Chapter 15
Toward More Resilient Cyber Infrastructure:
A Practical Approach

Biljana Tanceska
Ministry of Defense, Macedonia

Mitko Bogdanoski
Military Academy "General Mihailo Apostolski", Macedonia

Aleksandar Risteski
University Ss. Cyril and Methodius, Macedonia

ABSTRACT

In this chapter, an analysis of security attacks on network elements along with the appropriate countermeasures is presented. The main goal of this chapter is to present the practical execution of various security attacks and their mitigation techniques due to more resilient cyber infrastructure. The network topology that has been attacked is designed in GNS3 software tool installed on Windows operating system, while the attacks are performed in Kali Linux operating system. Three groups of security attacks (Denial of Service, Man in the Middle, and Control Plane attacks) are observed in simulation scenarios with a detailed analysis on each of them, followed by a presentation of practical performance and ways of prevention (protection) against the attacks.

INTRODUCTION

In less than a generation, the electronic neighborhood called the Internet has established itself as the connection mechanisms bringing individuals, governments, corporations, colleges/universities, and other entities into a truly global system. This mechanism has affected political, economic, social, and educational interactions in a way that has produced significant benefits. However, when it comes to knowing how to cost - effectively protect the cyber infrastructure and the information that flows through it, we are all in uncharted territory (Kreitner, 2009). Malicious users are constantly looking for weaknesses and ways to disrupt the normal functioning of a given network, thereby

DOI: 10.4018/978-1-4666-8793-6.ch015

causing damage by stealing or modifying the information or by making a service unavailable to its legitimate users. This is why internet security is an essential feature for managers and administrators of all networks. After experiencing considerable financial and technological damage in recent years and after knowing that even extremely powerful companies such as Google, Microsoft, Facebook, Yahoo, has suffered of various complex security violations, the main question of every company is: How can we protect ourselves from a security violation?

The main aim of this chapter is to give some realistic and effective answers to these questions so we can effectively protect the network topology and its network elements from a security violation by analyzing some of the attacks that individuals or corporations are dealing with on a daily basis, or in resume to find an effective way toward more resilient cyber infrastructure. The purpose of this chapter is concluded (completed) using a theoretical and practical analysis of some of the before mentioned security attacks, followed by their appropriate countermeasures. To better understand the consequences and likelihood of such security disruptions, we put ourselves in the attacker's role. In this way the awareness of the vulnerabilities of the network infrastructure increases. And if the vulnerabilities are well-know, the effective way of mitigation is very easy to find and implement.

Before performing a theoretical and practical analysis of the security attacks, in the first section the purpose of implementing various internet security mechanisms and internet security policing will be explained. Then the term security attack will be defined presenting the division of the entire set of attacks on three groups that perfectly suit the chapter's goal. Knowing that the main goal of every malicious user (attacker) is to either perform a denial of service to the victim, or to steal information from the legitimate users, the entire set of security attacks in this chapter will be divided as follows:

1. Denial-of-service attack.
2. Man-in-the-middle attack.
3. Control plane attack.

From the first group of security attacks given above, a theoretical and practical analysis of a *DHCP (Dynamic Host Configuration Protocol) Starvation attack* will be presented. *ARP (Address Resolution Protocol) Poisoning* and DHCP Starvation with Rogue server are the security attacks that are chosen to be analyzed from the second group of security attacks - Man-in-the-middle attack. And finally, from the third group of security attack - Control plane attacks, the *CDP (Cisco Discovery Protocol) Flooding attack* will be theoretically and practically analyzed. The first section will be concluded with a detailed theoretical analysis of the previously mentioned three groups of security attacks, and ways to prevent from their malicious influence.

In order to provide more realistic analysis of the security attacks GNS3 - based network topology will be implemented. The GNS3 simulation tool is chosen because is an open source software that simulate complex networks while being as close as possible to the way the real networks perform. All of this without having a dedicated network hardware such as routers and switches. In short GNS3 is an excellent alternative tool to real labs for network engineer administrators and people studying for certifications. This network topology along with its network elements and their configuration techniques will be presented in the second section of the chapter.

In the third section, a detailed theoretical analysis of the following security attacks will be presented:

1. Theoretical analysis of DHCP Starvation with Rogue server attack.
2. Theoretical analysis of ARP Poisoning attack.
3. Theoretical analysis of CDP Flooding attack.