

12-2020

## Security Evaluation of Microsoft's Windows Under Cyber-Flood Attacks

Christina Y. Navarro  
*The University of Texas Rio Grande Valley*

Follow this and additional works at: <https://scholarworks.utrgv.edu/etd>



Part of the [Electrical and Computer Engineering Commons](#)

---

### Recommended Citation

Navarro, Christina Y., "Security Evaluation of Microsoft's Windows Under Cyber-Flood Attacks" (2020).  
*Theses and Dissertations*. 557.  
<https://scholarworks.utrgv.edu/etd/557>

This Thesis is brought to you for free and open access by ScholarWorks @ UTRGV. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of ScholarWorks @ UTRGV. For more information, please contact [justin.white@utrgv.edu](mailto:justin.white@utrgv.edu), [william.flores01@utrgv.edu](mailto:william.flores01@utrgv.edu).

SECURITY EVALUATION OF MICROSOFT'S WINDOWS  
UNDER CYBER-FLOOD ATTACKS

A Thesis

by

CHRISTINA Y. NAVARRO

Submitted to the Graduate College of  
The University of Texas Rio Grande Valley  
In partial fulfillment of the requirements for the degree of  
MASTER OF SCIENCE IN ENGINEERING

December 2020

Major Subject: Electrical Engineering



SECURITY EVALUATION OF MICROSOFT'S WINDOWS  
UNDER CYBER-FLOOD ATTACKS

A Thesis  
by  
CHRISTINA Y. NAVARRO

COMMITTEE MEMBERS

Dr. Sanjeev Kumar  
Chair of Committee

Dr. Wenjie Dong  
Committee Member

Dr. Yul Chu  
Committee Member

December 2020



Copyright 2020 Christina Navarro

All Rights Reserved



## ABSTRACT

Navarro, Christina Y., Security Evaluation of Microsoft's Windows Under Cyber-Flood Attacks.

Master of Science (MS), December 2020, 75 pp., 1 table, 64 figures, references, 69 titles.

Cyberattacks are quite common occurrences today as such can compromise entire networks producing collective vulnerabilities. As shown herein, manifold experimental findings exhibit ramifications for a cyberattack victim during multiple simulations. All experiments were conducted with Apple's iMac, the victim system, and different editions of Microsoft Windows 10 and Windows 8.1.

Cyberattacks herein categorize as Distributed Denial of Service (DDoS) attacks including Smurf, Ping Flood, Transmission Control Protocol-Synchronize (TCP-SYN) Flood, and User Datagram Protocol (UDP) Flood attacks. Experimental results from each cyberattack are recordings of computer activities such as memory consumption, disk utilization, and overall processor utilization.

DDoS attack simulations include networks with over 65 thousand systems per network which generate attack traffic for the victim system. Likewise, simulated legitimate traffic attempts to connect with a victim system for further evaluation purposes. Experimental data analysis involves comparing impactful differences between cyberattacks, Microsoft Windows versions, and editions of both versions.





## DEDICATION

I owe a great debt of gratitude to my loving family for providing me with endless amounts of support and opportunity to complete a graduate master's program. My mother Lucy Navarro, my father, Rene Navarro, motivated me constantly, in every positive aspect, to achieve this goal. I am deeply appreciative for their encouragement and succor during this endeavor.



## ACKNOWLEDGMENTS

Special thanks to Dr. Kumar, Chair of Committee, for his advisement and belief in my studies which aided in accomplishing this thesis. Dr. Kumar consistently made himself available for mentoring which was a relieving non-issue. Furthermore, Dr. Kumar is a great advisor because he consistently helped me feel encouraged by providing constructive criticism with positive affirmations which is admirable. Furthermore, I thank committee members Dr. Yul Chu and Dr. Wenjie Dong for all of their contributions. The aforementioned committee members provided a great deal of advice and guidance for the betterment of this thesis.

I am greatly appreciative of my colleagues from the Network Research Lab (NRL) at the University of Texas – Rio Grande Valley (UTRGV) for helping me gain familiarity with the NRL and its innerworkings. Some colleagues became people whom I can call friends for a lifetime.

This research work was supported in part by the U.S. National Science Foundation (NSF) under Grant No. 0421585, and Lloyd M. Bentsen, Jr. Endowed Chair in Engineering Fellowship awarded to Dr. Kumar. Genuine and immense thanks to the NSF and Bentsen Jr. Endowed Fellowship for providing this funding resource thereby allowing research shown herein.



## TABLE OF CONTENTS

	Page
ABSTRACT .....	iii
DEDICATION .....	iv
ACKNOWLEDGMENTS .....	v
TABLE OF CONTENTS .....	vi
LIST OF TABLES .....	ix
LIST OF FIGURES .....	x
CHAPTER I. INTRODUCTION .....	1
1.1 Problem Statement.....	6
1.2 Proposal .....	7
1.3 Thesis Outline .....	8
CHAPTER II. BACKGROUND OF DISTRIBUTED DENIAL OF SERVICE ATTACKS	10
2.1 Ping-Based DDoS Attacks .....	10
2.1.1 Ping Flood Attack .....	11
2.1.2 Smurf Attack .....	11
2.2 Transport-Layer-Based DDoS Attacks .....	13
2.2.1 TCP-SYN Flood Attack .....	14
2.2.2 UDP Flood Attack .....	15
2.3 Chapter II Summary .....	16

CHAPTER III. EXPERIMENTAL SETUP .....	17
3.1 Performance Parameters .....	19
3.2 Chapter III Summary .....	20
CHAPTER IV. COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 ENTERPRISE VERSIONS .....	21
4.1 Microsoft Windows Enterprise Versions' under Ping Flood Attack .....	21
4.2 Microsoft Windows Enterprise Versions' under Smurf Attack .....	26
4.3 Microsoft Windows Enterprise Versions' under TCP-SYN Flood Attack .....	31
4.4 Microsoft Windows Enterprise Versions' under UDP Flood Attack .....	34
4.5 Chapter IV Summary .....	37
CHAPTER V. COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 PROFESSIONAL VERSIONS .....	38
5.1 Microsoft Windows Professional Versions' under Ping Flood Attack .....	38
5.2 Microsoft Windows Professional Versions' under Smurf Attack .....	41
5.3 Microsoft Windows Professional Versions' under TCP-SYN Flood Attack ....	44
5.4 Microsoft Windows Professional Versions' under UDP Flood Attack .....	46
5.5 Chapter V Summary .....	48
CHAPTER VI. COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 CORE VERSIONS .....	49
6.1 Microsoft Windows Core Versions' under Ping Flood Attack .....	49
6.2 Microsoft Windows Core Versions' under Smurf Attack .....	52
6.3 Microsoft Windows Core Versions' under TCP-SYN Flood Attack .....	55
6.4 Microsoft Windows Core Versions' under UDP Flood Attack .....	58
6.5 Chapter VI Summary .....	61
CHAPTER VII. FURTHER COMPARISON .....	62

CHAPTER VIII. CONCLUSION .....	66
REFERENCES .....	69
BIOGRAPHICAL SKETCH .....	75





## LIST OF TABLES

	Page
Table 1: Average of HTTP Transactions Per Second within 300 to 500 Mbps Of Attack Traffic .....	57



## LIST OF FIGURES

	Page
Figure 1.1: Layers of OSI Model .....	2
Figure 1.2: CIA Triad .....	3
Figure 1.3: Traditional Botnet Configuration .....	4
Figure 2.1: Simplified Echo Message Format .....	11
Figure 2.2: Smurf Attack Configuration .....	12
Figure 2.3: Simplified TCP Header .....	13
Figure 2.4: Three-Way Handshake Visual Representation.....	14
Figure 2.5: Simplified UDP Header.....	14
Figure 3.1: Experimental Setup .....	18
Figure 4.1: Microsoft Windows Enterprise Versions' Overall Processor Utilization under Ping Flood Attack.....	23
Figure 4.2: Microsoft Windows Enterprise Versions' Memory Consumption under Ping Flood Attack.....	23
Figure 4.3: Microsoft Windows Enterprise Versions' Disk Utilization under Ping Flood Attack .....	24
Figure 4.4: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under Ping Flood Attack.....	26
Figure 4.5: Microsoft Windows Enterprise Versions' Overall Processor Utilization under Smurf Attack .....	27
Figure 4.6: Microsoft Windows Enterprise Versions' under Memory Consumption under Smurf Attack .....	28
Figure 4.7: Microsoft Windows Enterprise Versions' Disk Utilization under Smurf Attack .....	29

Figure 4.8: Microsoft Windows Enterprise Versions' HTTP transaction rates under Smurf Attack .....	30
Figure 4.9: Microsoft Windows Enterprise Versions' Overall Processor Utilization under TCP-SYN Flood Attack .....	31
Figure 4.10: Microsoft Windows Enterprise Versions' Memory Consumption under TCP-SYN Flood Attack .....	32
Figure 4.11: Microsoft Windows Enterprise Versions' Disk Utilization under TCP-SYN Flood Attack .....	33
Figure 4.12: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under TCP-SYN Flood Attack .....	34
Figure 4.13: Microsoft Windows Enterprise Versions' Overall Processor Utilization under UDP Flood Attack .....	35
Figure 4.14: Microsoft Windows Enterprise Versions' Memory Consumption under UDP Flood Attack .....	35
Figure 4.15: Microsoft Windows Enterprise Versions' Disk Utilization under UDP Flood Attack .....	36
Figure 4.16: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under UDP Flood Attack .....	37
Figure 5.1: Microsoft Windows Professional Versions' Overall Processor Utilization under Ping Flood Attack.....	39
Figure 5.2: Microsoft Windows Professional Versions' Memory Consumption under Ping Flood Attack.....	39
Figure 5.3: Microsoft Windows Professional Versions' Disk Utilization under Ping Flood Attack .....	40
Figure 5.4: Microsoft Windows Professional Versions' HTTP Transaction Rates under Ping Flood Attack.....	41
Figure 5.5: Microsoft Windows Professional Versions' Overall Processor Utilization under Smurf Attack .....	42
Figure 5.6: Microsoft Windows Professional Versions' Memory Consumption under Smurf Attack .....	42
Figure 5.7: Microsoft Windows Professional Versions' Disk Utilization under Smurf Attack .....	43

Figure 5.8: Microsoft Windows Professional Versions' HTTP Transaction Rates under Smurf Attack .....	43
Figure 5.9: Microsoft Windows Professional Versions' Overall Processor Utilization under TCP-SYN Flood Attack .....	44
Figure 5.10: Microsoft Windows Professional Versions' Memory Consumption under TCP-SYN Flood Attack .....	44
Figure 5.11: Microsoft Windows Professional Versions' Disk Utilization under TCP-SYN Flood Attack .....	45
Figure 5.12: Microsoft Windows Professional Versions' HTTP Transaction Rates under TCP-SYN Flood Attack .....	46
Figure 5.13: Microsoft Windows Professional Versions' Overall Processor Utilization under UDP Flood Attack .....	46
Figure 5.14: Microsoft Windows Professional Versions' Memory Consumption under UDP Flood Attack .....	47
Figure 5.15: Microsoft Windows Professional Versions' Disk Utilization under UDP Flood Attack .....	47
Figure 5.16: Microsoft Windows Professional Versions' HTTP Transaction Rates under UDP Flood Attack .....	48
Figure 6.1: Microsoft Windows Core Versions' Overall Processor Utilization under Ping Flood Attack .....	50
Figure 6.2: Microsoft Windows Core Versions' Memory Consumption under Ping Flood Attack .....	50
Figure 6.3: Microsoft Windows Core Versions' Disk Utilization under Ping Flood Attack .....	51
Figure 6.4: Microsoft Windows Core Versions' HTTP Transaction Rates under Ping Flood Attack .....	51
Figure 6.5: Microsoft Windows Core Versions' Overall Processor Utilization under Smurf Attack .....	52
Figure 6.6: Microsoft Windows Core Versions' Memory Consumption under Smurf Attack .....	53
Figure 6.7: Microsoft Windows Core Versions' Disk Utilization under Smurf Attack .....	53
Figure 6.8: Microsoft Windows Core Versions' HTTP Transaction Rates under Smurf Attack .....	54

Figure 6.9: Microsoft Windows Core Versions' Overall Processor Utilization under TCP-SYN Flood Attack .....	55
Figure 6.10: Microsoft Windows Core Versions' Memory Consumption under TCP-SYN Flood Attack .....	56
Figure 6.11: Microsoft Windows Core Versions' Disk Utilization under TCP-SYN Flood Attack .....	56
Figure 6.12: Microsoft Windows Core Versions' HTTP Transaction Rates under TCP-SYN Flood Attack .....	58
Figure 6.13: Microsoft Windows Core Versions' Overall Processor Utilization under UDP Flood Attack .....	58
Figure 6.14: Microsoft Windows Core Versions' Memory Consumption under UDP Flood Attack .....	59
Figure 6.15: Microsoft Windows Core Versions' Disk Utilization under UDP Flood Attack .....	60
Figure 6.16: Microsoft Windows Core Versions' HTTP Transaction Rates under UDP Flood Attack .....	61
Figure 7.1: Microsoft Windows Versions' Disk Utilization under Smurf Attack .....	62
Figure 7.2: Microsoft Windows Versions' HTTP Transaction Rates under TCP-SYN Flood Attack .....	63
Figure 7.3: Microsoft Windows 8.1 Core Version Disk Utilization under Various DDoS Attacks .....	63
Figure 7.4: Microsoft Windows 8.1 Core Version HTTP Transaction Rates under Various DDoS Attacks .....	64
Figure 7.5: Microsoft Windows 10 Enterprise Version Overall Processor Utilization under Various DDoS Attacks .....	65
Figure 7.6: Microsoft Windows 10 Enterprise Version Memory Consumption under Various DDoS Attacks .....	65
Figure 8.1: Microsoft Windows 8.1 Disk Utilization Near 100 Percent under Smurf Attack .....	66

## CHAPTER I

### INTRODUCTION

During the early 2000s, electronics with Internet capabilities gradually became a basic necessity for most industries in advanced societies. Inevitably, these devices or machines sustained various cyberattacks such as, Distributed Denial of Service (DDoS). DDoS attacks are roughly defined as the following: multiple preconfigured Denial of Service (DoS) agents which deliver immense amounts of attack traffic to a victim system [1]. As further described in Chapter II, an attacker or bot-master predetermines types of attack traffic to transmit. Amidst a DDoS attack, inundation consumes systems of available resources unpredictably dependent upon cyberattack magnitude. As a result of DDoS attacks, numerous repercussions surface such as, losing legitimate Hypertext Transfer Protocol (HTTP) client connections [2]. For example, a business unwillingly ceases services for HTTP transactions while under attack due to oversaturation within their network. Consequently, negative and costly effects compromise a business' overall integrity after a detrimental attack [3]. Moreover, when systems or networks pause business operations possible outcomes can include loss of key clientele.

For clarity, the following paragraphs briefly describe foundational background information regarding network communication basics such as, the Open Standards Interface (OSI) reference model. This rudimentary model illustrates the overall procedure and process for information and data transfer between devices. The OSI model consists of seven different sections, or more commonly referred to as protocol layers, which individually depict data communication



principles as shown in Figure 1.1 [4]. Each layer of the OSI model represents a different stage in the overall process of data transmission between devices [5]. Additionally, all seven protocol layers mirror themselves representing both transmitter and receiver sides of communication. Overall, the OSI model consistently serves as a visual aid for introductory data transmission methodology.

1. Physical	Transmission of an unstructured bit stream over the physical medium
2. Data Link	Reliable transmission of frames over a single network connection
3. Network	End-to-end communication across one or more subnetworks
4. Transport	Reliable and transparent transfer of data between end points
5. Session	Control structure and management of sessions between applications
6. Presentation	Data representation (encoding) during transfer
7. Application	Information processing and provision of services to end users

Figure 1.1: Layers of OSI Model [5]

Both information and data transition across each layer of the OSI model via protocol data units (PDUs) as variable-length packets in two main parts: header and data [6]. Headers contain key routing and delivery instructions for subsequent protocol layers of the OSI model [6]. Based on individual protocols, PDU formats mainly differ by header requirements, such as, a source and destination Internet Protocol (IP) address of a Layer-3 PDU [6]. The data section of a PDU mainly contains content such as an image or document. Examples of PDUs are an IP datagram (Layer-3), TCP segment (Layer-4), and Institute of Electronics and Electrical Engineers (IEEE) 802.3 standard Medium Access Control (MAC) frame (Layer-2) [6].

PDUs transition through the OSI model by implementing control information via headers for data communication [6]. Essentially, each transmitter protocol layer adds headers to packets until it reaches a predetermined receiver [6]. Then, a receiver's protocol layers proceed by removing headers until originally sent data is received at the destination process [6]. Likewise, a protocol interface may incorporate additional PDUs while using a similar concept to support further

actions required by the OSI model [6]. However, every PDU of a protocol interface is not required in the OSI model [6]. Examples of PDUs within protocol interfaces are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) messages.

Amid DDoS attack, victim devices uncontrollably lose availability which negatively and directly affects the renown CIA (confidentiality, integrity, and availability) triad. The CIA triad is another visual representation in network communications displaying key principles for data and information security [7]. Roughly, the CIA triad defines its three main concepts as the following: [8]

1. Availability: An attacker compromises computer resource availability or denial of use
2. Integrity: An attacker modifies computer information or data
3. Confidentiality: An attacker obtains computer information or data

If effective, DDoS attacks of medium to large magnitudes can compromise devices such as, processor, memory, and bandwidth exhaustion [9][10][11][12]. For instance, Dr. Kumar and associates simulate a series of DDoS attacks where they determine the following: overutilization of system memory and its processors directly correlates with receiving vast amounts of data [10][11][12]. Entities inherently respond quickly during an apparent cyberattack of any size due to violations of security principles such as those depicted in the CIA triad, as shown in Figure 1.2.

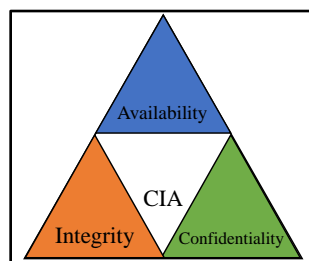


Figure 1.2: CIA Triad

Inevitably, electronics with Internet capabilities fully expose their vulnerabilities when hackers intervene with various cyberattack techniques such as, malicious botnets [13]. A botnet is as an interconnected group of compromised devices or bots that commonly perpetrate DDoS attacks [14]. Within a botnet, individual bots are programmed with malicious software by a master, or bot-master, for command and control (C&C) and potential victim exploitation [15]. For example, as described by Herrera, multiple botnets of varying magnitudes greatly diminish a victim system's resources by receiving overwhelming amounts of traffic [16]. In Herrera's case, a botnet exhausts a victim's resources via DDoS attack. Following a successful botnet attack, a victim system becomes unavailable to legitimate users and virtually inoperable.

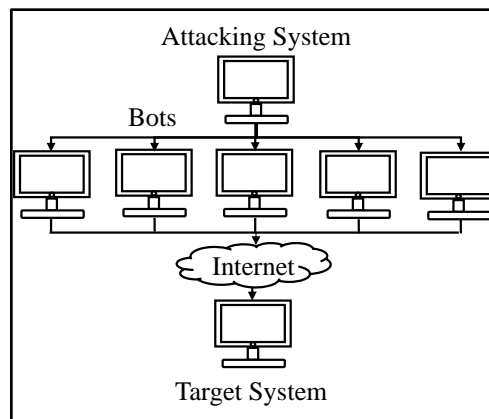


Figure 1.3: Traditional Botnet Configuration

Botnets are typically categorized by one main characteristic which is size [17]. Arbitrarily selected by bot-masters, botnet magnitudes are roughly measured by sheer intensity. For example, Gunnam states each bot or host within a single botnet is assigned an Internet Protocol version 4 (IPv4) address via an addressing scheme known as classful addressing [18][19]. Thus, an attacker may manipulate the classful addressing scheme within multiple networks each containing several hosts to curate a botnet for potential cyberattack [15][18]. Additionally, each

botnet size directly corresponds to a class from the classful addressing scheme as further described in the following paragraph. In short, botnet sizes are determined by two main parameters: number of networks and bots per network.

IPv4 is an original method for IP addresses however it is insufficient and thus incapable of supporting massive networks due to expansion limitations [20]. However, IPv4 remains prevalent amongst users today due to attributes like security and robustness. Generally, IPv4 addresses categorize within two different schemes: classful IP addressing and classless IP addressing [21]. A convenient advantage for classful IP addressing is unique identification of available host and network space [22]. The classful addressing scheme has three principal attributes: subnet mask, network, and host space [23]. However, these properties define a fixed range for both network and host space within each class of classful IP addressing thus limiting potential for expansion, as mentioned earlier [24]. In comparison, the superior IP addressing scheme is classless because of wider IP address availability without network or host space restrictions as in classful addressing [25]. Nonetheless, some hackers meticulously use classful addressing to target victims with fewer IP addresses for intensification purposes [20][21]. In total, the classful IP addressing scheme includes five different classes: Classes A-E [26]. Class A addresses serve 16,777,214 hosts per network while Class C addresses support a maximum of 254 hosts. A Class B address was incorporated throughout each experiment herein which holds 65,534 hosts per network [21]. Classes D and E are reserved for multicasting and research and development purposes, respectively [26].

## 1.1 Problem Statement

As mentioned previously, electronics with Internet capabilities are prone to cyberattack as evolution has driven society into technology-dependent entities. More cyberattacks occur each year worldwide however, the United States of America ranks highest in targets [27] [28]. In 2020, a significant increase in cyberattacks are shown due to a worldwide pandemic [27] [29].

For example, in May 2020, researchers discovered a platform which launches DDoS attacks such as, TCP-SYN and UDP Flood attacks [30][31]. Researchers could trace these attacks after several reported incidents [30][31]. Furthermore, the DDoS-launching platform known as Lucifer was mainly targeting Microsoft Windows hosts [31][32]. Microsoft has since released updates and patches for Lucifer [31][32]. According to several sources, the most common cyber-flood attacks are TCP-SYN Flood and UDP Flood attacks [33][34][35][36].

As customers transition to cloud services, cyber-flood attacks increase in attempt to maliciously disrupt users [36]. According to Microsoft Windows, researchers found DDoS attacks occurring more regularly and frequently during the pandemic [36]. Furthermore, threat researchers mitigated approximately 800 attacks per day in March 2020 which is a fifty percent increase in comparison with pre-pandemic records [36]. Between January and June of 2020, Microsoft recorded TCP-SYN and UDP Flood attacks as the most common DDoS attack observed by their platforms [36].

Herein realistic and conventional cyberattacks provide awareness for tangible possibilities in society. Network security systems have improved significantly over time which increases difficulty levels for potential hacks. However, hackers still manage to intervene at times which seems like a separate yet, simultaneously ongoing pandemic considering coronavirus.

## 1.2 Proposal

Herein multiple DDoS attacks are executed to provide indications of harmful cyber-flood attacks. DDoS attacks under test include TCP-SYN, UDP Flood, Ping Flood, and Smurf attack for comparison purposes. As a test environment, an Apple platform with several versions of Microsoft Windows serves as a victim system for multiple cases. Microsoft Windows editions under evaluation include Enterprise, Core, and Professional as further described in Chapter III. As an objective, experimental data herein presents recordings of computer activities and behaviors to determine which Microsoft Windows version is superior. Furthermore, evaluations of DDoS attack effects are described for further comparison. As a hypothesis, I theorize Windows 10 outperforms Windows 8.1 in all recordings for each edition under test. Microsoft Windows 8.1 was developed based upon Windows 10 which includes overall better features such as, security enhancements as further described in Chapter III. Similarly, Microsoft Windows versions are based upon one another with Core serving as the base version [37].

In 2006, a Microsoft Windows simulation shows processor-intensive Ping Flood attacks in comparison with overall processor utilization [11]. Therefore, a prediction for this experiment is Ping Flood attacks will cause complete exhaustion of overall processor utilization for Windows 8.1 versions. In a similar case, a Microsoft Windows platform under Ping Flood attack crashes due to memory depletion in 2010 [38]. As a hypothesis, Microsoft Windows 8.1 versions under Ping Flood attacks will exhaust all available memory. In 2017, a Smurf attack completely exhausted HTTP transaction rates via Microsoft Windows Server while comparing Ping Flood, TCP-SYN, and UDP Flood attacks [18]. Thus, as another prediction, HTTP transaction rates will

cease due to Smurf attack for Microsoft Windows 8.1 versions. Recent research for disk utilization recordings while under DDoS attacks were not found after several failed attempts.

After extensive research, DDoS attacks mentioned herein which include Microsoft Windows 10 and 8.1 versions were not found however, few vaguely similar attacks are described below. For example, in 2018, researchers executed TCP-SYN Flood attacks on servers including Microsoft Windows 2016 Server [39]. Researchers recorded outgoing data rates for each server where Microsoft's Windows Server outperformed an Apache2 server [39]. Another case in 2017, compares Microsoft's Windows Server Lion and 2012 R2 which shows Lion with an overall lower performance especially during TCP-SYN Flood attack [10]. Furthermore, this experiment depicts relatively slow upstream data rates for the victim system. Similarly, in 2018, Microsoft Windows Server 2012 R2 shows TCP-SYN Flood attack as a more harmful attack than UDP Flood attack with respect to processor utilization and outgoing data rates [16].

### **1.3 Thesis Outline**

This manuscript provides a security evaluation of an Apple platform with various Microsoft Windows operating systems. Although, before an evaluation takes place, an introduction to network security and cyberattack concepts are given for background purposes. Then, a problem statement and proposal are presented in Chapter I to support this document with intent and purpose. In Chapter II, DDoS attacks under evaluation are described in detail to present further background information for subsequent chapters. Chapter III describes victim performance parameters under evaluation and an experimental setup. Chapters IV through VII extensively transcribe and illustrate experimental results from several iterations of various DDoS attacks

performed on the device under test (DUT) with different versions and editions of Microsoft Windows. Lastly, the final chapter includes an overall comparison and conclusion for all experiments herein as explicitly explained in previous chapters. The purpose of this outline is to briefly elaborate on the Table of Contents shown on page iv.



## CHAPTER II

### BACKGROUND FOR DISTRIBUTED DENIAL OF SERVICE ATTACKS

Cyberattack effects circumstantially vary based on arbitrary techniques which include cyberattack types and unique platforms. As previously mentioned in Chapter I, outcomes of a DDoS attack potentially compromise the availability component of the CIA triad [40][41][42][43]. Several studies support that DDoS attacks expose network security vulnerabilities with resource exhaustion as an apparent result [44][45][46]. Particular DDoS attacks in frequent practice include TCP-SYN and Ping Flood attacks [39][47][48]. These two DDoS attacks and a couple alike are described in further detail throughout this chapter.

#### **2.1 Ping-Based DDoS Attacks**

Types of DDoS attacks categorize based upon specific types of data undesirably received in large amounts via the OSI model. Ping-based DDoS attacks directly originate from Layer-3 of the OSI model because, Ping messages generate via ICMP [1][49]. The Network Layer (Layer-3) primarily forwards, or routes, packets across multiple networks based on Internet Protocol [50]. If necessary, ICMP supports Layer-3 with important network troubleshooting and management information as procedural aid for protocol transition [51]. An IP datagram generates a reserved protocol value to indicate when ICMP is necessary [6][51]. Common ICMP messages are echo-request and echo-reply which exchange between hosts to check reachability and other parameters

via a common command known as Ping [49][51]. The Ping command is a native component within systems to test reachability of a host [11]. Additionally, an echo-reply is mandatory for each request received, as claimed by RFC 792 [51]. As PDUs, echo-request and echo-reply messages also include a header and data section which is shown in Figure 2.1 [6]. As a query, echo-request and echo-reply message headers hold important information for identification while a data section presents optional data [6][11]. Figure 2.1 shows a rudimentary frame format of ICMP echo-request and echo-reply messages.

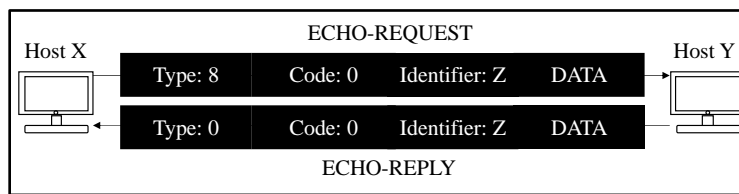


Figure 2.1: Simplified Echo Message Format

### 2.1.1 Ping Flood Attack

ICMP messages are vastly exploited by hackers and pose cyberattacks on a host or multiple hosts [3]. For instance, in a Ping Flood attack, a victim receives excessive amounts of echo-request packets which saturates their capacity [11]. Typically, multiple spoofed echo-requests are sent to victims via a botnet which defines the severity of each DDoS attack, as described in subsequent sections [12]. As mentioned before, each request requires a response which further exhausts a victim system's resources hindering proper operation [49].

### 2.1.2 Smurf Attack

Smurf attacks also exploits ICMP messages however, Smurf is more overall complex [1]. Ping Flood attacks solely incorporate echo-request messages while Smurf attacks utilize both

echo messages [16]. However, Smurf attacks largely incorporate echo-reply messages to execute a more intensive and sophisticated DDoS attack [18]. Initially, attackers send several echo-request messages to an unprotected broadcast domain for Smurf Attacks [43]. Then, attackers incorporate a spoofed source IP address to match the victim's IP address [44]. As a result of Smurf attack, a victim receives several unsolicited echo-reply messages thus crippling their system [18][43]. Generally, a broadcast domain spreads a packet widely to interconnected devices as a method for mass communication [1][16]. Therefore, all hosts connected to a broadcast domain must respond to all echo-request messages with a corresponding echo-reply [1][44]. In a Smurf attack, broadcast domains amplify to magnitudes that are based on calculations and several factors such as, echo-request message size, number of broadcast domains, and number of hosts in each broadcast domain [1]. Simplified, the amplified attack rate (AAR) is shown below as an equation in bits per second (bps) where bandwidth is a data rate selected by attackers [1].

$$\text{AAR} = \text{Number of Broadcast Domains} * \text{Number of Hosts in each Broadcast Domain} * \text{Bandwidth (bps)}$$

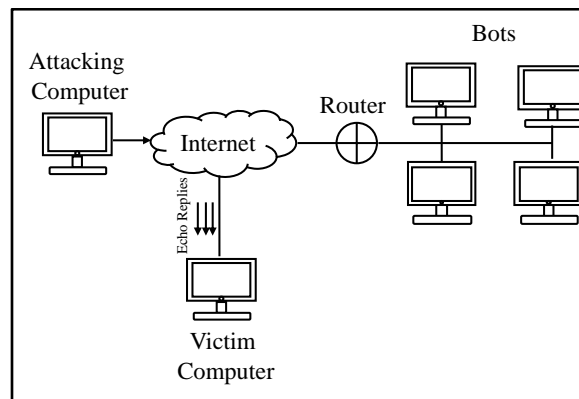


Figure 2.2: Smurf Attack Configuration

## 2.2 Transport-Layer-Based DDoS Attacks

TCP-SYN and UDP Flood DDoS attacks share one main similarity which is both attacks originate from Layer-4 (Transport Layer) of the OSI model [6][18]. Layer-4 entails data transfer logistics for communication networks where hackers may maliciously intervene [10][16][52][53]. For example, TCP ensures users of data delivery based on a concept known as the three-way handshake [52]. Essentially, three-way handshakes establish a reliable connection for hosts before data transmission [52]. Likewise, data transfer utilizes a similar three-way handshake for further reliability [6][52]. Three-way handshakes create connections between two hosts via a TCP control segment [6]. Within a TCP segment, a header includes important numbering and sequencing data for data transfer such as, information for three-way handshakes as shown in Figure 2.3 [6]. Furthermore, TCP headers incorporate single-bit flags to indicate specific directions such as, resetting or closing a connection. Likewise, a series of flags conduct three-way handshakes principally as shown below [6]:

1. Control segment sent from Host X to Host Y with SYN flag set [SYN segment]
2. Control segment sent from Host Y to Host X with SYN and Acknowledgment (ACK) flags set [SYN-ACK segment]
3. Control segment sent to Host X from Host Y with ACK flag set [ACK segment]

Note: SYN Segments usually indicate a request for connection.

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Header Length	Reserved	Flags	Window Size

Figure 2.3: Simplified TCP Header

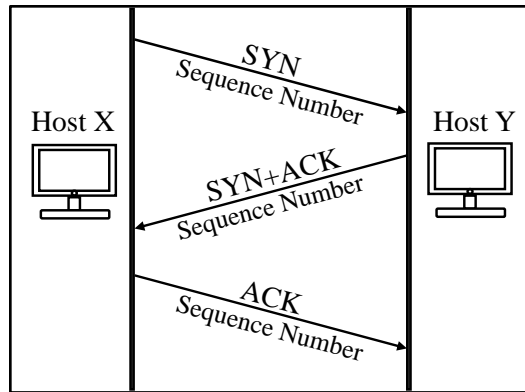


Figure 2.4: Three-Way Handshake Visual Representation

As mentioned earlier in this section, both UDP and TCP categorize under Layer-4 (Transport Layer) of the OSI model. However, UDP unreliably delivers data without prior connection as required in TCP (three-way handshake) [6]. As a transaction-oriented protocol, UDP states a packet of data is sent to a receiver without guarantee of delivery as mentioned in RFC 768 [6][53]. UDP datagrams also include a header and data section as shown in Figure 2.5 [6]. Essentially, UDP requires connectionless and immediate data delivery without any regard for reliability [6][18].

Source Port	Destination Port
Segment Length	Checksum

Figure 2.5: Simplified UDP Header

### 2.2.1 TCP-SYN Flood Attack

The foundation of a TCP-SYN DDoS attack is the three-way handshake [10]. In accordance with RFC 793, a sender requests connectivity via SYN segments as mentioned in Section 2.2 [52]. Then, receivers respond with a corresponding SYN-ACK segment for acknowledgment and approval purposes [6]. Finally, receivers prompt senders for a final ACK segment to establish a

connection [6]. In a TCP-SYN attack, attackers use a spoofed IP address to create a system vulnerability known as a half-open connection [16]. Half-open connections are only parts one and two of the three-way handshake since the final ACK segment cannot respond to an unsolicited SYN-ACK segment [38][52]. Therefore, victim systems under a TCP-SYN flood attack cannot close the connection by not receiving the final ACK segment as required by the three-way handshake [45]. At this point, attackers send overwhelming amounts of SYN segments to victim hosts during half-open connection timeout periods [47]. The result of a TCP-SYN flood attack usually causes system resource saturation due to several amounts of SYN segments [54].

### **2.2.2 UDP Flood Attack**

Attackers execute UDP Flood attacks to flood victim systems via ports [16]. Layer-4 PDUs transmit to predetermined ports for subsequent protocols [52][53]. However, TCP-SYN DDoS attacks do not incorporate port interaction because that occurs during a preliminary process described as the three-way handshake [16][18]. UDP Flood attacks occur with a four-step procedure which includes spoofing and a protocol interface PDU [18]. An UDP Flood attack typically deploys with the following sequence [16][55]:

1. An attacker sends numerous UDP packets to random ports within a victim system via botnet
2. The victim system determines which applications have requested data from the targeted port
3. Once the victim system determines no applications have requested data, an ICMP-based message known as “destination unreachable” is generated

4. ICMP messages are sent back to the victim with a spoofed IP address generated by the attacker (similar to Smurf Attack)

Clearly, UDP Flood attack takes blatant advantage of UDP due to its lack of requirements as shown in Figure 2.4 on the following page [16][18][55].

### **2.3 Chapter II Summary**

DDoS attacks in this experiment include Ping-based and Transport Layer-Based DDoS attacks. Ping-based DDoS attacks are Ping Flood attack and Smurf attack. Transport Layer-Based DDoS attacks are TCP-SYN Flood attacks and UDP Flood attacks. Background information included in this chapter serves as conceptual information for subsequent chapters.

## CHAPTER III

### EXPERIMENTAL SETUP

This experiment included an attack system setup in a controlled and closed network environment to simulate numerous DDoS attacks of Class B botnet size on a victim system. In this case, the victim system under attack was an Apple iMac (21.5-inch, Mid-2011) installed with several up-to-date versions of Microsoft Windows one at a time, as listed below.

1. Windows 10 Professional
2. Windows 10 Core
3. Windows 10 Enterprise
4. Windows 8.1 Professional
5. Windows 8.1 Core
6. Windows 8.1 Enterprise

Editions of Microsoft Windows 10 and 8.1 differ based on additional features [37][56]. For example, Microsoft Windows Professional and Enterprise were developed based upon Windows Core versions [37][56]. Additional features include enhanced security features such as, machine learning analytics for threat response purposes within Microsoft Windows 10 Enterprise [37][56]. Furthermore, Microsoft Windows 10 Professional incorporates native information protection for users [37]. Microsoft Windows 8.1 editions differ in features such as, a Windows 8.1 Enterprise exclusive feature which controls applications and files accessibility per user [57][58][59]. Microsoft Windows 8.1 Professional includes features not shown in Windows 8.1 Core such as, hard drive encryption [59]. Similarly, Microsoft Windows 8.1 editions differ from Windows 10 editions because the predecessor is developed based upon its successor



[60][61][62]. For instance, Microsoft Windows 10 editions include better security features than Windows 8.1 such as, support for biometric scanning [60]. Additionally, the victim system has the following specifications:

- Quad-Core 2.5 gigahertz (GHZ) Intel "Core i5" I5-2400S (Sandy Bridge) Processor
- Eight gigabytes (GB) [two four-GB components] of 1,333 megahertz DDR3 Random-Access Memory (RAM)
- Thirty-two nanometers Lithography (Processor Housing)
- 500 GB (7,200 revolutions per minute [RPM]) hard disk drive (HDD)
- 10/100/1,000BASE-T Gigabit Ethernet (RJ-45 Connector)

Figure 3.1 depicts the complete configuration with each system under experiment within aforementioned environment.

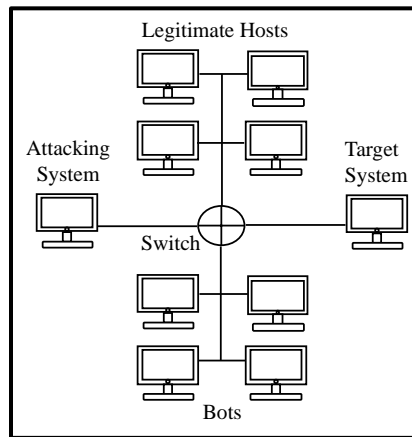


Figure 3.1: Experimental Setup

In each DDoS attack, two different types of network traffic were sent to the victim system simultaneously which are legitimate and attack traffic. In this case, legitimate traffic is roughly defined as simulated hosts performing multiple requests of a basic website for reachability. The victim system hosts a simple website originating from a built-in Microsoft Windows service.

Furthermore, these simulated hosts send 3,000 Hyper-Text Transfer Protocol (HTTP) transaction requests per second to the victim system to simulate legitimate traffic [63].

In this case, attack traffic was generated by a botnet of varying traffic amounts via Ethernet cable which has the followings specifications and characteristics:

- Berk-Tek Hyper Plus Category 5e
- Maximum Transmission Speed: One gigabit per second (Gbps)

The programmed botnet transmits attack traffic toward the victim system beginning with a line rate 100 megabits per second (Mbps), then increases by 100 Mbps until 1000 Mbps (1 Gbps) is reached. Essentially, attack traffic was delivered beginning with 100 Mbps then, increments of 100 Mbps, ending with the total link bandwidth. The purpose for this particular experiment is to further investigate impact endured by the victim system. Each experiment follows the subsequent procedure: only legitimate traffic is sent to the victim system which serves as a baseline for each test. Thereafter, legitimate and attack traffic are sent simultaneously while only attack traffic incrementally intensifies for an overall duration of approximately one hour.

### **3.1 Performance Parameters**

Each simulated DDoS attack performed, based on the experimental setup, is deployed to obtain the following information: Hyper-Text Transfer Protocol (HTTP) transaction rates, overall processor utilization (OPU), available Random-Access Memory (RAM), and disk utilization (DU). Analysis and evaluation of each data set considers the effects of each DDoS attack posed on the victim system. Each data set is obtained by a built-in Microsoft Windows application named Performance Monitor.

HTTP transaction rates transcribe amounts of successful requests per second [63]. Essentially, each HTTP transaction that successfully requested the website, which serves a purpose for legitimate traffic, is recorded for analysis and evaluation. Overall processor utilization data shows an average of each core's processor utilization as a percentage based on time per program [64][65]. In this case, the iMac under evaluation has four cores which represents the number of independent central processing units within Intel Corporation's chip [66]. Recorded memory consumption depicts overall RAM used by the victim system in megabytes. Disk utilization data describes the overall main hard disk utilization within the victim system [67]. A hard disk stores operating system, executable programs, and files [68].

### **3.2 Chapter III Summary**

This experiment involves several simulations of the four aforementioned DDoS attacks which are Ping Flood, Smurf, TCP-SYN Flood, and UDP Flood. Each aforementioned DDoS attack was simulated to cyberattack six different Microsoft Windows operating systems for evaluation purposes. Two different types of traffic were simultaneously sent toward the victim system which are legitimate and attack to simulate a real-world scenario. The application Performance Monitor from Microsoft recorded four different performance parameters for each simulation. In total, twenty-four simulations were conducted which are shown in several following chapters.

## CHAPTER IV

### COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 ENTERPRISE VERSIONS

The following chapters include data and results from each DDoS attack simulation. The sole purpose of these simulations is to compare between various versions of Microsoft Windows 10 and 8.1 based on gathered data. For example, in this chapter, a comparison between both Enterprise versions of Microsoft Windows 10 and 8.1 consider the aforementioned performance parameters. Security evaluations for each DDoS attack simulation are based on each comparison which is described within each of the following chapters. Each figure within this chapter includes a legend signifying both enterprise versions of Windows 10 and Windows 8.1 within each graph as follows: Win10Enterprise (Windows 10 Enterprise) and Win81Enterprise (Windows 8.1 Enterprise).

#### **4.1 Microsoft Windows Enterprise Versions' under Ping Flood Attack**

This attack causes significant disruption to the victim system since both echo-request and reply messages are expected. Figure 4.1 shows the overall processor utilization of the victim system while under Ping Flood attack for both Enterprise versions of Windows 10 and 8.1. Furthermore, Ping Flood attack poses an obvious fluctuation throughout the entire duration of this simulation for both operating systems. More specifically, Figure 4.1 shows a gradual

increase in processor utilization from zero (baseline) to 200 Mbps of attack traffic sent toward the victim system in Windows 10 Enterprise Again, only legitimate traffic is transmitted at the baseline thus, zero attack traffic is delivered at this point. Yet, Microsoft Windows 8.1 Enterprise hardly changes within the aforementioned range (zero to 200 Mbps) excluding zero Mbps. Then, dissimilar fluctuation patterns occur between both operating systems from 200 to 600 Mbps of attack traffic. For Windows 10 Enterprise in Ping Flood attack, overall processor utilization decreases after 200 Mbps of attack traffic then an incline pattern forms from 300 to 500 Mbps. Finally, another decrease in OPU values is shown after 500 Mbps which becomes a starting point for a steady-state pattern with a value of approximately thirty-five percent that continues for the remainder of this simulation.

As mentioned before, Windows 8.1 Enterprise also shows significant fluctuation in values during this simulation however, this pattern does not exactly compare to Windows 10 Enterprise. Windows 8.1 Enterprise under Ping Flood attack has a significant decline in OPU after 200 Mbps of attack traffic however, this decline in value continues until 400 Mbps. After 400 Mbps of attack traffic, a small incline occurs at 500 Mbps then, similar to Windows 10 Enterprise during Ping Flood attack, a steady-state pattern is shown with an approximate value of twenty-three percent until the end of simulation. Also, Windows 10 Enterprise OPU data is significantly greater in value compared to Windows 8.1 Enterprise while under Ping Flood attack.

An overall higher processor utilization value is shown near 200 Mbps than the total link bandwidth in both cases of Figure 4.1 which is further described in this section. Figure 4.1 clearly depicts Microsoft Windows 10 is a direct software upgrade from Windows 8.1 based upon differences between OPU values. As mentioned earlier, Microsoft Windows 10 includes more built-in features than its predecessor.

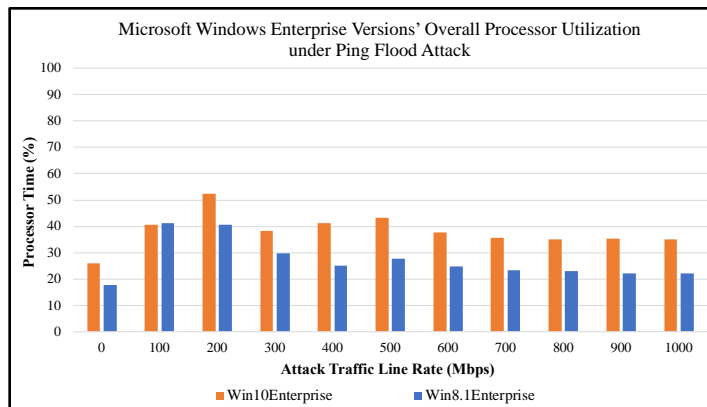


Figure 4.1: Microsoft Windows Enterprise Versions' Overall Processor Utilization under Ping Flood Attack

Figure 4.2 depicts Ping Flood attack posing a significant steady-state effect on the victim system in both operating systems. Every attack traffic line rate remains at one approximate value which is around 1,300 and 800 megabytes of memory consumed for Windows 10 and 8.1, respectively. Notably, Ping Flood attack is not memory intensive on Microsoft Windows Enterprise versions due to nearly identical memory consumption values throughout this entire experiment. Also, Microsoft Windows 10 has noticeably more memory consumption than Windows 8.1 in this simulation as shown in Figure 4.2. As previously mentioned, Microsoft Windows 10 includes more built-in features than Windows 8.1 as depicted in Figure 4.2.

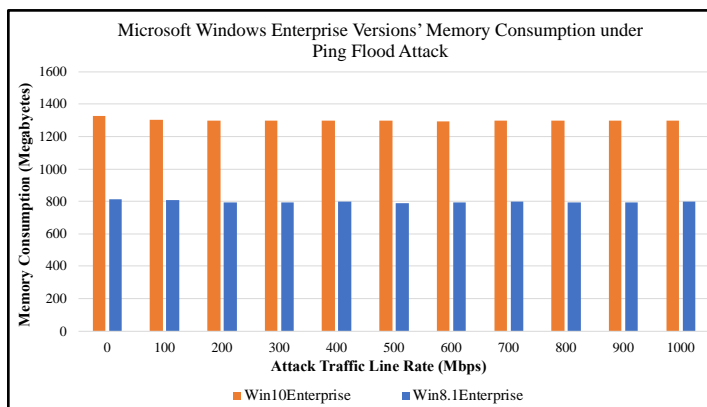


Figure 4.2: Microsoft Windows Enterprise Versions' Memory Consumption under Ping Flood Attack

The system's hard disk is not significantly affected in this entire simulation of Ping Flood attack as shown in Figure 4.3. Only Microsoft Windows 10 Enterprise exceeds ten percent of overall disk utilization near 200 Mbps of attack traffic which is shown as an obvious point of fluctuation for the victim system in Figure 4.3. Furthermore, a minimal initial disk utilization value is shown at zero attack traffic then, values slightly decrease at 100 Mbps and increase again near 200 Mbps for Windows 10 Enterprise during this simulation. The aforementioned fluctuation is determined as background processes during DDoS attack launch. After 200 Mbps of attack traffic, a similar steady-state pattern is shown with an approximate value of zero percent DU as seen in Figure 4.3. Also, in this simulation, Microsoft Windows 8.1 Enterprise shows DU values less than ten percent during this entire simulation along with a slow decline until a steady-state pattern is reached with a value of approximately zero percent matching Windows 10. As described for Figures 4.1 and 4.2, Windows 10 Enterprise values overall exceed Windows 8.1 Enterprise such as DU values during this simulation.

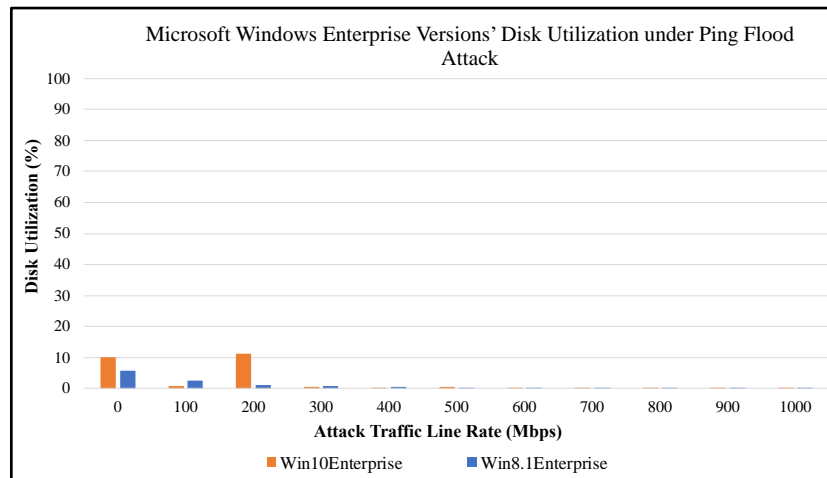


Figure 4.3: Microsoft Windows Enterprise Versions' Disk Utilization under Ping Flood Attack

While under Ping Flood attack, HTTP transactions rates completely diminished by 800 Mbps in both plots of Figure 4.4. However, Microsoft Windows 8.1 Enterprise hardly exchanged any

HTTP transactions after 500 Mbps. Although, Microsoft Windows 10 continued generating small yet, note-worthy amounts of HTTP transactions after 500 Mbps until ceasing all at 800 Mbps of attack traffic. Both Windows 10 and 8.1 Enterprise maintained all requested HTTP transactions until 200 Mbps during this simulation. The main difference between both operating systems in this experiment is within 300 and 500 Mbps of attack traffic because each operating system declines at different rates under Ping Flood attack. Microsoft Windows 10 Enterprise downgrades drastically from 3,000 to 1,300 between 300 and 500 Mbps of attack traffic during this simulation. After 300 Mbps of attack traffic, a steady decline can be seen in Figure 4.4 for Windows 10 Enterprise until completely ceasing all HTTP transactions. Windows 8.1 Enterprise shows a similar pattern in comparison with Windows 10 Enterprise during this simulation such that, HTTP transaction rates decline after 200 Mbps of attack traffic except with an approximate value of 2,000 transactions per second. Then, a steep decline occurs with a margin of approximately 1,300 HTTP transactions per second between 300 and 400 Mbps of attack traffic. Lastly, from 400 to 500 Mbps of attack traffic, a steady-state pattern is shown during this simulation for Microsoft Windows 8.1 with a value of approximately 640 transactions per second. Ultimately, Windows 10 and 8.1 Enterprise under Ping Flood attack show quite similar HTTP transaction decline patterns with a significant difference in rates of change.



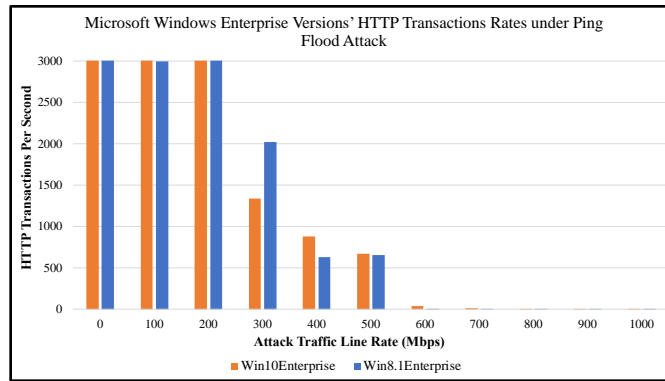


Figure 4.4: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under Ping Flood Attack

Cause for sporadic behaviors due to DDoS attack deployed on a victim system are not widely researched however, assumptions can be made such as the following. In both operating systems, as attack traffic increases, OPU also increases until 300 Mbps likewise, HTTP transaction rates are affected until approximately 300 Mbps. Thus, a tradeoff is shown near 300 Mbps of attack traffic in Figures 4.1 and 4.4 for both OPU and HTTP transaction rates. Simultaneously, OPU also decreases due to obvious resource compensation purposes during this simulation. During the remainder of this simulation, OPU stabilizes with a steady-state pattern and thereon only HTTP transaction rates are affected. Microsoft Windows 8.1 requires a unique configuration setting for legitimate traffic which explains prioritization for HTTP transactions in this case. This simulation is a clear indication of exhaustion of system resources for both systems.

#### 4.2 Microsoft Windows Enterprise Versions' under Smurf Attack

As mentioned in Chapter II, Smurf attack amplifies an attack by broadcasting echo requests on behalf of a victim via spoofed IP address. In Figure 4.5, OPU nears one hundred percent after just legitimate traffic (zero attack traffic) is sent to the victim system with Windows 10

Enterprise. Similarly, Windows 8.1 nears ninety percent OPU only after 100 Mbps of attack traffic is delivered as shown in Figure 4.5. However, the main difference between the two plots shown in Figure 4.5 is near 100 Mbps of attack traffic since a significant thirty percent difference in OPU is present. Also, as mentioned before, Windows 10 Enterprise values are significantly higher than Windows 8.1 Enterprise OPU values for this entire simulation. Both Windows 10 and 8.1 Enterprise versions show steady-state patterns for most of this simulation. As shown in Figure 4.1 and 4.5, initial OPU values for both Windows 10 and 8.1 Enterprise versions are nearly identical during Ping and Smurf attacks which consistently supports these simulations with a common baseline.

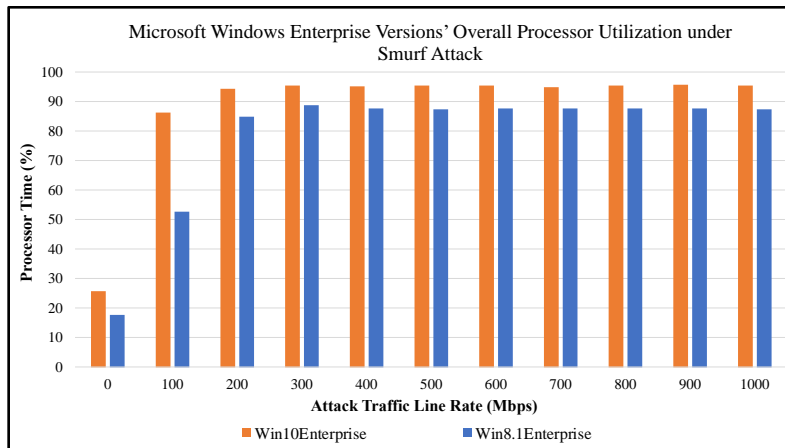


Figure 4.5: Microsoft Windows Enterprise Versions' Overall Processor Utilization under Smurf Attack

Figure 4.6 illustrates quite similar steady-state patterned plots in comparison to Figure 4.2 thus, note that each DDoS attack may affect memory consumption behaviors, for the victim system, in similar manners. However, memory consumption values differ slightly as shown in both Figures 4.2 and 4.6 primarily by approximately 160 megabytes for Windows 10 Enterprise.

Thus, memory consumption steady-state values for Windows 10 and 8.1 Enterprise under Smurf attack are near 1,470 and 800 megabytes, respectively.

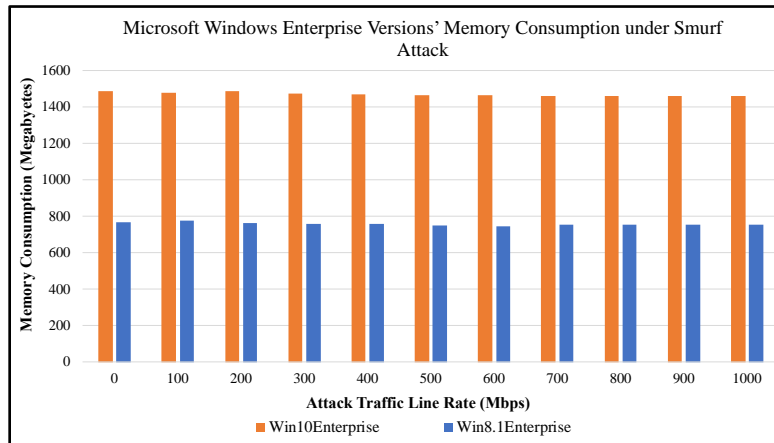


Figure 4.6: Microsoft Windows Enterprise Versions' under Memory Consumption under Smurf Attack

In comparison, Windows 10 Enterprise disk utilization plots from both Ping Flood and Smurf attacks show nearly identical patterns throughout each simulation with exception of overall larger magnitude during Smurf attack. As shown in Figures 4.3 and 4.7, the aforementioned pattern shows initial DU data fluctuation then a steady-state correlation until the end of simulation. However, Windows 8.1 Enterprise disk utilization values initially show an inverse behavior at a smaller magnitude only with respect to Windows 10 Enterprise initial data fluctuation as shown in Figure 4.7. After initial fluctuation in Windows 8.1 Enterprise data, disk utilization spikes from roughly five percent to one hundred percent of DU between 300 and 400 Mbps during this simulation. However, after 400 Mbps, Figure 4.7 shows significant fluctuation of DU for Windows 8.1 ranging from approximately eighty to one hundred percent of DU for the remainder of the simulation. This data fluctuation shows a declining slope from 400 to 800 Mbps of attack traffic then an increase in DU values from 800 Mbps until end of simulation. Disk utilization spikes occur under a process name of NT Kernel and System Application which is

further described in Chapter VII. Apparently, Smurf attack triggers another performance counter for this specific victim system due to resource compensation.

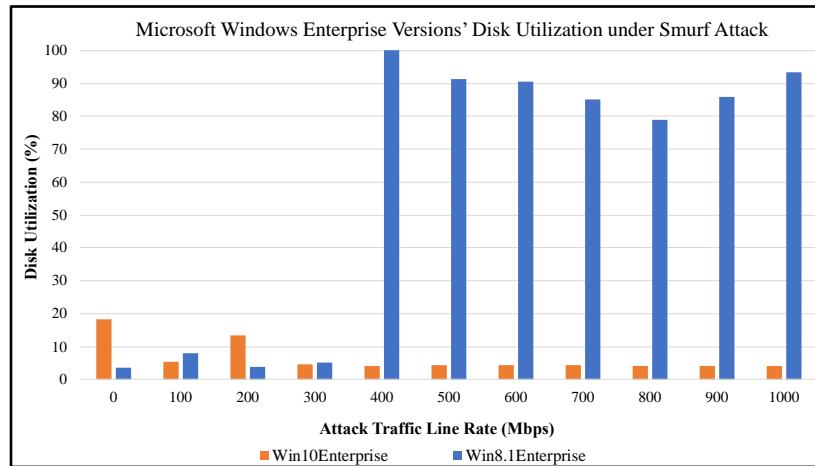


Figure 4.7: Microsoft Windows Enterprise Versions' Disk Utilization under Smurf Attack

Figure 4.8 shows significant differences between both operating systems under evaluation in this simulation for the following reasons. Windows 10 Enterprise nearly ceases HTTP transactions at 200 Mbps of attack traffic only providing approximately 250 HTTP transaction rates per second. Meanwhile, Windows 8.1 supports numerous HTTP transactions until 400 Mbps which quite steadily declined until ultimately ceasing all transactions. Nearly all HTTP transactions were successful until 300 Mbps of attack traffic which shows 1,500 HTTP transactions then approximately zero at 400 Mbps. Both Windows 10 and 8.1 Enterprise versions relatively cease all HTTP transactions after 300 Mbps whereas, Windows 8.1 shows small HTTP values at 400 and 500 Mbps. Again, Windows 8.1 prioritizes HTTP transactions instead of disk utilization due to a preconfigured setting.

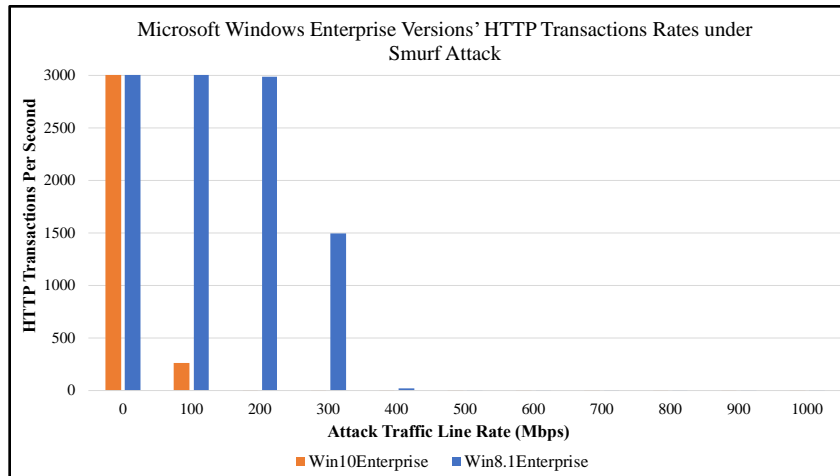


Figure 4.8: Microsoft Windows Enterprise Versions' HTTP transaction rates under Smurf Attack

In comparison, Figures 4.7 and 4.8 depict correlating fluctuation patterns due to large amounts of attack traffic. For example, in both Figures 4.7 and 4.8, Windows 8.1 plots show drastic changes at 400 Mbps such as, a decline in HTTP transaction rates and DU spikes to 1 Gbps. In comparison, Microsoft Windows 10 OPU data sharply increases at 100 Mbps of attack traffic as shown in Figure 4.5. Similarly, Figure 4.8 illustrates Windows 10 HTTP transaction rates significantly decrease at 100 Mbps of attack traffic. Clearly, the victim system is compensating for this large influx of attack traffic. As shown in Figure 4.7, this simulation forced the victim system to incorporate more resources in order to fulfil given instructions within Windows 8.1 which henceforth is dubbed resource compensation.

### 4.3 Microsoft Windows Enterprise Versions' under TCP-SYN Flood Attack

During a TCP-SYN flood attack, a hacker manipulates the three-way handshake to exhaust a victim's resources. As shown in Figure 4.9, both operating systems under evaluation, approach 100 percent of OPU after 300 Mbps of attack traffic. Although, Windows 10 Enterprise reaches near 100 percent of OPU faster than Windows 8.1 at just 100 Mbps of attack traffic during this simulation. Also, Figure 4.9 shows apparent fluctuation between zero and 400 Mbps of attack traffic for Windows 8.1 Enterprise OPU data similar to Ping Flood attack initial data fluctuation in both operating systems under investigation. However, unlike Ping Flood attack OPU data both operating systems do not present an alike pattern during this simulation. Windows 10 Enterprise shows an expected baseline value then, a steady pattern occurs during this attack. As mentioned before, Microsoft Windows 8.1 Enterprise shows initial fluctuation then a rough steady-state pattern. As described in Section 4.1, fluctuation is typically a result of multiple resources compensating one another as attack traffic increases over time especially near 300 Mbps of attack traffic.

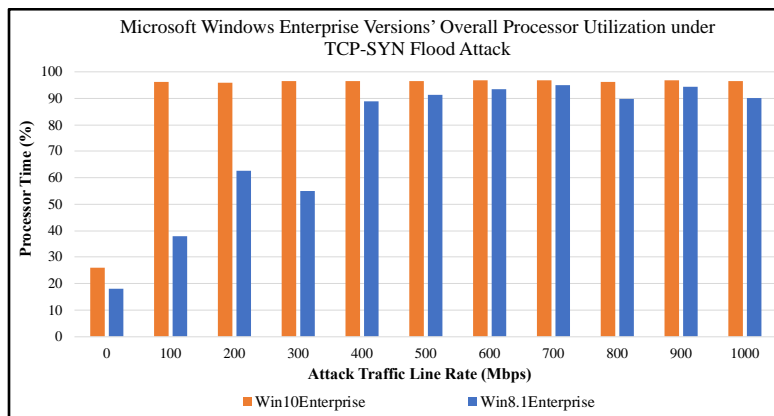


Figure 4.9: Microsoft Windows Enterprise Versions' Overall Processor Utilization under TCP-SYN Flood Attack

Presumably, the victim system does not change memory consumption data patterns for neither operating systems during this simulation, particularly only data values as shown in Figure 4.10. As described in a previous section, typically Windows 10 consumes more memory than Windows 8.1 operating system while under DDoS attack. Windows 10 and 8.1 Enterprise show steady-state values of approximately 1,460 and 760 megabytes of consumed memory, respectively.

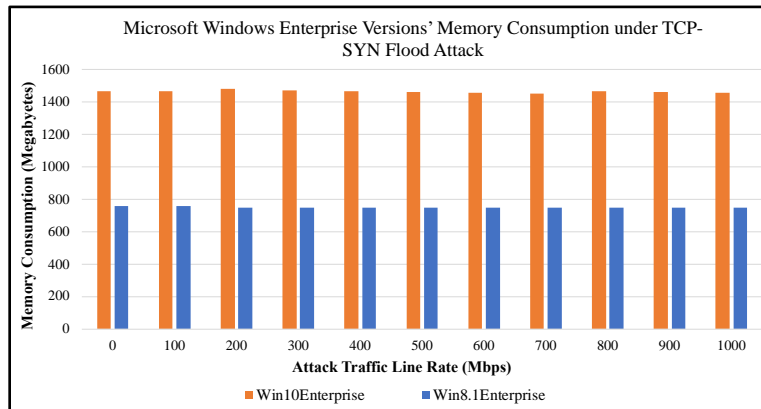


Figure 4.10: Microsoft Windows Enterprise Versions' Memory Consumption under TCP-SYN Flood Attack

Similar to Figure 4.3, Figure 4.11 shows neither operating system is notably affected by this simulation. However, at the baseline, Windows 10 DU data shows small spikes in value which are assumed as background processes. Similar to Ping Flood attack, Microsoft Windows 10 shows initial fluctuation while Windows 8.1 remains at a steady state. As attack traffic increases, the victim system responds sporadically proving flaws within Microsoft Windows 8.1 therefore not reoccurring for its successor.

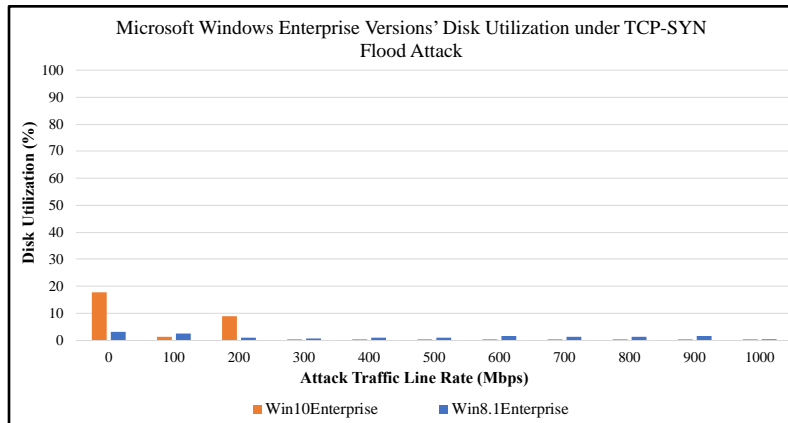


Figure 4.11: Microsoft Windows Enterprise Versions' Disk Utilization under TCP-SYN Flood Attack

HTTP transaction rates for both operating systems, as shown in Figure 4.12, differ significantly because Windows 10 data shows a familiar negative correlation from the victim system. However, Windows 8.1 data shows substantial fluctuation of HTTP transaction rates that relatively depict a negative trendline within this simulation. Although this negative trendline persists for nearly the entire simulation, a steep drop-off occurs between 900 Mbps and 1 Gbps of attack traffic.

Figures 4.9 and 4.12 illustrate Windows 8.1 overall performance as resource reliant for the following reasons. During this simulation, Windows 8.1 OPU increases as attack traffic intensifies which is expected however, once 300 Mbps of attack traffic is deployed HTTP transaction rates decrease for compensation purposes. This compensation within Windows 8.1 occurs throughout the course of this simulation as shown in Figures 4.9 and 4.12. Furthermore, OPU shows similar data patterns for both operating systems during this simulation. However, Windows 10 consumes more overall memory than Windows 8.1 and Windows 10 HTTP transaction rates decline quicker than Windows 8.1 during this simulation. Thus, in this simulation, Windows 8.1 holds an advantage in system performance over Windows 10 for the



aforementioned reasons. As mentioned previously in this chapter, Microsoft Windows 8.1 prioritizes HTTP transaction due to a preset configuration for legitimate traffic.

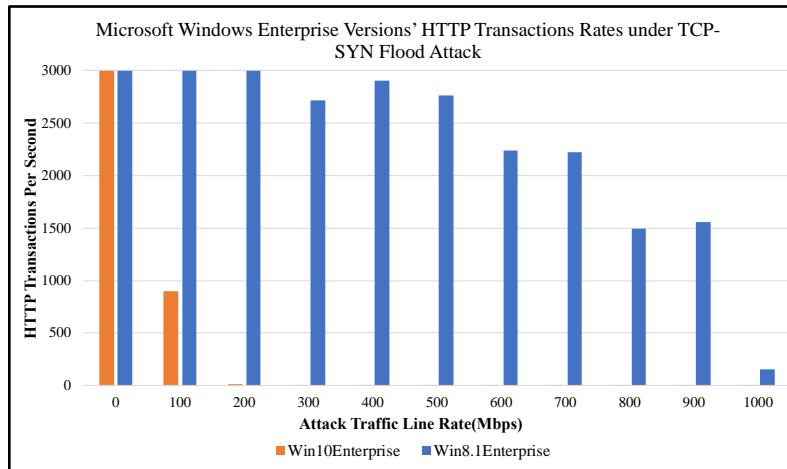


Figure 4.12: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under TCP-SYN Flood Attack

#### 4.4 Microsoft Windows Enterprise Versions' under UDP Flood Attack

As mentioned in a previous section, UDP Flood attack sends numerous UDP packets to maliciously overwhelm a victim system. During this simulation, a UDP Flood attack is sent to the victim system which causes a familiar fluctuation of data pattern for OPU in both operating system as shown in Figure 4.13. This data pattern begins to fluctuate from zero to 500 Mbps of attack traffic in both cases due to resource compensation as described earlier. Furthermore, both operating systems OPU values fluctuate until 400 Mbps of attack traffic due to resource compensation.

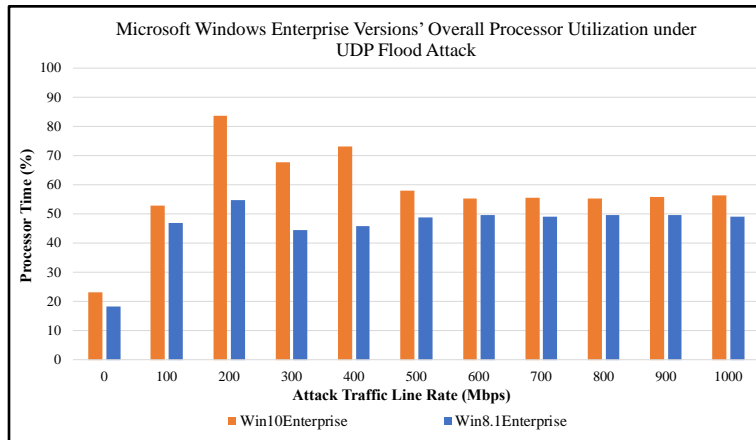


Figure 4.13: Microsoft Windows Enterprise Versions' Overall Processor Utilization under UDP Flood Attack

Figure 4.14 illustrates Windows 10 and 8.1 memory consumption as a steady-state phenomenon which is also recorded for all other DDoS attack simulations shown in each section of this chapter. During this simulation, memory consumption includes a maximum value of approximately 1,450 and 750 megabytes for both Windows 10 and 8.1, respectively while under UDP Flood attack.

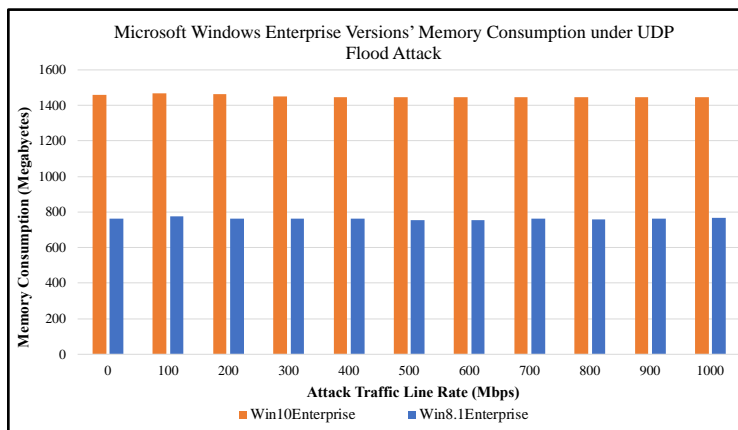


Figure 4.14: Microsoft Windows Enterprise Versions' Memory Consumption under UDP Flood Attack

Figure 4.15 shows disk utilization for both operating systems as slightly more active than Ping Flood and TCP-SYN Flood simulations. Although, Windows 8.1 disk utilization data has

greater values than Windows 10 for a majority of the duration of all attacks under investigation excluding Smurf. Figures 4.3 and 4.11 vaguely show similar disk utilization data patterns to Figure 4.15 for Windows 10 Enterprise during Ping, TCP-SYN, and UDP Flood attacks. Windows 10 and 8.1 disk utilization values measured during UDP Flood attack are recorded higher than Ping and TCP-SYN Flood due to compensation of resources which varies throughout each DDoS attack. Both operating systems under test fluctuate yet, inversely of one another during this simulation as shown in Figure 4.15.

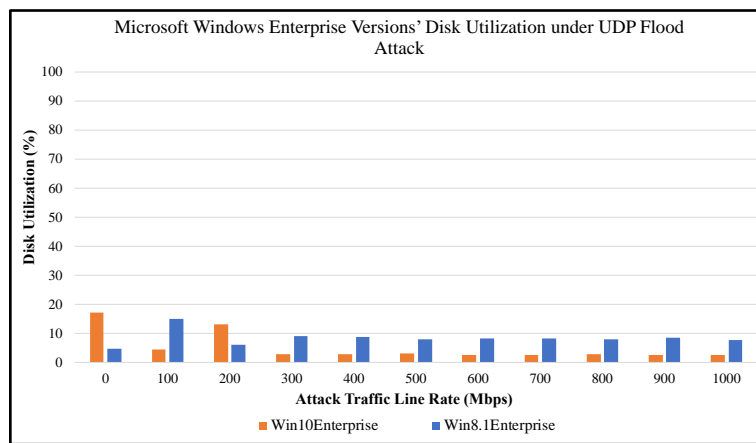


Figure 4.15: Microsoft Windows Enterprise Versions' Disk Utilization under UDP Flood Attack

Figure 4.16 depicts HTTP transaction rates, for both operating system, decreasing as the attack intensifies. As expected, Windows 10 HTTP transaction rates decreases drastically after 200 Mbps of attack traffic as a result of resource compensation. Similarly, Windows 8.1 data displays a negative correlation beginning after 200 Mbps yet, not as drastically as Windows 10. All HTTP transactions cease after 600 Mbps of attack traffic as shown in Figure 4.16. In this experiment, both operating systems show similar behaviors as Ping Flood attack.

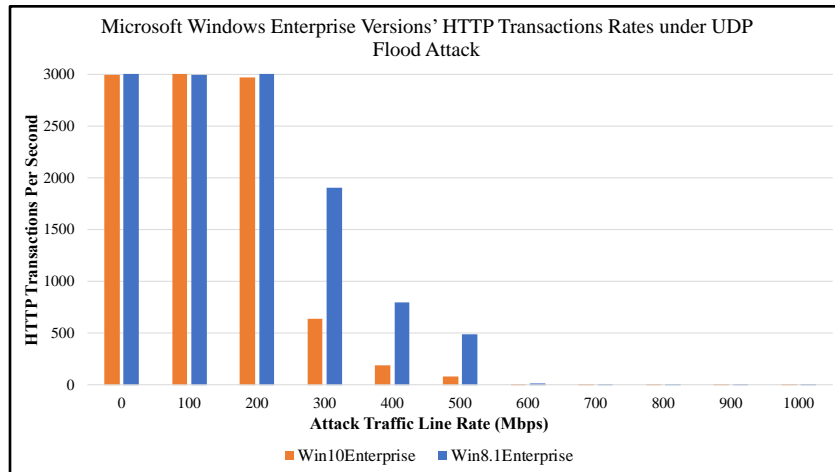


Figure 4.16: Microsoft Windows Enterprise Versions' HTTP Transaction Rates under UDP Flood Attack

#### 4.5 Chapter IV Summary

In this chapter, several iterations of various DDoS attacks are analyzed for evaluation purposes. In this case, several iterations consisted of two different operating systems which are both enterprise versions of Microsoft Windows 10 and 8.1. In comparison, Windows 10 and 8.1 both perform in quite similar manners due to resource compensations which are required by these operating systems in order to operate. Particularly, in both operating systems while under Ping Flood and UDP Flood attack, these compensations take affect by decreasing performance of one resource in order to support another, as shown above. However, another example of this is shown within TCP-SYN Flood attack for Windows 8.1 operating system. In Smurf attack, disk utilization was compromised in order to compensate other resources such as processor utilization due to intense amounts of attack traffic.

## CHAPTER V

### COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 PROFESSIONAL VERSIONS

Similar to Chapter III, chapter four describes a comparison of two operating systems which are both professional versions of Microsoft Windows 10 and 8.1 for analysis and evaluation purposes. Likewise, all four DDoS attacks and performance parameters shown in Chapter III are analyzed and evaluated within this chapter. Each figure within this chapter includes a legend signifying both professional versions of Windows 10 and 8.1 within each graph as follows: Win10Pro (Windows 10 Professional) and Win81Pro (Windows 8.1 Professional).

#### **5.1 Microsoft Windows Professional Versions' under Ping Attack**

Ping attack caused familiar fluctuation in OPU data for both enterprise versions of Windows operating systems under evaluation. Similarly, Figure 5.1 shows an identical OPU data pattern as Figure 4.1 which occurs due to resource compensation. Although, OPU percentage values for Windows 8.1 operating system are slightly different due to resource compensation throughout this attack in comparison with Figures 4.1 and 5.1.

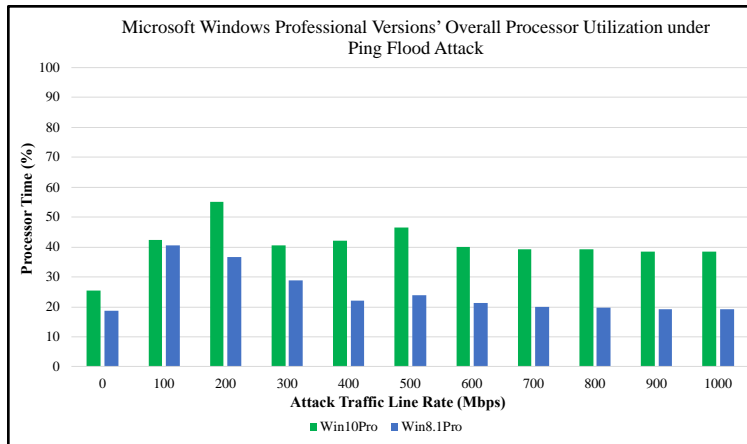


Figure 5.1: Microsoft Windows Professional Versions' Overall Processor Utilization under Ping Flood Attack

Figure 5.2 shows a steady-state pattern for both operating system during this simulation. However, Windows 8.1 Professional version memory consumption data under Ping Flood attack is notably lower than memory consumption data for Windows 8.1 Enterprise version by two hundred megabytes. Windows 10 Enterprise and Professional versions negligibly differ in memory consumption value during this simulation.

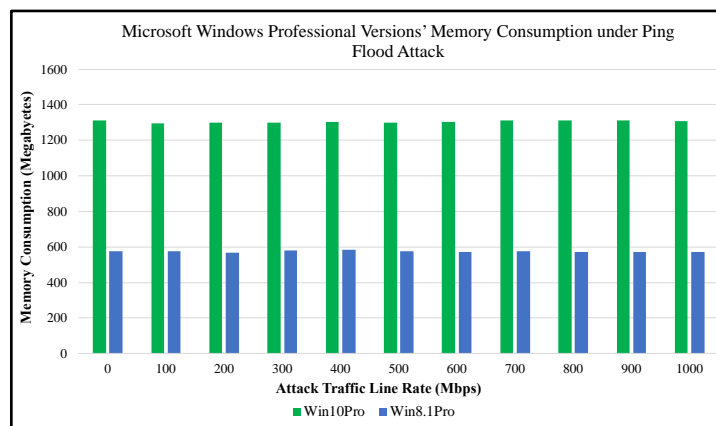


Figure 5.2: Microsoft Windows Professional Versions' Memory Consumption under Ping Flood Attack

Likewise, disk utilization shown in Figure 5.3 depicts a similar looking graph in comparison to Ping Flood and TCP-SYN Flood DU graphs within the previous chapter. As shown in Figure

5.3, a steady state trendline shows redundant DU data for both operating systems under evaluation with the exception of the baseline data for Windows 10. As described in Chapter 4, this baseline data short spike in DU value is likely caused by background processes.

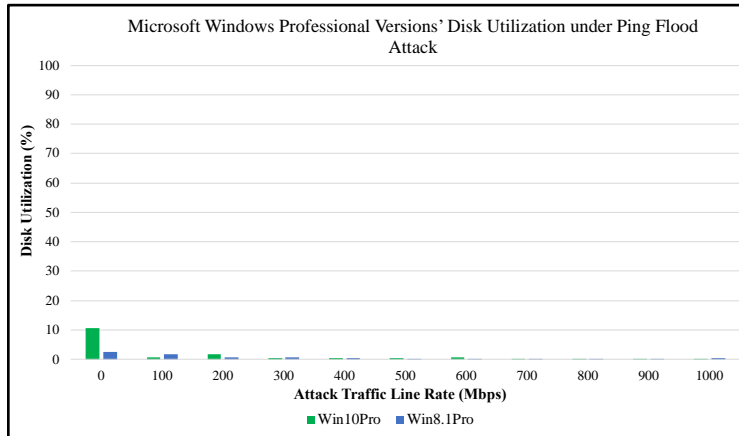


Figure 5.3: Microsoft Windows Professional Versions' Disk Utilization under Ping Flood Attack

As expected, similar-looking data is shown in Figure 5.4 because both operating systems HTTP transactions rates decrease near 300 Mbps of attack traffic. As mentioned previously, Windows 10 HTTP transactions rates decreases at a more rapid rate than Windows 8.1 during this simulation as shown in Section 4.1. However, during this simulation, Windows 10 HTTP transaction data shows a trendline even more similar to Windows 8.1. An educated assumption is made to describe the aforementioned behavior follows: Ping Flood attack in this section is not as intense as shown in Figure 4.4. Figure 4.4 illustrates further resource compensation than Figure 5.4 at 300 Mbps of attack traffic which causes HTTP transaction rates to drop in value for both operating systems. Again, Microsoft Windows 8.1 outperforms Windows 10 in HTTP transaction rates due to a preconfigured setting.

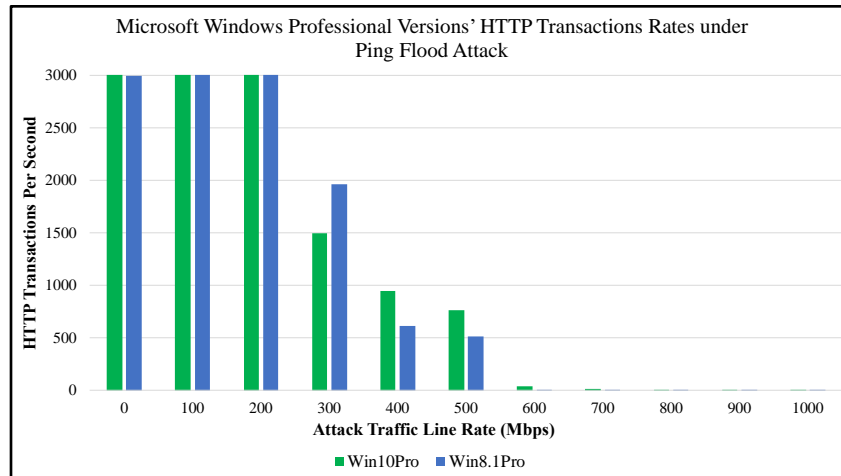


Figure 5.4: Microsoft Windows Professional Versions' HTTP Transaction Rates under Ping Flood Attack

## 5.2 Microsoft Windows Professional Versions' under Smurf Attack

Based on results from section 5.2, the following results shown within this section probably appear as identical to Chapter IV. Similarities may appear across different versions of Microsoft Windows 10 and 8.1 because both versions share many features as further described in Chapter VI. Although these results are from quite similar Windows versions, the purpose of this paper is to determine whether differences or similarities exist between versions while under various DDoS attack. Therefore, in Figure 5.5, a steady state trendline is shown in both operating systems which is similar to Figure 4.5.



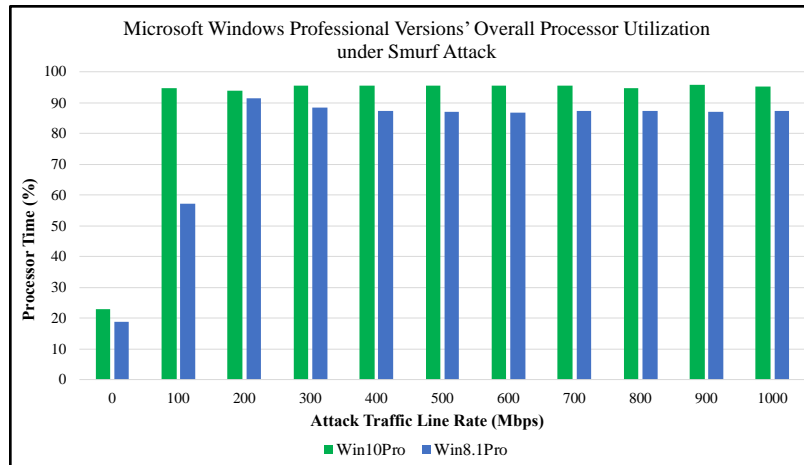


Figure 5.5: Microsoft Windows Professional Versions’ Overall Processor Utilization under Smurf Attack

Memory consumption remains as a constant steady-state trendline for both operating systems during this simulation. Although, Figure 5.6 conveys lower memory consumption values for both operating systems in comparison to each DDoS attack in Chapter IV with the exception of Ping Flood attack.

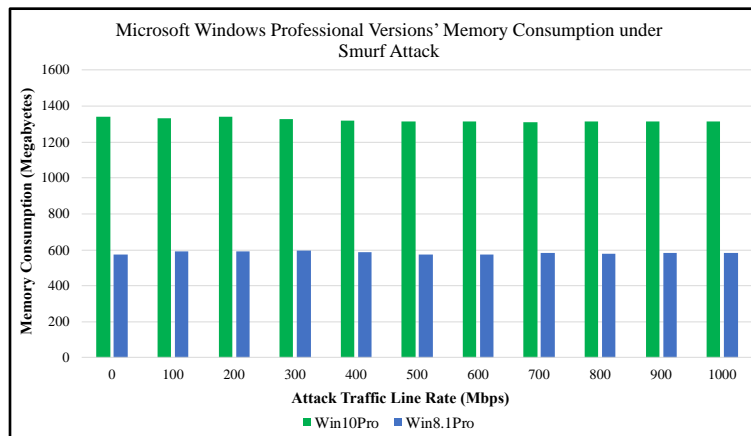


Figure 5.6: Microsoft Windows Professional Versions’ Memory Consumption under Smurf Attack

During this DDoS attack, disk utilization shows significant activity in comparison to each other DDoS attack which shows typically redundant data. Figure 5.7 conveys a closely identical

trendline compared to the Smurf attack DU data shown in Chapter IV which is caused by resource compensation. Likewise, the disk utilization process name is NT Kernel and System Application which is described in further detail in Chapter VIII.

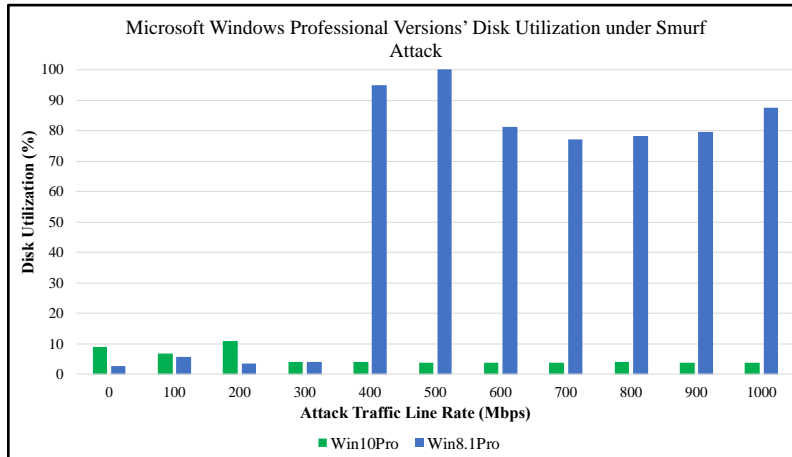


Figure 5.7: Microsoft Windows Professional Versions' Disk Utilization under Smurf Attack

In Figure 5.8, HTTP transaction rates begin to drop near 300 Mbps of attack traffic for Microsoft Windows 8.1 Professional. However, transaction rates quick diminish near 200 Mbps of attack traffic for Microsoft Windows 10 Professional. Disk utilization compensation accounts for differences seen in Figure 5.8.

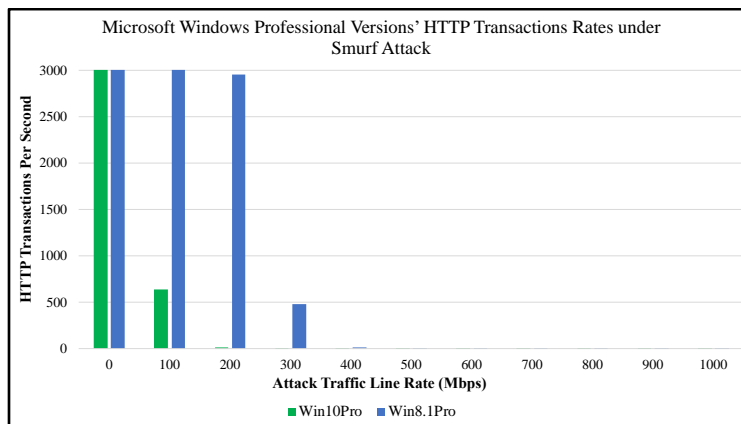


Figure 5.8: Microsoft Windows Professional Versions' HTTP Transaction Rates under Smurf Attack

### 5.3 Microsoft Windows Professional Versions' under TCP-SYN Flood Attack

In Chapter IV, TCP-SYN Flood attack caused a significant fluctuation data pattern from zero to 400 Mbps of attack traffic in Windows 8.1 yet, a steady-state OPU data pattern for Windows 10 version. Figure 5.9 illustrates this very aforementioned phenomenon occurred as well as similar OPU percentage values during this simulation for both operating systems.

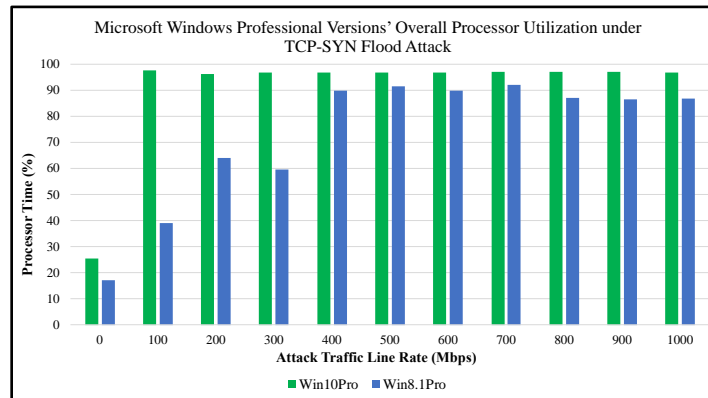


Figure 5.9: Microsoft Windows Professional Versions' Overall Processor Utilization under TCP-SYN Flood Attack

As mentioned previously, the following image continues to portray a constant and redundant graph for both operating systems in comparison with Section 4.3 as shown in Figure 5.10.

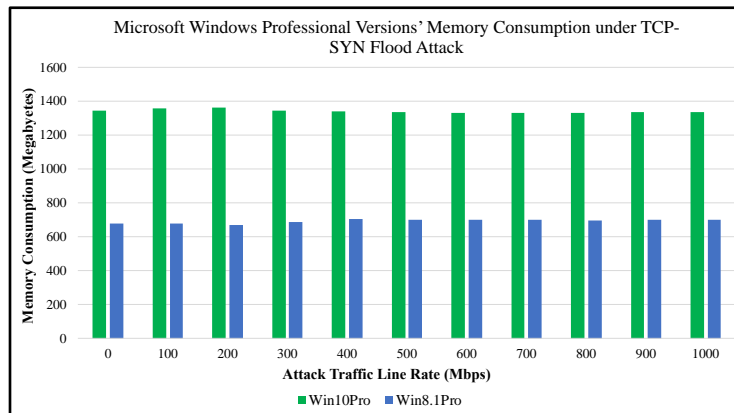


Figure 5.10: Microsoft Windows Professional Versions' Memory Consumption under TCP-SYN Flood Attack

Similarly, the following image shows a lack of noteworthy data for both operating systems under evaluation during this simulation.

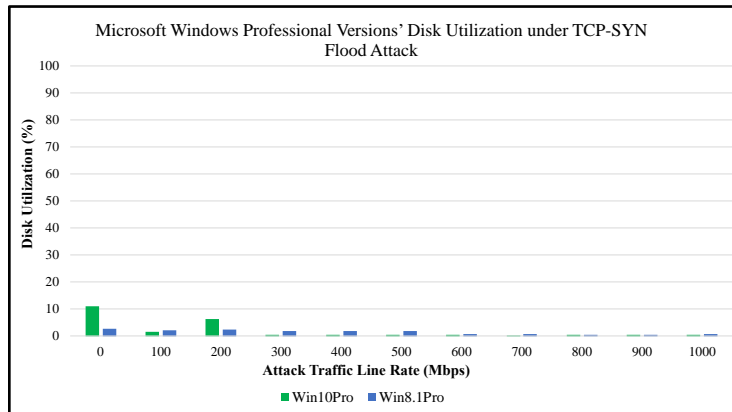


Figure 5.11: Microsoft Windows Professional Versions' Disk Utilization under TCP-SYN Flood Attack

As in Section 4.3, Windows 10 HTTP transactions decline quickly as attack traffic intensifies due to a threshold or resource compensation. Windows 8.1 HTTP transaction rates, during this simulation, are notably higher than other DDoS attacks yet, the cause for this is due to resource compensation. For example, in Figure 5.12, HTTP transactions do not completely cease for Windows 8.1 version however, OPU is much higher than UDP Flood and Ping Flood in overall value throughout this simulation. Windows 10 does not perform well during this attack opposed to Windows 8.1 because it cannot support HTTP transaction rates although overall memory consumption is higher than Windows 8.1. Also, consider OPU is quite similar during this simulation for both operating systems.

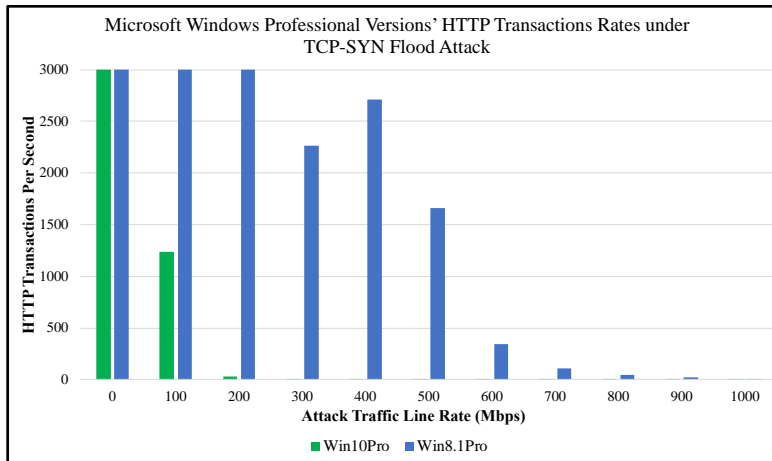


Figure 5.12: Microsoft Windows Professional Versions' HTTP Transaction Rates under TCP-SYN Flood Attack

#### 5.4 Microsoft Windows Professional Versions' under UDP Flood Attack

As shown in Section 4.4, UDP Flood attack OPU data fluctuates for both operating systems which is a result of resource compensation. In Figure 5.13, Windows 10 OPU data reaches a maximum of approximately eighty percent at 200 Mbps of attack traffic. Thereafter, OPU data for both operating systems eventually reach a steady-state trend which also results from resource compensation as described in Section 4.4.

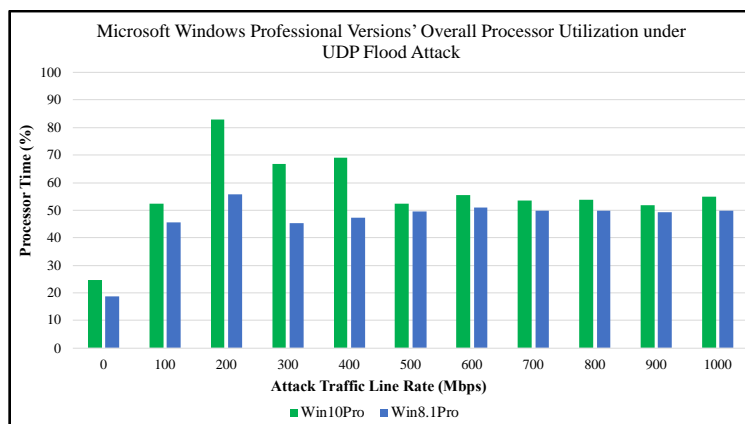


Figure 5.13: Microsoft Windows Professional Versions' Overall Processor Utilization under UDP Flood Attack

Figure 5.14 shows an image of memory consumption for both operating systems under evaluation which persists as portraying a steady state trendline during a UDP Flood attack. Additionally, Windows 10 Pro. shows quite similar memory consumption data in comparison with Windows 10 Ent. However, both Windows 8.1 Enterprise and Professional show a significant difference in steady-state values of approximately two hundred megabytes as shown in Figures 4.14 and 5.14.

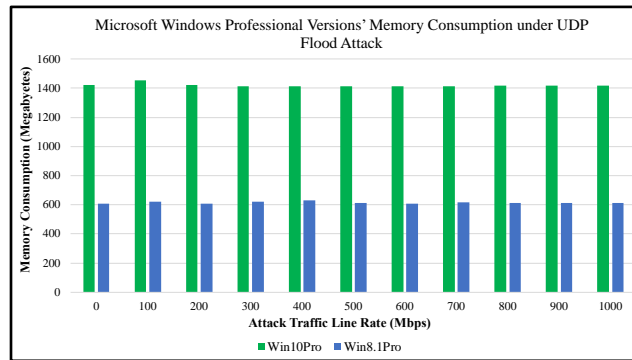


Figure 5.14: Microsoft Windows Professional Versions' Memory Consumption under UDP Flood Attack

The following graph shows redundant data as disk utilization is only affected while under Smurf attack as mentioned in detail above. Although, an initial DU value is shown which can be described as background processes during simulation initialization.

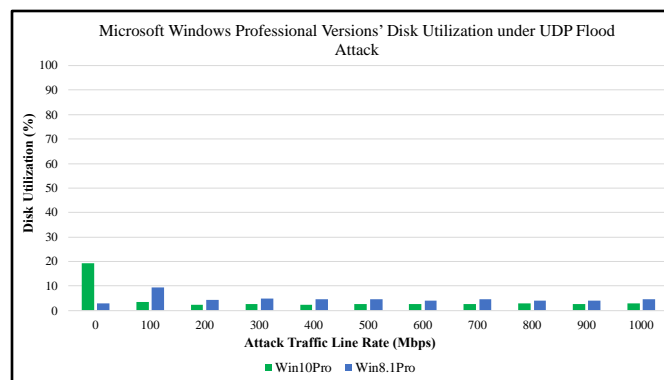


Figure 5.15: Microsoft Windows Professional Versions' Disk Utilization under UDP Flood Attack

Figure 5.16 shows similar HTTP transaction data compared to Section 4.4 because nearly each operating system shows nearly identical trendlines while comparing Windows 10 versions and Windows 8.1 versions, respectively. Figures 5.13 and 5.16 clearly show resource compensation for both operating systems except, Windows 10 quickly declines while Windows 8.1 does so slowly.

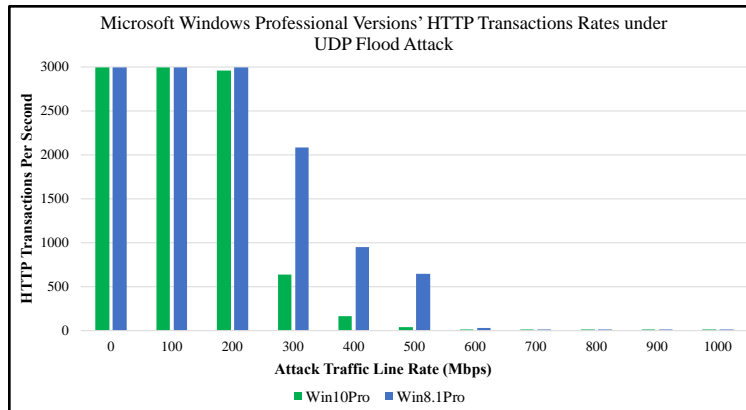


Figure 5.16: Microsoft Windows Professional Versions' HTTP Transaction Rates under UDP Flood Attack

## 5.5 Chapter V Summary

This chapter reflects data shown throughout Chapter IV however, these simulations support strong similarities between both professional versions of Windows 10 and 8.1. Based on Chapters III and IV, Smurf attack is the overall most intense attack of all four DDoS attacks because, this simulation causes the victim system to incorporate another resource in order to function properly. The least intense attack is Ping Flood attack because OPU for both operating systems do not exceed sixty percent which occurs in all other DDoS attacks.

## CHAPTER VI

### COMPARISON BETWEEN MICROSOFT WINDOWS 10 AND WINDOWS 8.1 CORE VERSIONS

As in previous chapters, Chapter VI describes a comparison of two operating systems which are both core versions of Microsoft Windows 10 and 8.1 for analysis and evaluation purposes. A core version of an operating system means the basic version since each succeeding version builds upon this version as a foundation. All four DDoS attacks and performance parameters shown in Chapter IV and V are analyzed and evaluated within this chapter. Each figure within this chapter includes a legend signifying both core versions of Windows 10 and 8.1 within each graph as follows: Win10Core (Windows 10 Core) and Win8.1Core (Windows 8.1 Core).

#### **6.1 Microsoft Windows Core Versions' under Ping Flood Attack**

As shown in previous chapters, a fluctuant trendline within the early stages of an attack signifies resource compensation during a simulation. Figure 6.1 shows the aforementioned trendline for both operating systems during this simulation. OPU data is quite similar to Section 5.1 while Section 4.1 shows higher OPU values for both operating systems. Although, these changes in values are caused by resource compensation most commonly near 300 Mbps of attack traffic for each simulation.



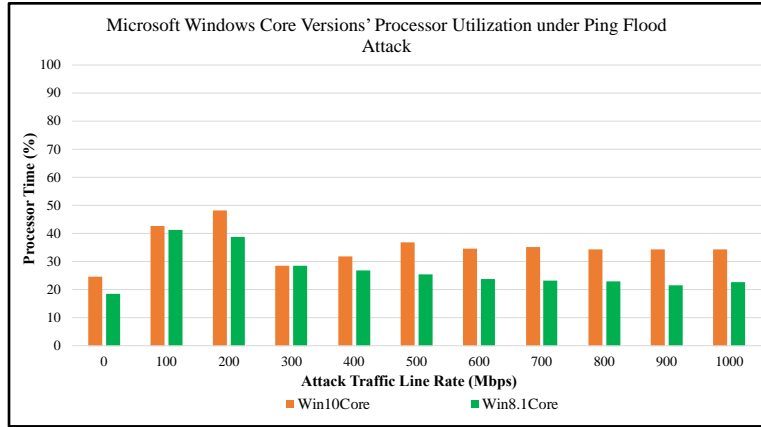


Figure 6.1: Microsoft Windows Core Versions' Overall Processor Utilization under Ping Flood Attack

As shown in Figure 6.2, the following performance parameter has shown consistent trendlines for both operating systems undergoing each DDoS attack in discussion throughout this paper. Additionally, Windows 8.1 Core memory consumption plot shows similar data values in megabytes as Windows 8.1 Professional version. However, Windows 8.1 Enterprise version memory consumption is significantly higher than both Core and Professional versions of Windows 8.1 due to installments of additional features.

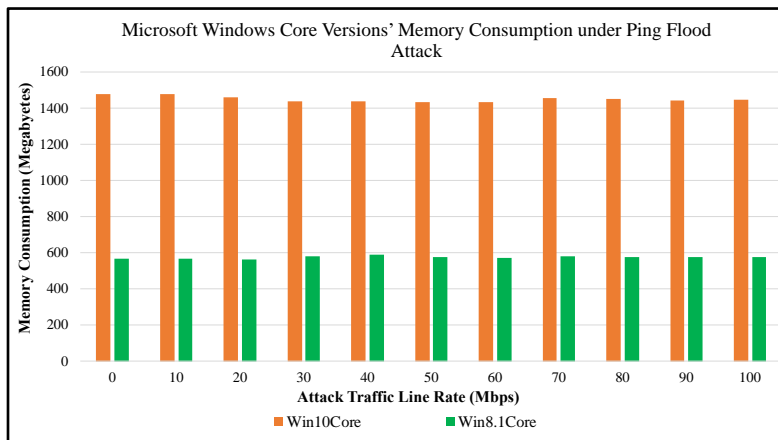


Figure 6.2: Microsoft Windows Core Versions' Memory Consumption under Ping Flood Attack

Disk utilization data did not depict substantial amounts of data while under Ping Flood attack for any Windows versions under evaluation. However, previous comparative chapters show a small baseline spike of DU for Windows 10 primarily. Windows 8.1 DU data did not show any note-worthy activity while under Ping Flood attack.

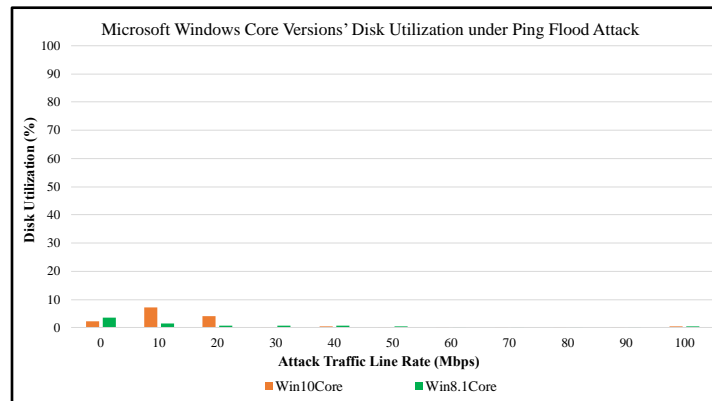


Figure 6.3: Microsoft Windows Core Versions' Disk Utilization under Ping Flood Attack

Interestingly, Ping Flood attack causes Windows 10 versions HTTP transaction data rates to convey similar data as Section 4.1 because a steep decline in data incurs at 300 Mbps of attack traffic due to resource compensation. HTTP transaction rates for all Windows 8.1 versions show a similar negative correlation during Ping Flood attack.

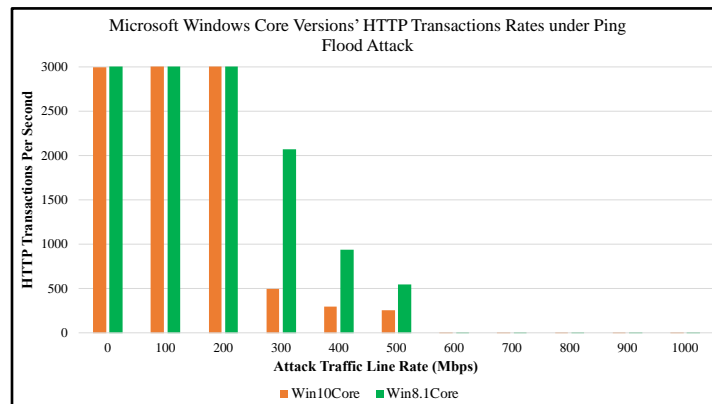


Figure 6.4: Microsoft Windows Core Versions' HTTP Transaction Rates under Ping Flood Attack

## 6.2 Microsoft Windows Core Versions' under Smurf Attack

In previous chapters, Smurf attack DU data shows obvious resource compensation with high OPU and low HTTP transaction rates in Windows 8.1 versions under evaluation. Likewise, as shown in Figure 6.5, both operating systems produce high OPU percentages after 100 Mbps of attack traffic.

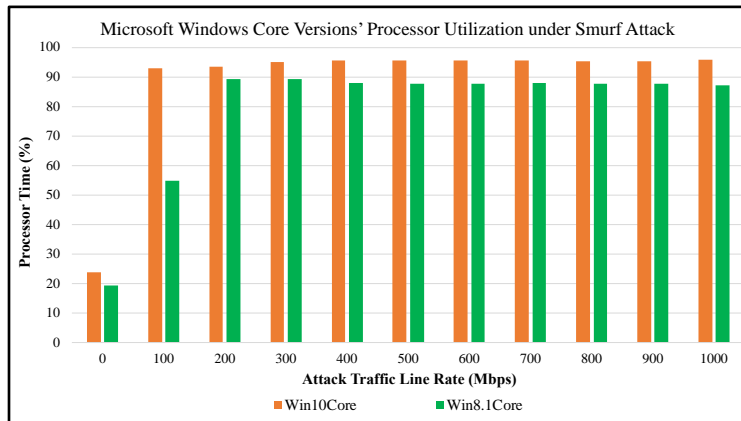


Figure 6.5: Microsoft Windows Core Versions' Overall Processor Utilization under Smurf Attack

Figure 6.6 shows two plots of memory consumption during a Ping Flood attack which is continually portrays as a steady state trendline for both operating systems undergoing each DDoS attack in discussion throughout this paper. Additionally, Windows 8.1 Core memory consumption plot shows similar data values in megabytes as Windows 8.1 Professional version during this simulation such as, Ping Flood attack. However, Windows 8.1 Enterprise version memory consumption is significantly higher than both Core and Professional versions of Windows 8.1 due to installments of additional features.

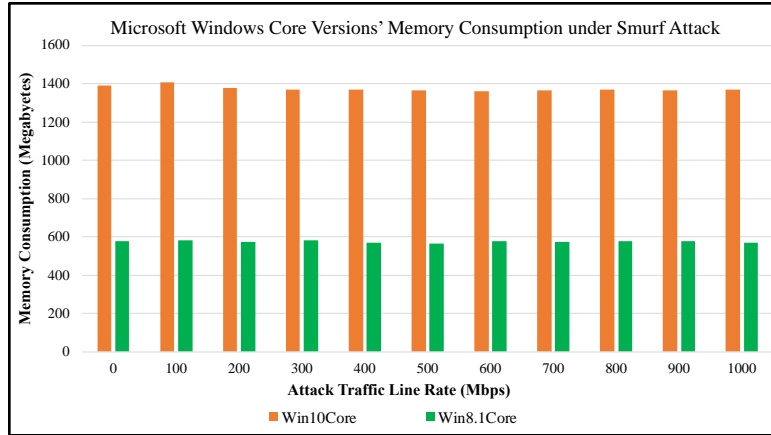


Figure 6.6: Microsoft Windows Core Versions' Memory Consumption under Smurf Attack

As expected, Windows 8.1 DU data shows high percentage values while under Smurf attack. Thus, in each comparative chapter, all versions of Windows 8.1 under evaluation initiated high DU percentage values during this attack. All Windows 10 version under evaluation significantly increased compensation of other resources such as, HTTP transaction rates because relatively similar values for DU are shown herein. In all Smurf attacks, high disk utilization values are caused by a process called NT Kernel & System Application in Microsoft Windows 8.1.

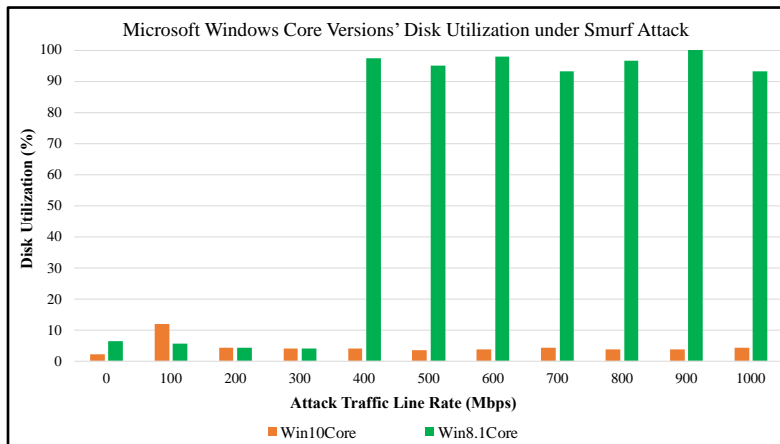


Figure 6.7: Microsoft Windows Core Versions' Disk Utilization under Smurf Attack

In Figure 6.8, Smurf attack causes HTTP transaction data rates for Windows 10 to convey similar data as Section 3.1 and 4.1 because a steep decline in data incurs at 100 Mbps of attack traffic due to resource compensation. However, the severity of each decline differs within each Smurf attack against Windows 10 versions under evaluation. HTTP transaction rates for Windows 10 versions under Smurf attack recorded as follows: Windows 10 Enterprise measured approximately two hundred and fifty transactions per second, Windows 10 Professional nearly five hundred, and Windows Core of about one thousand. HTTP transaction rates for all Windows 8.1 versions show a similar negative correlation during Smurf attack near 300 Mbps of attack traffic. However, similar to Windows 10, HTTP transaction rates differ in magnitude at 300 Mbps for each Windows 8.1 version as follows: Windows 8.1 Enterprise exchanged nearly one thousand five hundred transactions per second while Windows 8.1 Professional and Core measured about five hundred during each of their individual simulations.

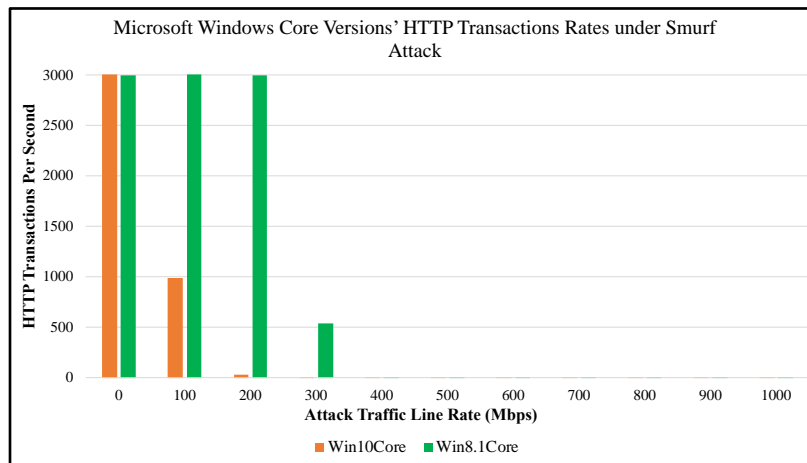


Figure 6.8: Microsoft Windows Core Versions' HTTP Transaction Rates under Smurf Attack

### 6.3 Microsoft Windows Core Versions' under TCP-SYN Flood Attack

In all comparative chapters, including this one, TCP-SYN Flood attack caused a significant fluctuation data pattern for OPU from zero to 400 Mbps of attack traffic in all versions of Windows 8.1 yet, a steady-state data pattern for Windows 10 versions. Furthermore, each comparative chapter included quite similar values of OPU throughout the duration of each attack for all operating systems under evaluation. Microsoft Windows 8.1 surpasses ninety percent of OPU near 400 Mbps of attack traffic. In most experiments, significant fluctuation is shown near 300 Mbps of attack traffic which is further described in Chapter VIII.

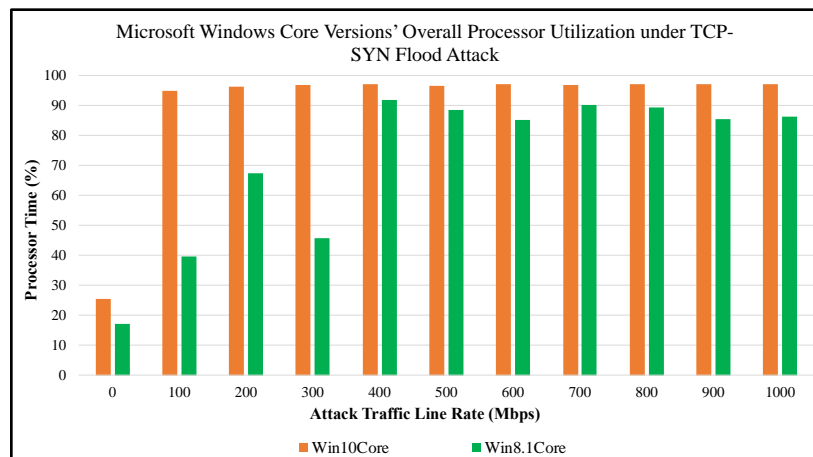


Figure 6.9: Microsoft Windows Core Versions' Overall Processor Utilization under TCP-SYN Flood Attack

Memory consumption data trendlines remained consistent throughout this paper during each TCP-SYN Flood attack and operating system under evaluation. In magnitude, each operating system stayed within a range of less than two hundred megabytes of one another during each simulation. These minor fluctuations were most likely caused by resource compensation which occurred during each TCP-SYN Flood attack for both operating systems.

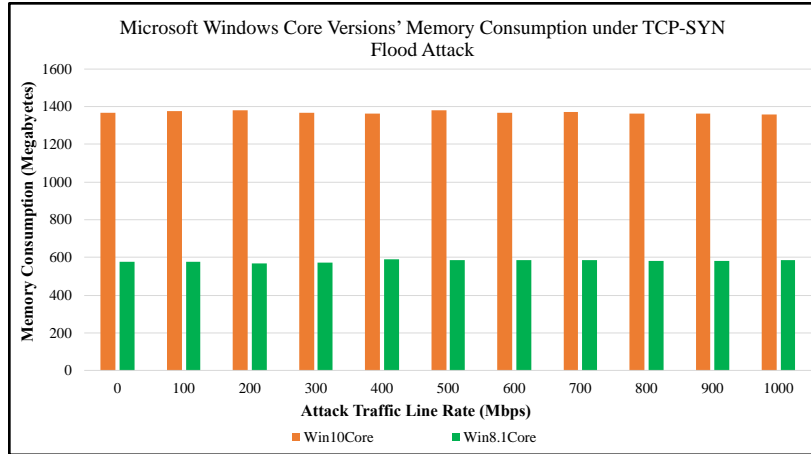


Figure 6.10: Microsoft Windows Core Versions' Memory Consumption under TCP-SYN Flood Attack

Disk utilization data trendlines remained consistent throughout this manuscript during each TCP-SYN Flood attack in both operating systems under evaluation. In magnitude, each operating system stayed within a range of less than twenty percent DU of one another during each simulation. These minor fluctuations were most likely caused by background processes during each simulation as mentioned earlier.

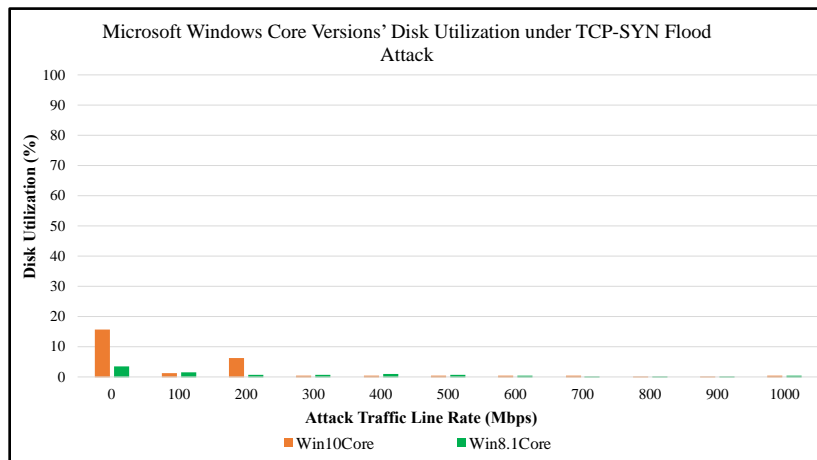


Figure 6.11: Microsoft Windows Core Versions' Disk Utilization under TCP-SYN Flood Attack

While comparing all three Windows 10 versions under evaluation, an apparent pattern shows TCP-SYN Flood attack quickly diminishing virtually all HTTP transactions near 200 Mbps of attack traffic during each iteration. Likewise, Windows 8.1 versions produce a similar pattern, in comparison, such that HTTP transaction rates begin to fall below three thousand HTTP transactions per second near 300 Mbps. Then, as previously mentioned, transaction rates rise again at 400 Mbps of attack traffic. Shortly thereafter, HTTP transaction rates fail to recover due to high amounts of attack traffic inundating the victim system. However, Windows 8.1 Core is affected more than both Windows 8.1 Professional and Enterprise versions because HTTP transactions significantly drop in value. For example, averaging raw values of HTTP transactions rates from 300 to 500 Mbps of attack traffic in each Windows 8.1 version accurately depicts this steep decline as shown below in approximation.

Table 1: Average HTTP Transactions Per Second within 300 to 500 Mbps of Attack Traffic

<b>Windows 8.1 Version</b>	<b>HTTP Transactions Per Second</b>
Core	1,185
Professional	2,214
Enterprise	2,797



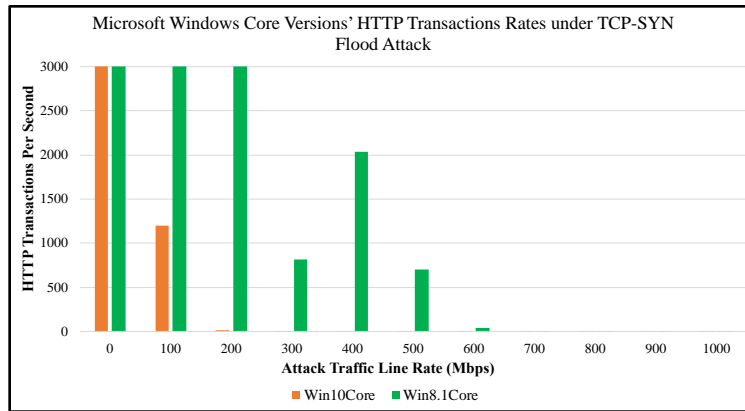


Figure 6.12: Microsoft Windows Core Versions' HTTP Transaction Rates under TCP-SYN Flood Attack

### 6.4 Microsoft Windows Core Versions' under UDP Flood Attack

Similar to most subsections in this paper, UDP Flood Attack affected the victim system showing familiar data trendlines as shown in Figures 4.13, 5.13, and 6.13. OPU data from UDP Flood attacks throughout Chapters IV, V, and VI for each operating system under evaluation maintain clear resemblance in comparison. As aforementioned, trendlines for OPU during UDP Flood attacks for all operating systems resemble a pair of brief inclines then, a steady-state pattern.

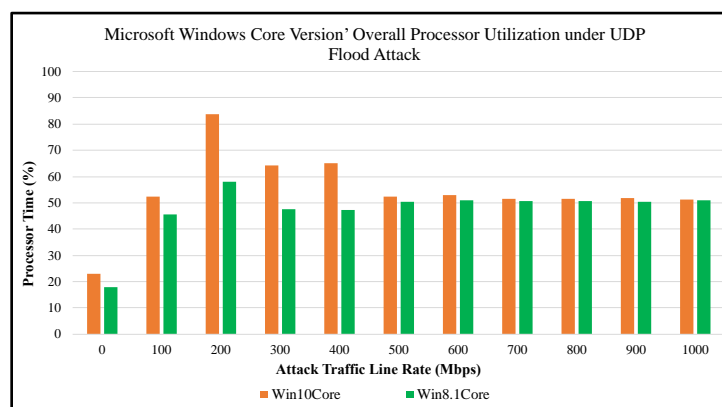


Figure 6.13: Microsoft Windows Core Versions' Overall Processor Utilization under UDP Flood Attack

As mentioned throughout this paper, memory consumption has consistently shown an overall steady-state pattern during each DDoS attack for all operating systems under evaluation. As shown in Figure 6.14, a similar data pattern for memory consumption is quite obvious for both versions. However, a steady-state value of approximately 1,300 megabytes is shown for Windows 10 Core throughout this attack. Dissimilarly, Windows 10 Enterprise and Professional memory consumption steady-state values both slightly exceed 1,400 megabytes. Furthermore, Windows 8.1 Core shows very similar steady-states memory consumption values in comparison with Windows 8.1 Professional. Microsoft Windows 8.1 consumes less memory consumption than Windows 10 in all cases.

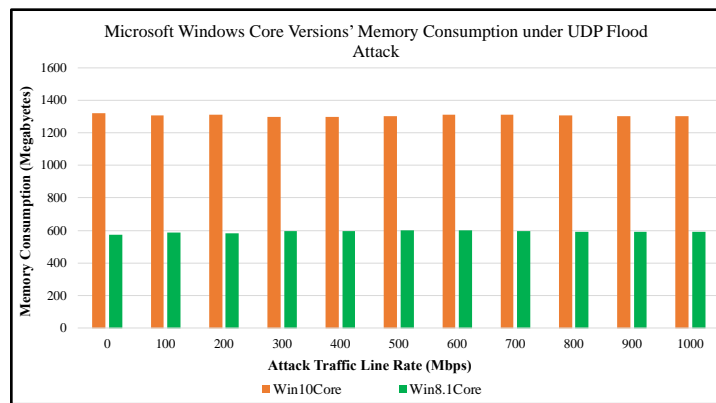


Figure 6.14: Microsoft Windows Core Versions' Memory Consumption under UDP Flood Attack

In Figure 6.15, Windows 10 Core plot shows an initial value of about ten percent of disk utilization then, a steady-state pattern until the end of simulation with a value of about three percent. Windows 8.1 Core DU plot illustrates a similar fluctuation pattern shown from zero to 200 Mbps of attack traffic while under UDP Flood attack. After 200 Mbps of attack traffic, another steady-state pattern is shown until end of simulation with a value of about five percent of DU. UDP Flood attack did not significantly affect Windows 10 and 8.1 Core versions as all DU

values are below ten percent. Small fluctuations are sporadic in Windows 8.1 due to gradual increase in attack traffic which is not seen in Windows 10.

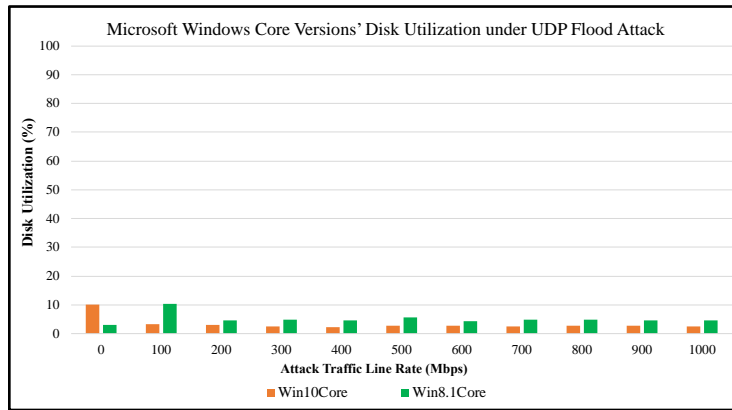


Figure 6.15: Microsoft Windows Core Versions' Disk Utilization under UDP Flood Attack

Familiarly, Windows 10 Core plot shows HTTP transaction rates persist until 300 Mbps of attack traffic during this simulation. At 300 Mbps of attack traffic, HTTP transaction rates plummet to about four hundred in value. After 300 Mbps of attack traffic, transaction rates never recover for Windows 10 Core while enduring UDP Flood attack. Windows 8.1 Core shows a similar pattern in comparison to Windows 10 only until 300 Mbps of attack traffic. After 300 Mbps of attack traffic, for Windows 8.1 Core HTTP transaction rates plot, a gradual decline is shown until 600 Mbps. At 600 Mbps of attack traffic, all transactions cease for Windows 8.1 Core while under UDP Flood attack which can also be seen in the Ping Flood attack section of this chapter. Microsoft Windows 8.1 consistently outperformed Windows 10 in HTTP transaction rates due to legitimate traffic setting.

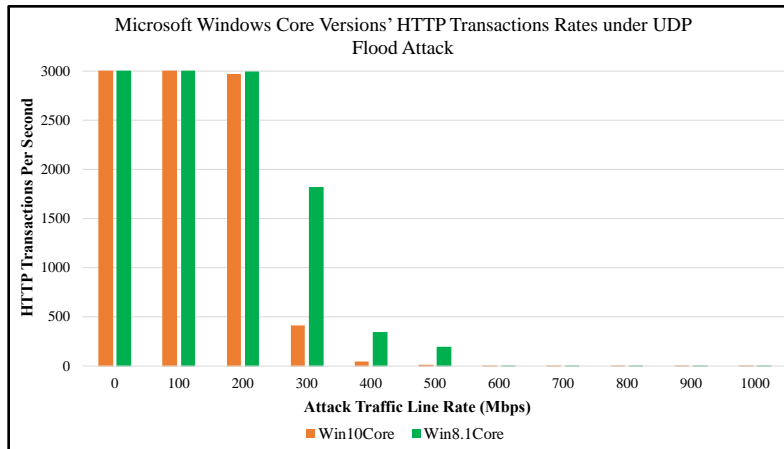


Figure 6.16: Microsoft Windows Core Versions' HTTP Transaction Rates under UDP Flood Attack

### 6.5 Chapter VI Summary

Similar plot patterns are shown throughout this chapter such as in previous chapters however, Windows 8.1 Core data shows a particular oddity while under TCP-SYN Flood attack. In section 6.3, Windows 8.1 Core plot for HTTP transaction rates shows an unusual fluctuation pattern between 300 and 500 Mbps of attack traffic. Clearly, this unusual fluctuation is shown in all TCP-SYN Flood attacks for each Windows 8.1 version under investigation. Furthermore, each Windows 8.1 version under TCP-SYN Flood attack surpasses ninety percent of OPU. Yet, Ping Flood, UDP Flood, and Smurf attack do not cross ninety percent of OPU because either attack is not intense enough or compensation occurs elsewhere. Thus, the aforementioned unusual fluctuation occurs due to compensation because as HTTP transaction rates increase during this attack OPU increases simultaneously.

## CHAPTER VII

### FURTHER COMPARISON

In this chapter, additional comparisons are given to highlight outcomes in previous chapters. Additional comparisons include analysis of particular attacks and operating systems herein. As shown in Figure 7.1, a clearer indication of a familiar fluctuation is shown in Microsoft Windows 8.1 Enterprise. Likewise, Microsoft Windows 8.1 Core spikes to a maximum value of 100 percent disk utilization at 900 Mbps then, slightly drops back to 1 Gbps. After further research, attack traffic was overloading the victim system's disk and other resources. As a result, overflow traffic offloaded to other processes such as non-recorded performance parameters.

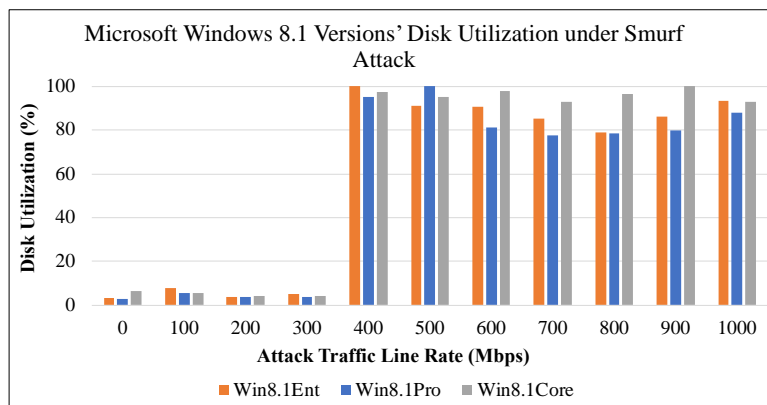


Figure 7.1: Microsoft Windows Versions' Disk Utilization under Smurf Attack

As shown in Figure 7.2, a similar pattern is shown for all plots of Microsoft Windows 8.1 under TCP-SYN Flood attack while Enterprise version lasts throughout the entire simulation. As an observation, Microsoft Windows Enterprise persists longer than its comparisons due to its robust built-in security features. As mentioned in Chapter III, Microsoft Windows Professional and Core versions do not include as many features as Enterprise.

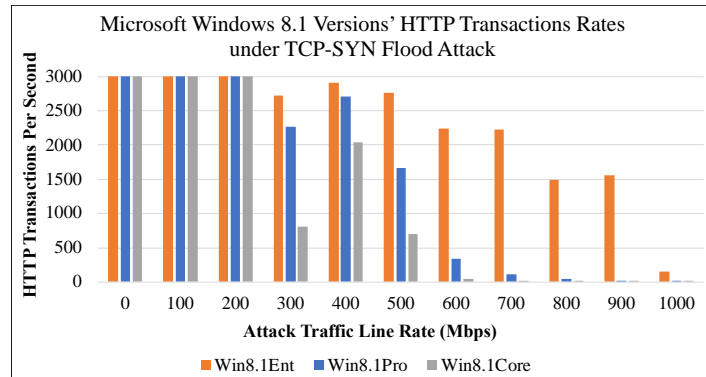


Figure 7.2: Microsoft Windows Versions' HTTP Transaction Rates under TCP-SYN Flood Attack

As shown in Figure 7.3, a broader analysis of this experiment is depicted as results and conclusions remain mostly consistent across all windows versions in these simulations. High disk utilization values under Smurf attack for Microsoft Windows 8.1 Core version while all other attacks show minimal values mentioned in further detail in Chapter VIII.

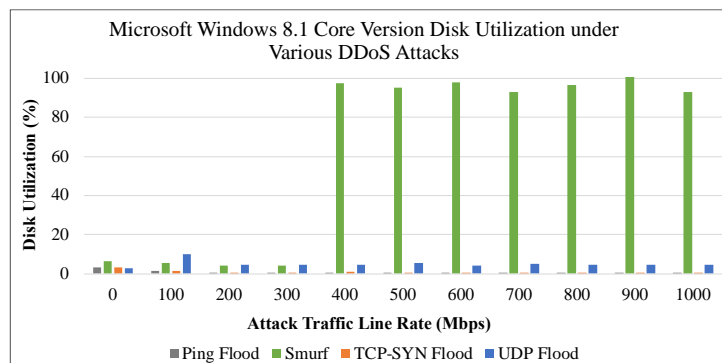


Figure 7.3: Microsoft Windows 8.1 Core Version Disk Utilization under Various DDoS Attacks

As shown earlier, high HTTP transaction rates can be seen only during TCP-SYN Flood attack for Microsoft Windows 8.1 Enterprise version. Meanwhile, other attacks near zero transactions between 300 and 500 Mbps whereas TCP-SYN transactions last until maximum data rate. After further investigation, Microsoft Windows 8.1 prioritizes HTTP transaction rates over other resources due to preconfigured settings for legitimate traffic.

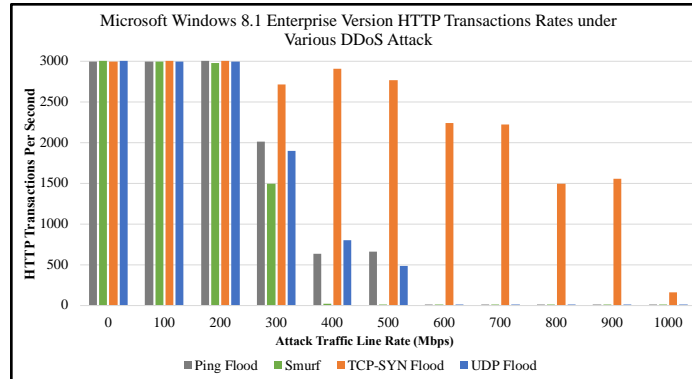


Figure 7.4: Microsoft Windows 8.1 Enterprise Version HTTP Transaction Rates under DDoS Various Attacks

As shown in Figure 7.5, Microsoft Windows 10 Enterprise version shows a steady baseline for processor utilization under all attacks. Subsequently, higher OPU values for Smurf and TCP-SYN Flood attacks whereas Ping Flood and UDP Flood do not utilize as much. As a conclusion, PDU architecture explains Figure 7.5 because both Ping Flood and UDP Flood attacks require response via ICMP, while Smurf and TCP do not. Therefore, Ping and UDP Flood attacks only process their requests until a response is requested. Then, the victim system drops their packets consequently which is less intensive for victim systems. In comparison, Smurf and TCP-SYN Flood attacks receive all packets sent [38].

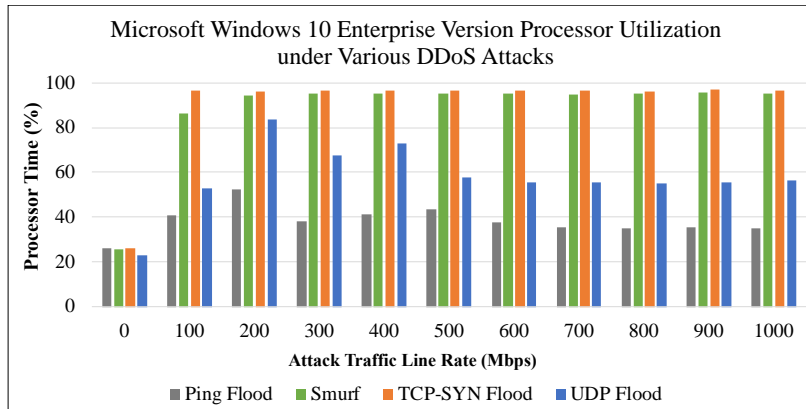


Figure 7.5: Microsoft Windows 10 Enterprise Version Overall Processor Utilization under Various DDoS Attacks

As shown in Figure 7.6, Ping Flood attack records a high memory consumption value which concludes Ping and UDP Flood Attacks are more memory intensive in Microsoft Windows 10 Professional and Core versions respectively due to PDU requirements.

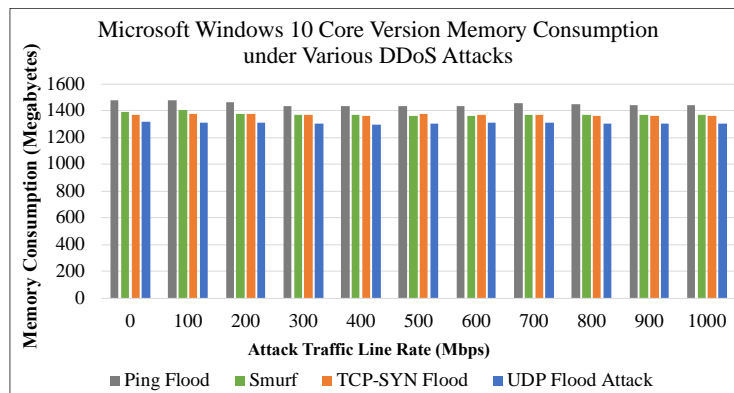


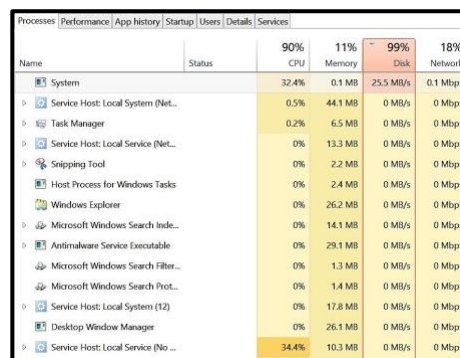
Figure 7.6: Microsoft Windows 10 Enterprise Version Memory Consumption under Various DDoS Attacks



## CHAPTER VIII

### CONCLUSION

Generally, each experiment presents fair indications of interesting findings for DDoS attacks mentioned herein. These DDoS attacks serve as threats typically yet, in this case, substantial data is observed and evaluated for exposure purposes. DDoS attacks under test herein show different outcomes in each simulation. For example, Smurf attack served as the greatest threat to the victim system for both operating systems under evaluation. An obvious example is disk utilization values for each Windows 8.1 version which reached 100 percent during multiple simulations. With further investigation, a process named NT Kernel & System Application included this high disk utilization value as shown in Figure 8.1. Furthermore, this process handles operations in protocol interfaces to reduce memory consumption [69]. Thus, one additional resource was required for Microsoft Windows 8.1 versions while under Smurf attack for resource compensation purposes. Obviously, Microsoft fixed this issue for Windows 10 versions.



The screenshot shows the Windows Task Manager Performance tab. The 'Disk' section is highlighted in red, indicating a critical level of usage. The 'Disk' usage is at 99%, with a progress bar showing 25.5 MB/s. The 'System' process is highlighted in yellow, indicating high CPU usage at 32.4%.

Name	Status	90% CPU	11% Memory	99% Disk	18% Network
System		32.4%	0.1 MB	25.5 MB/s	0.1 Mbps
Service Host: Local System (Net...)		0.5%	44.1 MB	0 MB/s	0 Mbps
Task Manager		0.2%	6.5 MB	0 MB/s	0 Mbps
Service Host: Local Service (Net...)		0%	13.3 MB	0 MB/s	0 Mbps
Snipping Tool		0%	2.2 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.4 MB	0 MB/s	0 Mbps
Windows Explorer		0%	26.2 MB	0 MB/s	0 Mbps
Microsoft Windows Search Indexing		0%	14.1 MB	0 MB/s	0 Mbps
Antimalware Service Executable		0%	29.1 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filter...		0%	1.3 MB	0 MB/s	0 Mbps
Microsoft Windows Search Prot...		0%	1.4 MB	0 MB/s	0 Mbps
Service Host: Local System (12)		0%	17.8 MB	0 MB/s	0 Mbps
Desktop Window Manager		0%	26.1 MB	0 MB/s	0 Mbps
Service Host: Local Service (No ...)		34.4%	10.3 MB	0 MB/s	0 Mbps

Figure 8.1: Microsoft Windows 8.1 Disk Utilization Near 100 Percent under Smurf Attack

Similarly, Microsoft Windows 8.1 prioritized HTTP transactions instead of disk utilization during TCP-SYN Flood attacks because of a preconfigured firewall setting. Furthermore, Windows 8.1 requires enabling of a firewall rule before HTTP transaction can be exchanged whereas Windows 10 does not require such beforehand. Therefore, this firewall rule favors HTTP transactions due to a manual setting opposed to other resources such as OPU. Likewise, Microsoft Windows 10 and 8.1 preconfigured setting negatively affected UDP Flood attack in all aspects. In Microsoft Windows 8.1 a required setting for legitimate traffic caused the victim system significant harm during each simulation under UDP Flood attack. Likewise, Microsoft Windows 10 required a similar setting for configuration of UDP Flood attacks resulting in nonideal conditions for the victim system. Further research regarding these cases were not found.

In light of predictions, Microsoft Windows 8.1 versions did not completely exhaust their memory and OPU while under Ping Flood attack in this experiment. However, after 600 Mbps of attack traffic HTTP transactions did cease as predicted during each Smurf attack in Microsoft Windows 8.1. Microsoft Windows 10 output lower OPU, memory consumption, and HTTP transaction values than Window 8.1 throughout entire experiment. Additionally, in each experiment, Microsoft Windows 10 editions could not withstand high amounts of attack traffic causing HTTP transactions rates to diminish quickly. Memory consumption and most disk utilization maintained consistent steady-state values throughout all simulations. Thus, DDoS attacks simulations herein are shown as processor, and in certain cases, hard disk intensive. Overall, all Microsoft Windows 10 version's results are better than Microsoft Windows 8.1 version due to high disk utilization in Smurf attack and HTTP transaction rates in TCP-SYN Flood attack simulations. Likewise, Microsoft Windows Enterprise versions shows better security features than Professional in Figure 7.2. Similarly, Microsoft Windows Professional

performs better than Windows Core in Figure 7.2 as well. Smurf and TCP-SYN Flood serve as most intense attacks overall which is based on PDU architecture as mentioned in Chapter VII [43]. Likewise, UDP Flood and Ping Flood attacks less overall intensive due to PDU architectures.

## REFERENCES

- [1] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, San Jose, CA, 2007, pp. 25-25.
- [2] B. A. Mah, "An empirical model of HTTP network traffic," *Proceedings of INFOCOM '97, Kobe, Japan, 1997*, pp. 592-600 vol.2.
- [3] G. R. Gunnam and S. Kumar, "Do ICMP Security Attacks Have Same Impact on Servers?" *Journal of Information Security*, vol. 08, no. 03, pp. 274–283, 2017.
- [4] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," in *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425-432, April 1980.
- [5] Siris, Vasilios A. "The OSI Model and Switching." *Enterprise Networking: Multilayer Switching and Applications*. IGI Global, 2002. 1-14.
- [6] Stallings, William. "Data and Computer Communications Tenth Edition". *Pearson Education Inc./Prentice Hall*, 2014.
- [7] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," *2013 International Conference on Availability, Reliability and Security, Regensburg*, 2013, pp. 546-555.
- [8] Sattarova Feruza, Y., and Tao-hoon Kim. "IT security review: Privacy, protection, access control, assurance and system security." *International journal of multimedia and ubiquitous engineering 2.2: 17-32*. 2007.
- [9] Farooq, Muhammad Umar, et al. "A critical analysis on the security concerns of internet of things (IoT)." *International Journal of Computer Applications 111.7*. 2015.
- [10] S. Kumar and S. Surisetty, "Microsoft vs. Apple: Resilience against Distributed Denial-of-Service Attacks," in *IEEE Security & Privacy*, vol. 10, no. 2, pp. 60-64, March-April 2012.
- [11] S. Kumar, "PING Attack – How Bad Is It?" *Computers & Security Journal*, Vol.25, July 2006.

- [12] Junior, Rodolfo Baez, and Sanjeev Kumar. "Apple's Lion vs Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks." *Journal of Information Security* 5.03: 123. 2014.
- [13] Purcell, Aaron. "3 Key Ideas to Help Drive Compliance in the Cloud." IBM Corp.'s *Cloud Computing News.*, 15 Jan. 2018.
- [14] M. Feily, A. Shahrestani and S. Ramadass, "A Survey of Botnet and Botnet Detection," *2009 Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Glyfada, 2009*, pp. 268-273.
- [15] G. Vormayr, T. Zseby and J. Fabini, "Botnet Communication Patterns," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2768-2796, Fourth quarter 2017.
- [16] H. A. Herrera, W. R. Rivas and S. Kumar, "Evaluation of Internet Connectivity Under Distributed Denial of Service Attacks from Botnets of Varying Magnitudes," *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, 2018, pp. 123-126.
- [17] S. Liu, J. Gong, W. Yang and A. Jakalan, "A Survey of Botnet Size Measurement," *2011 Second International Conference on Networking and Distributed Computing*, Beijing, 2011, pp. 36-40.
- [18] Gunnam, Ganesh R. "Security Evaluation of Virtualized Computing Platforms", *The University of Texas Rio Grande Valley*, 2017.
- [19] Ballew, Scott. "Managing IP networks with Cisco routers". *O'Reilly Media, Inc.*, 1997.
- [20] Blank, Andrew G. "TCP/IP Jumpstart: Internet protocol basics". *John Wiley & Sons Inc.*, 2006.
- [21] Padole M, Kanani P, Raut L, Jhaveri D, Nagda M. "An insight into IP Addressing." *Oriental Journal of Computer Science & Technology*. 2017.
- [22] Kozierok, Charles M. *The TCP/IP-Guide: A Comprehensive, Illustrated Internet Protocols Reference*. San Francisco, CA: No Starch Press, 2009
- [23] Garg, Umang, et al. "MAC and logical addressing (A Review Study)". *International Journal of Engineering Research and Applications (IJERA)*. 2012.
- [24] D. Pao, C. Liu, A. Wu, L. Yeung and K. S. Chan, "Efficient hardware architecture for fast IP address lookup," *Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, New York, NY, USA, 2002, pp. 555-561 vol.2.
- [25] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy", *RFC 1519*

- [26] "IP Addressing and Subnetting for New Users." *Cisco Systems Inc.* 19 Oct. 2017.
- [27] "2019 Cyber Security Statistics Trends & Data." *PurpleSec.us.* 18 Nov. 2020.
- [28] "Top Cyberattacks of 2020 and How to Build Cyberresiliency." *Information Systems Audit and Control Association (ISACA).*
- [29] "The Evolution of Cybersecurity Threats During COVID-19 and What You Can Do About It." *U.S. Chamber of Commerce.* 03 Oct. 2020.
- [30] Kupreev, Oleg, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS Attacks in Q2 2020." *Kaspersky Lab's Securelist English.*
- [31] Hsu, Ken, Durgesh Sangvikar, Zhibin Zhang, and Chris Navarrete. "Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices." *Palo Alto Networks Inc.'s Unit42.* 30 June 2020.
- [32] Kupreev, Oleg, Ekaterina Badovskaya, Alexander Gutnikov, "DDoS Attacks in Q1 2020." *Kaspersky Lab's Securelist English.*
- [33] "2020 Mid-Year DDoS Attack Landscape Report." *NSFOCUS, Inc., a Global Network and Cyber Security Leader, Protects Enterprises and Carriers from Advanced Cyber Attacks.* 29 Oct. 2020.
- [34] Bannister, Adam. "DDoS Attacks More Numerous, Diverse, but Smaller in Q3 of 2020." *The Daily Swig / Cybersecurity News and Views.* Port Swigger Ltd., 20 Nov. 2020.
- [35] Imperva, Inc. "Imperva Research Labs Records Largest DDoS Attacks of the Year as COVID-19 Shutdowns Continue." *Apollo Global Management, LLC's GlobeNewswire News Room.,* 20 Aug. 2020.
- [36] "Microsoft Digital Defense Report". *Microsoft Corp.* Rep. Sept. 2020.
- [37] "Compare Windows 10 Business Editions." *Microsoft Corp.*
- [38] R. S. R. Gade, H. Vellalacheruvu and S. Kumar, "Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," *2010 Fourth International Conference on Digital Society, St. Maarten, 2010,* pp. 188-191.
- [39] R. R. Zebari, S. R. M. Zeebaree and K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers," *2018 International Conference on Advanced Science and Engineering (ICOASE), Duhok, 2018,* pp. 156-161

- [40] S. Surisetty and S. Kumar, "Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks?," *2010 Fifth International Conference on Internet Monitoring and Protection, Barcelona*, 2010, pp. 60-64.
- [41] Kumar, S., & Gomez, O. Denial of Service due to direct and Indirect ARP storm attacks in LAN environment. *Journal of Information Security*, 1(02), 88. 2010.
- [42] Perez, M., & Kumar, S. A Quick Survey on Cloud Computing and Associated Security, Mobility and IoT Issues. *Journal of Computer and Communications*, 5(12), 80-95. 2017.
- [43] S. Kumar, M. Azad, O. Gomez and R. Valdez, "Can Microsoft's Service Pack2 (SP2) Security Software Prevent SMURF Attacks?," *Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06), Guadelope, French Caribbean*, 2006, pp. 89-89.
- [44] Kumar, S., et al. "Survivability evaluation of wireless sensor network under DDoS attack." *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*. IEEE, 2006.
- [45] Koushicaa Sundar and Sanjeev Kumar, "Blue Screen of Death observed for the Microsoft's Server 2012 R2 under Denial of Service Attacks," *Journal of Information Security*, vol. 7, pp. 225-231, July 2016.
- [46] Surisetty, Sirisha, and Sanjeev Kumar. "Is McAfee securitycenter/firewall software providing complete security for your computer?." *2010 Fourth International Conference on Digital Society*. IEEE, 2010.
- [47] Kumar, Sanjeev, and Raja Sekhar Reddy Gade. "Evaluation of Microsoft Windows Servers 2008 & 2003 against Cyber Attacks." *Journal of Information Security* 6.02 (2015): 155.
- [48] Einar Petana and S. Kumar, "TCP SYN-based DDoS attack on EKG signals monitored via a wireless sensor network," *Wiley Journal of Security and Communication Networks*, Sept. 2011
- [49] Townsend, Kevin. "Large-scale DDoS Attack Abuses HTML's Hyperlink Audit Ping Facility." *Wired Business Media Inc.'s SecurityWeek*. Apr. 2019.
- [50] "Internet Protocol - DARPA Internet Program Protocol Specification," RFC 791, *USC/Information Sciences Institute*, September 1981.
- [51] Postel, J., "Internet Control Message Protocol - DARPA Internet Program Protocol Specification," *RFC 792, USC/Information Sciences Institute*, September 1981.
- [52] "Transmission Control Protocol - DARPA Internet Program Protocol Specification," RFC 793, *USC/Information Sciences Institute*, September 1981.

- [53] Postel, J., "User Datagram Protocol - DARPA Internet Program Protocol Specification," *RFC 768, USC/Information Sciences Institute*, August 1980.
- [54] Specht, Stephen M., and Ruby B. Lee. "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures." *International Conference on Parallel and Distributed Computing Systems (ISCA PDCS)*, 2004, pp. 543–550.
- [55] "Network DoS Attacks." *TechLibrary - Juniper Networks, Inc.*
- [56] Santos, Allan B. "Running the Latest Operating System on Your Pc Is Essential. In This Guide, We Compare Different Editions of Windows 10." *SoftwareKeep; Microsoft Corp. Certified Gold Partner*.
- [57] Trent, Rod "Differences between Windows 8.1, Windows 8.1 Pro, and Windows 8.1 Enterprise." *Informa USA, Inc. 's IT Pro Today*. 17 Oct. 2013
- [58] Khanse, Anand. "Windows 8.1 Editions Comparison Chart." *Khanse Webmedia Pvt Ltd.'s The Windows Club*. 2 Oct. 2013.
- [59] Leonhard, Woody. "The 5 Versions of Windows 8.1." *John Wiley & Sons Inc. 's Dummies*. Web. 09 Dec. 2020.
- [60] "Windows 10 vs Windows 8.1 vs Windows 7 - Microsoft OS Head-to-head." *Dennis Publishing Ltd. 's IT Pro*. 18 Apr. 2018.
- [61] Parrish, Kevin. "Windows 10 Vs. Windows 8.1: The Major Differences." *Future US Inc. 's Pcgamer.*, 29 May 2015.
- [62] Harris, Jaime "Windows 8.1 vs Windows 10: How Do They Match Up?" *British Telecom (BT) Group plc*.
- [63] Shiflett, Chris. "HTTP Transactions: An Introduction." *Pearson Education Plc. 's InformIT*. 27 Jun. 2003.
- [64] Heurung, Al. "CPU Usage Vs. Processor Time." *Leaf Group Ltd.'s It Still Works*. 10 Jan. 2019.
- [65] "What Is CPU Time? - Definition from Techopedia." *Techopedia Inc*. Web. 09 Dec. 2020.
- [66] "Intel® Core™ I5-2400S Processor (6M Cache, up to 3.30 GHz) Product Specifications." *Intel Corp*.
- [67] "Disk Utilization." *Microsoft Corp. 's Microsoft Docs*.



[68] Ghandeharizadeh, S., James Stone, and Roger Zimmermann. “Techniques to quantify SCSI-2 disk subsystem specifications for multimedia”. *Technical Report USC-CS-TR95-610*, USC, 1995.

[69] “Ntoskrnl.exe Windows Process - What Is It?” *Microsoft Corp.*

## BIOGRAPHICAL SKETCH

Christina Navarro was born during the mid-90s in McAllen, Texas. She graduated from the University of Texas – Rio Grande Valley with both Bachelor and Master of Science degrees in electrical engineering during December 2016 and December 2020, respectfully. Her personal email address is:

stina3@live.com

Achievements during her graduate career include:

- Navarro, Christina Y. and Kumar, S. “Security Evaluation of Apple’s iMac under Cyber Flood Attack” Accepted Poster Presentation for 2nd International Conference on Data Intelligence and Security (ICDIS), 2019. South Padre Island, Texas.
- Navarro, Christina Y. and Herrera, H. “Performance Under Impact of a Large-Scale Botnet Utilizing Smurf Attack on Windows 2012 R2” Accepted Poster Presentation for Hispanic Engineering, Science, and Technology Hispanic Engineering Science and Technology (HESTEC), 2018. Edinburg, Texas.
- Outstanding Graduate Student Award, HESTEC National Engineers Week, 2018. Edinburg, Texas.