Jackson Warren

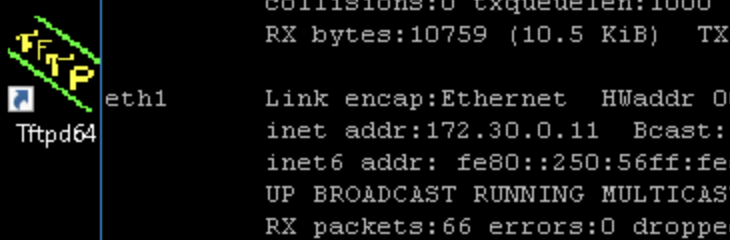
Jeremy Bergen

CSCI 370

12/13/21

Lab 15

Section 1:



Tcdump is a system-independent interface for network capture. If there are vulnerabilities in your web traffic, tcdump can pick this up and capture the data to be analyzed to show these vulnerabilities.

Skipfish is an active web application used for web reconnaissance. By mapping the targeted site using a dictionary through a recursive crawl, skipfish is able to return a number of active security checks, noting if any are disruptive.

The live HTTPS Headers file gathered info mostly on what was loaded on the site. The css file, the Javascript file, images and logos, php, and for each: their host IP, platoform being used, language, connection type, and much more for each.

HTTPS Headers add-on is very similar in use to the skipfish in my mind. It collects data about the site you are accessing and this data can be used to investigate any security breaches. If a malicous file is loaded onto your PC by this site, the add-on will collect the loading of this data from the website you accessed.

Part 3:

Many threats are posed to this one since it is a public retail outlet. False information can be entered or gathered and used without the actual user’s knowledge. Loss of security of cards and locations that is taken maliciously. Exploiting any of these could result in lawsuits, loss of customers, loss of business, legal issues in general, loss of product, and much more.

For the law firm, the scenario is very similar but the main threat is the information and not so much business and product. Obviously, business can be lost, but losing their personal info is very bad if this does occur and the website is exploited. Results would be similar to above.

Again, similar description of threats and results. Incorrect appraisals could lead to false info and lost money for clients, resulting in loss of business and lawsuits. Once again, leaking personal information is a threat. Threats if this does occur are similar once again.

For the hosted websites, these threats could be vast. If they are corrupted, all the users utilizing this service could have information and business threatened. If this is exploited, once again, similar results can occur.

Section 2:

For a lot of these sections, its similar threats and situations so I’m going to do a general summary for these:

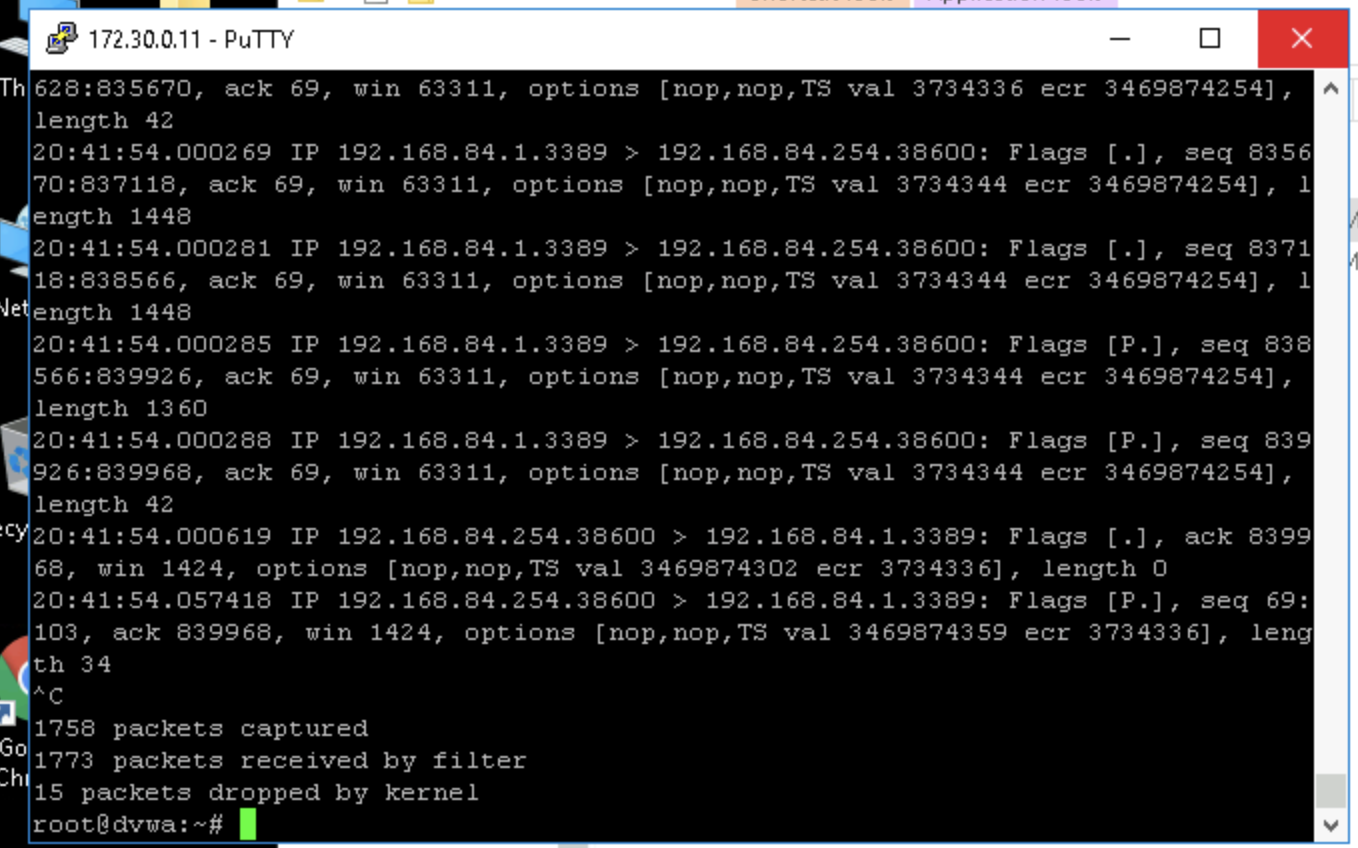
Description of Business Threats: For all these scenarios, these threats are vast. Loss of product, sales, customers, suppliers, services, licenses — the list goes on.

Effects of Compromised Applications: Once again, these scenarios are all very bad if these systems are compromised. Usernames and passwords can be collected, personal data, location, credit cards, social security numbers, identities as a whole, personal documents and classified information, money lost on both the business and the customer, etc.

Section 3:

Part 1: Reviewing HTTP headers is important for multiple reasons. One, to make sure the websites HTTP headers are all correct and cohesive in the desired way. Two, headers give up a lot of information. Making sure this information is secure in general and can’t be used to comprise the system or leak information is important.

Part 2:



Part 3:

A lot of the information I am seeing here is pretty similar from both platforms. A lot of information of the data being collected from the website as mentioned previously is coming in and being logged by both services. If there is notable differences between the data being collected, I did not spot it.

Sources:

<https://www.sciencedirect.com/topics/computer-science/tcpdump>

<https://www.kali.org/tools/skipfish/#:~:text=Skipfish%20is%20an%20active%20web,non%2Ddisruptive)%20security%20checks>.