.

Go to CNET.com and download one of their free Internet speed testers. Examples are Broadband Speed Test or Internet Speed Test or CNET Bandwidth Meter or any one of a hundred others. Install it. Turn it on so it will be testing your Internet connection and measure how fast it is. Record/remember this as you surf a bit on the Net.

Next, let's test your new ZoneAlarm. Begin by surfing a location on the Net. Then send an email to anyone. Proceed with this process for several minutes. Pay close attention to your Internet speed and any messages which may appear.

Then produce a one-page analysis of this product. Evaluate it in these categories:

- ⌃ Ease of installation
- ⌃ Price
- ⌃ Platforms supported
- ⌃ Execution (how well did it execute? did it continually interrupt your life with annoying messages? did you notice any degrading of your Internet speed after it was installed and executed? and so on...)

Run Shields Up! and LeakTest again. Compare the results of this Shields UP! / LeakTest run and the earlier one you performed before you installed ZoneAlarm. Report on any differences. Also, submit a print screen of each of these tasks.

Cyber Security Topic Area: Authentication

Go here: http://www.majorgeeks.com/mg/sortname/password_recovery.html. These are FREE apps that perform various password recovery/discovery functions. There are many other password apps on the web at www.download.com or other locales...Simply locate some password cracker/recovery apps and try them out in order to get a good idea what they are like, what capability is out there in this domain, etc. You can fine them all over the Web. It is your choice where you get them.

Download, install and execute three of these apps. Produce a brief report where you report as follows:

Include a screen shot of each running on your computer.

- ⌃ Price
- ⌃ Platforms supported

For each: A one-paragraph report analyzing how it works, whether it is effective, when it was/was not effective, etc.

Include a screenshot of each app running on your system.

Compare/contrast them. Which would you use and why?

Dashlane

Go to www.dashlane.com.

Install and execute this app. Dashlane saves your passwords when your visit websites and stores them in an encrypted folder. Only by entering ONE master password, can this folder be accessed so it provides enhanced security. Also, and perhaps as importantly, you no longer have ot memorize a log id and password for all your websites from Amazon to eBay and so on since Dashlane memorizes them for you. Very handy tool.

Execute Dashlane and produce a report on how well it executes. Is it effective? What are its strengths/weaknesses?

Include a screenshot of its execution and upload all this.

Cyber Security Topic Area: Network Monitoring

In order to be an effective network administrator, you MUST know how to capture/look at and analyze the data on your network. Wireshark is the acknowledge tool of choice to do this. Therefore, you MUST know it!

For this assignment, analyze the attached Wireshark sample and provide ten insights into it. You must produce ten facts about the captured data.

Upload a file where you document your findings AND a screenshot of its execution on your system. Wireshark can be found in various locations on the web including https://www.wireshark.org. << you can also include another network monitoring tool such as *tcpdump* if you desire >>

Cyber Security Topic Area: Wireless Security

   Did you forget your wireless password again? At a friends house and they have no idea what their login information is? Well, there are several tools out there to help you. Unfortunately, hackers sometimes use them as well for nefarious purposes (but YOU won't!)

Download WiFi Password Hacker for Android at
http://www.apk4fun.com/apps/com.brnk.apps.wifihacker/
---- or ---
Download WiFi password revealer at http://wifi-password-revealer.soft112.com/.

WiFi password revealer is a small program which will show you all stored passwords to your wireless (WiFi) network(s). Each time you connect to a wireless network using a password - Windows OS encrypts and stores it in the system. This program (WiFi password revealer) will find, decrypt and show you all your WiFi passwords, whenever it is your home wireless network with WPA / WPA2 encryption or WEP network in a coffee-shop.

WiFi password revealer can recover WiFi passwords from on Windows XP, Windows Vista, 7 and 8.
--- or ---
Download WIfi Password Finder. This tool can locate passwords on WEP, WPA, or WPA2 WLANs. It's very simple -- you can use it by clicking one button. http://wifi-password-finder.com/

Submit a one-page analysis of your efforts and screen shots of them running on your system. Select any two of these (or a similar tool from somewhere else).

Advanced IP scanner

Download this app (Advanced IP Scanner OR another app called Angry IP Scanner.. Install and execute one of these. Or, select a similar app to this one. You can find them from various places on the web. Here is one: www.***angryip***.org or www.advanced-ip-scanner.com.

Produce a one-paragraph report where you describe the operational characteristics. Include a screen shot of its operation. What benefits can be derived from this? What did you learn?

WiFi encryption methods

There are three primary encryption methods used in wireless LANs: WEP, WPA and WPA2.

STEP 1 -- Produce a one-page paper where you discuss the evolution of these methods from the oldest, WEP, to the latest WPA2. Address the primary characteristics of each as well as how difficult is to "break" each and their strengths/weaknesses.

STEP 2 -- Also, download an app for either your Android or iPhone and attempt to hack a local Wi-Fi (whom have given you prior approval first). Develop a one-paragraph analysis of what the tool is, and each step of the process you employed, followed by your results, if any. There are many FREE apps you can download from iTunes or the Android Store for this purpose. They can easily "break" WEP Wi-Fi in a few seconds, for example. Here are several examples:
http://www.wikihow.com/Hack-Wi-Fi-Using-Android and
http://www.hackersthirst.com/2012/01/four-best-wifi-cracking-applications.html.

Cyber Security Topic Area: Web Security

Zone-H

Go to www.zone-h.org. This site contains security news and a "cybercrime archive" which quickly be-came a success story. The goals of Zone-H were to follow security trends and analyze the growing im-portance of hacktivism. Recent website defacements are shown in detail as well. Pretty fascinating.

Read this website and carefully analyze the service this organization provides. Produce a one-paragraph analysis of this site's capabilities, its value, who it benefits the most/least, etc.

Web passwords

Sterlo Wirelesss Passwords discovers web passwords you may have forgotten, etc. Pretty handy tool. see http://www.sterjosoft.com/wireless-passwords.html

Download this app, install it and execute it. Produce a screenshot of it running on your PC along with a one-paragraph analysis of its performance.

Detecting open ports

SterJo NetStalker is an interesting network tool. This is a tool that will detect all the connections to your computer. It analyzes all your ports as well. Download it at
http://www.sterjosoft.com/netstalker.html.

Install and execute it and produce a one-paragraph analysis of its performance. Did it run? What did you discover and so on.

Cyber Security Topic Area: Network Vulnerabilities

Vulnerability scanners are an extension to a sniffer. They provide a more well-rounded picture of the "holes" in your network. Select one of these found at the below location or any other vulnerability tool you can find.

See
http://www.networkworld.com/article/2176429/security/6-free-network-vulnerability-scanners.html

Install the tool and execute it. Then upload a screenshot of the tool executing on your system and a one-paragraph analysis where you discuss the tool's effectiveness. Address how you came to this conclusion. Also address the price, platforms supported, etc.

Sam Spade

Sam Spade is an excellent general purpose vulnerability tester. Many network admins use it to see how vulnerable their own networks are. It can be found at many locations on the Net. Others say "Hey, its just a cool bunch of network tools". Which do YOU think it is?

Also, see this useful document on how to use Sam Spade:
http://www.sans.org/reading-room/whitepapers/tools/sam-spade-934

Download this tool install it and execute it on your system. Use several of its functions and report on your experience!

Upload a screenshot of its execution along with a one-paragraph analysis of its effectiveness.

The Cyber Security Range/Lab
Product Overview:
http://www.ixiacom.com/products/ixia-breakingpoint

FireStorm
Product Menu
- Overview(active tab)
- Features
- Specifications
- Resources
- Test Suites

Overview:

Whether validating a single device, an application or service, or an entire network, you need real-world traffic scenarios to test against. Ixia's FireStorm™ load module blade simulates massive-scale application and security traffic to power BreakingPoint® test solutions for your students.

Providing twenty universal 1/10GE SFP+ ports, and 60 ports per 4U chassis, the FireStorm 20 combines the high performance, realism, and large port densities needed by the large-scale development and testing labs of equipment manufacturers and carriers. Alternatively, the FireStorm ONE offers a 4-port appliance that meets the portability and performance needs of enterprises, equipment vendors, and government and military organizations.

These links will provide more information as well as the demo we will show at the conference.

Tutorial 1: Starting BreakingPoint
Tutorial 2: Reserving Ports on Ixia BreakingPoint
Tutorial 3: Configuring a Network Neighborhood
Tutorial 4: Building and Running and Appsim Test
Tutorial 5: Adding Security to a Test
Tutorial 6: Reviewing the Test Reports

For more information on how to get onboard with a cyber range such as Palm Beach State College now has, feel free to contact our grant director, Jose Ortiz:

Jose Ortiz
Director XCEL-IT
Palm Beach State College
Office: 561.868.3822 | Email: ortizj@palmbeachstate.edu
www.PalmBeachState.edu/Cybersecurity