A Project Report

on

Penetration Testing & Cyber Forensics

carried out as part of the course (CS 1634) Submitted by

Prerit Pathak
169105131

Rhythm Balooni
169105144

6th Semester B.tech CSE

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

In

Computer Science Engineering

MANIPAL UNIVERSITY
JAIPUR

Department of Computer Science & Engineering
School of Computing and IT,
Manipal University Jaipur,

April, 2019

Abstract

Crimes in this digital world are of different types and the one among them is Cyber-crime. As everything is digitized, there is a rapid increase in use of internet and at the same time more number of cyber-crimes happens that raised by the attackers. Some of the cyber-attacks are hacking, banking frauds, and email spamming etc. In order to investigate these fraudulent activities, the investigation agencies (enforcement law) should make use of technology which is a crucial part.

Digital forensic investigation is a branch of cyber forensics in which scientific methods and tools are used, that allows the prevention and analysis of digital evidence, that to be produced in a court of law. In this project we aim to perform some famous attacks including but not limited to DOS, DNS Spoofing, Phishing Attack etc. and research about cyber forensics. The characteristics of these attacks have been identified and described.

In this project, we aim to cover some major cyber attacks which still make Fortune 500 business lose billions of dollars in revenue each year. We go in depth in how these our performed & if and how they can be prevented. For the phishing attack, we aim to build a responsive, high performance web page which looks identical to our ION login page. We also perform a research on Windows Registry for the Cyber Forensics part of our project.

Table of contents

List of figures

1. Introduction

Over the years, the internet has expanded to enormous proportions, with increasing numbers of hosts and availability of high-speed connections. This expansion has also lead to an increase in the number of attacks on hosts. The Domain Name System (DNS) is one of the important parts of the internet. Without it most people would not be able to connect to their favorite website. It is not hard to imagine that DNS servers have also been the targets of attacks. These attacks are possible because of exploits in the DNS protocol or bugs in the DNS software.

There is also a group of attacks that overload a host with packets taking up massive amount of bandwidth and processing power in the hope of making the DNS server unavailable for genuine users. These attacks are called Denial of Service (DoS) attacks. The reasons for these attacks differ: for example a DNS cache poisoning attack is used to get control over a domain, while DoS attacks just want to disrupt normal service.

Although system administrators are continuously adding new lines of defense to protect their infrastructure, the new generation of attackers is continuously trying new approaches to find ways to circumvent these defenses. Recently there have been reports of domain hijacks of several Internet Corporation for Assigned Names and Numbers (ICANN) addresses. This implies that if a well maintained organization like ICANN can be victim of a domain hijack, then other organizations can also be a victim to the same.

1.1 Scope of the work

In today's digital era, one of the biggest threats comes from cyber criminals. Hackers were not taken seriously until a few years back. Recently, some big names in the Indian industry had to pay hefty sums of money to hackers to keep confidential information from being disclosed to the government. According to surveys conducted by cyber security firms in the country, Indian firms lost more than $4 billion in 2013 alone because of hackers.

With more and more companies entering the e-commerce ecosystem and adopting new technologies like cloud computing, the threat from imminent security breaches is clearly demanding the need for efficient information security systems. The rising threat from cyber-attacks has exposed the severe shortage of talent in this sector.

People these days are extensively inclined towards open networks like internet where business transactions, commercial activities and government services have become very frequent. This

has further resulted into robust development and evolution of information security challenges and cyber threats. Furthermore, the diffusion of IoT (Internet of Things) paradigms, particularly in industrial sectors are anticipated to generate a new wave of misconducts including cyber-attacks jeopardizing an individual's personal security and industrial espionage. The challenges in the digital forensics are further intensified by the leveraging usage of anti-forensics in malware, and cyber threat. However, the law-makers and digital forensics experts are constantly putting efforts to enhance their skills and abilities to dig out artifacts, and digital activities that are often hidden in massive database.

1.2 Motivation

Cyber security is of utmost importance in today's world. With data increasing at enormous speeds by the second, the need to secure it is dire. The fascinating world of hacking is not always done as the attacker with bad intentions, it is sometimes done with the intention of securing a vulnerable system. We can do this by performing attacks knowingly and then figuring out the changes in the victim's system and then figuring out the measures which can be taken to avoid these attacks in the future. Cyber security is the need of the hour because even a really small attack can lead to potential data loss and loss of customers which in turn results in loss of business along the lines of millions of dollars.

The pace at which digitalization is growing the world is anticipated to thrive for highly skilled professionals that can efficiently address and catapult the demand for digital forensics. To suffice the demand for awareness and understanding of digital forensics the government across the globe are organizing programs that support education of digital forensics. For instance, the University of Illinois at Urbana has taken an initiative to train its students on digital forensics and is anticipated to contribute to the increasing demand for skilled professionals in this field. Apart from this, Malaysia also has been promoting the readiness towards digital forensics and incorporates dedicated institute for digital forensics.

2. Requirement Analysis

2.1 Functional Requirements

System functional requirement describes activities and services that must provide.

1. Perform DOS Attack, DNS Spoofing, SSH Brute Force & Birthday Attack in a sophisticated manner
2. Store the username-password combinations in a text file after the user enters his credentials and clicks on the login button
3. The I-ON login page should look and work exactly like the actual login page so that the phishing attack is performed with no complications

2.2 Non Functional Requirements

Nonfunctional Requirements are characteristics or attributes of the system that can judge its operation. The following points clarify them:

1. **Speed & Responsiveness:** The ION login page should be fast and responsive otherwise the end user might notice that something is off and hence he won't try and login to the page. This will result in a failure of the phishing attack we were intending to perform.
2. **Usability:** The page should be usable by anyone with a basic knowledge of internet and computers
3. **Reachability:** For DOS, DNS Spoofing, Birthday attack & SSH Brute Forcing, the victim host should be reachable by our attacking machine. Preferably on the same network. We can check this by sending ICMPv4 packets using the PING command.
4. **Modifiability:** The system should be easy to modify.

2.3 Software Methodologies

Successful projects are managed well. To manage a project efficiently, we team must examine many software development methodologies to choose the one that will work best for the project at hand. A proper software methodology was followed by us throughout in the making of this project. Here's an overview of the software development methodologies that were used in building this project.

1. **Agile Development Methodology -** Agile software development is an approach to software development under which requirements and solutions evolve through the collaborative effort of self-organizing and cross-functional teams and their customer(s)/end user(s). The Agile methodology begins with clients describing how the end product will be used and what problem it will solve.

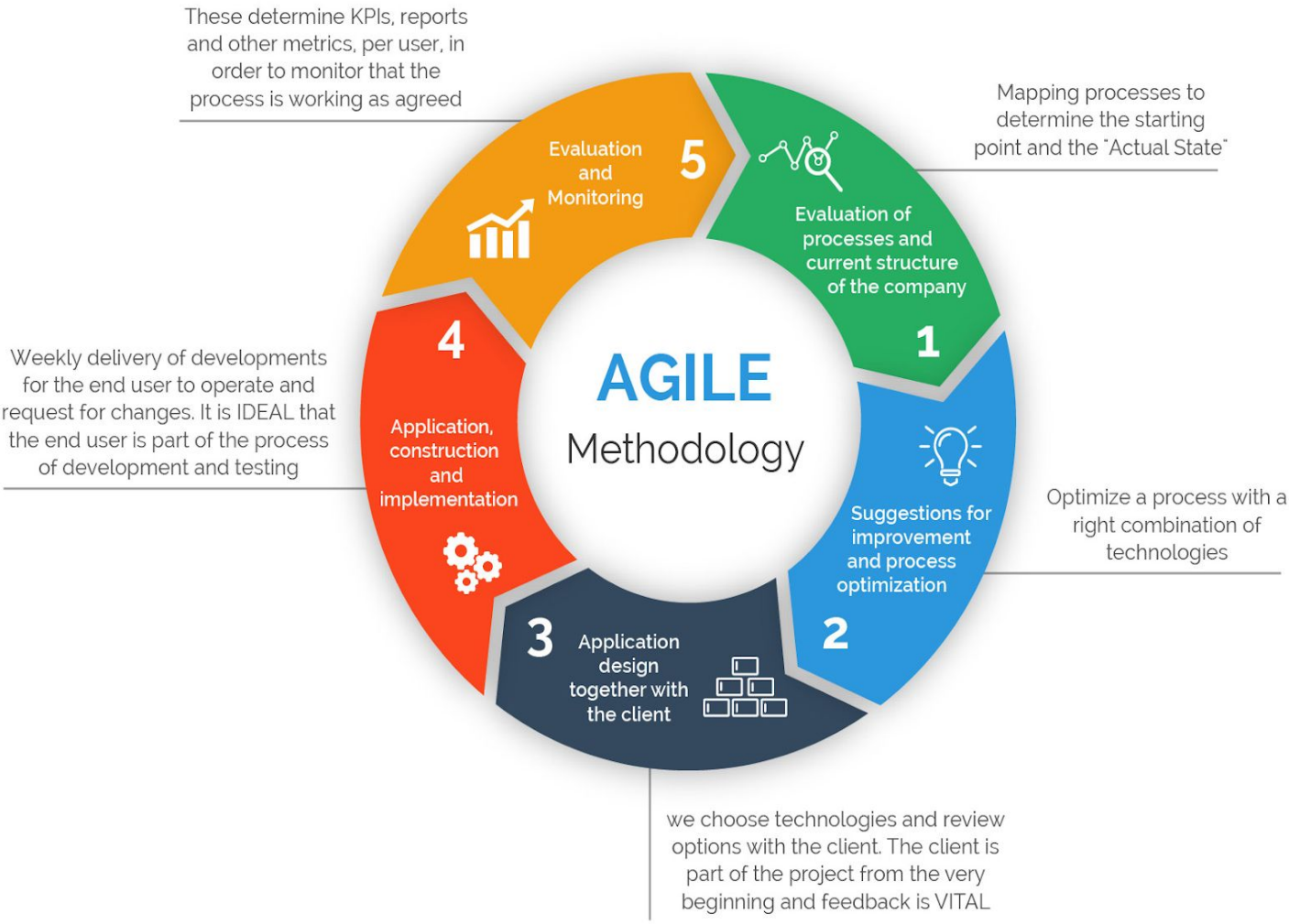

Fig 2.3.1 Agile Methodology

2. **Scrum Methodology:** Scrum is a framework that helps teams work together. Much like a rugby team (where it gets its name) training for the big game, Scrum encourages teams to learn through experiences, self-organize while working on a problem, and reflect on their wins and losses to continuously improve.

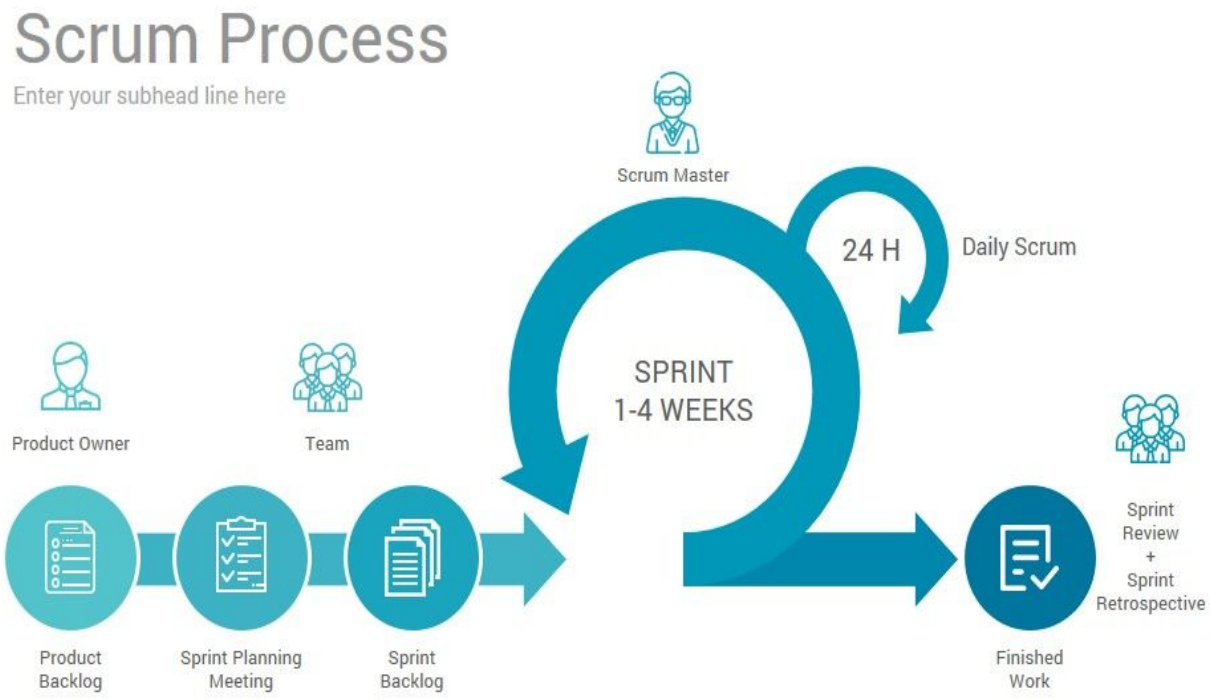

Fig 2.3.2 Scrum process

3. Literature Review

For the research part of our project, we studied two research papers on Cyber Forensics. This process helped us in a clear understanding of how cyber forensics works and why it is the need of the hour. The research papers we referred to are mentioned below:

1. **Forensics Analysis of Windows Registry** (Published by Lih Wern Wong)
2. **Windows Registry and Hiding Suspects' Secret in Registry (**Published by Youngsoo Kim, Dowon Hong)

3.1 Research Papers

3.1.1 Forensics Analysis of Windows Registry

Published by Lih Wern Wong

School of Computer and Information Science, Edith Cowan University

Windows registry contains lots of information that are of potential evidential value or helpful in aiding forensic examiners on other aspects of forensic analysis. This paper discusses the basics of Windows XP registry and its structure, data hiding techniques in registry, and analysis on potential Windows XP registry entries that are of forensic values.

Windows 9x/ME, Windows CE, Windows NT/2000/XP/2003 store configuration data in registry. It is a central repository for configuration data that is stored in a hierarchical manner. System, users, applications and hardware in Windows make use of the registry to store their configuration and it is constantly accessed for reference during their operation. The registry is introduced to replace most text-based configuration files used in Windows 3.x and MS-DOS, such as .ini files, autoexec.bat and config.sys. For instance, windows registry contains information on user accounts, typed URLs, network shared, and Run command history. Aspects discussed in this paper are based solely on Windows XP (Service Pack 2) registry.

3.1.2. Windows Registry and Hiding Suspects' Secret in Registry

Published by Youngsoo Kim, Dowon Hong

Electronics & Telecommunications Research Institute (ETRI)/Convergence Security Group

Windows registry, a central repository for configuration data, should be investigated for obtaining forensic evidences, since it contains lots of information that are of potential evidential value. Using some forensic tools, forensic examiners can investigate values of windows registry and get information can be forensic evidences. However, since windows registry contains huge amount of values and these values can be modified by users, suspect can hide his secret like password in registry values. In this paper, we discuss the basics of Windows XP registry and extract some registry entries related to forensic analysis.

Windows registry can be an excellent source for potential evidential data, since the vast amount of information, such as user accounts, typed URLs, network shared, and run command history, is stored in it. Using some forensic tools, forensic examiners can investigate values of windows registry and get information can be forensic evidences. However, since windows registry contains huge amount of values and these values can be modified by users, suspect can hide his secret like password in registry values.

3.2 Research Objective

Identifying various loopholes and any evidence of the attack left in the computer & studying in-depth about the Windows Registry and how it helps us to retrace cyber attacks.

3.3 Research Outcome

The best source for potential evidential data is the Windows Registry. Knowing the type of information that could possible exist in registry and location to it gives forensic examiner the edge in the forensic analysis process. The investigator will get a better picture of the whole case. This paper illustrates some of techniques to hides data in registry and registry keys of evidential value. The fact that Microsoft and other organizations treat the registry settings as in-house information without providing sufficient and comprehensive documentation about the registry keys used causes registry analysis difficult, which undermines the resourcefulness of registry. Thus, there is a need to unveil and publish evidentiary registry keys to assist forensic investigation on Windows system.

4. Work Done

4.1 Development Environment

The development environment is the set of processes and programming tools used to create the program or software product. Here we've enlisted all the tools and processes used to build this project.

4.1.1 Phishing Attack:

The frontend of the ION login page was built using HTML, CSS, Javascript & jQuery. The backend was built using PHP.

4.1.2 Cyber Attacks:

We've performed all the cyber attacks using virtual machines so that we don't harm our main systems in the process. For this, we used the Oracle VirtualBox software. The attacking OS used was Kali Linux, a popular OS for penetration testing and the victim OS was Microsoft Windows7.

Tools Used:

- DOS Syn Flood: Nmap for network scanning, Metasploit framework for performing the attack
- DNS Spoofing: Ettercap
- SSH Brute Forcing: Hydra

4.1.3 Cyber Forensics:

The research is based on Windows XP/Vista/7. We use the Windows Registry in the process of tracing the cyber crimes and also making sure that we look out for all evidences that the attacker might have had left in the computer

4.2 Results and discussion:

1. **DOS Attack:**

   We are implementing DOS attack using SYN flood attack. In a SYN flood, the attacker sends a high volume of SYN packets to the server causing the server to send a reply (SYN-ACK) and leave its ports half-open, awaiting for a reply from a host that doesn't exist. In this state, the target struggles to handle traffic which in turn will increase CPU usage and memory consumption ultimately leading to the exhaustion of its resources (CPU and RAM). At this point the server will no longer be able to serve legitimate client requests and ultimately lead to a Denial-of-Service.

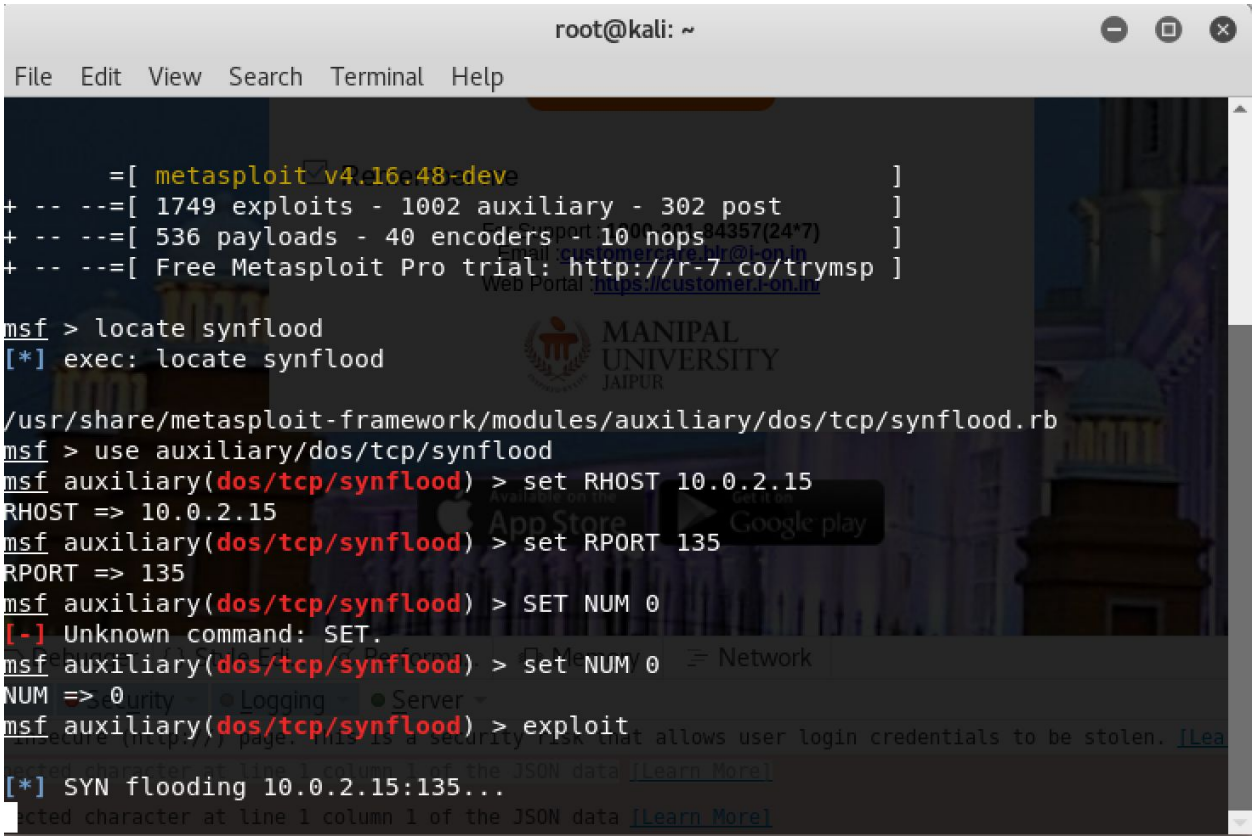

Fig 4.2.1 performing SYN flood attack using Metaspoilt Framework

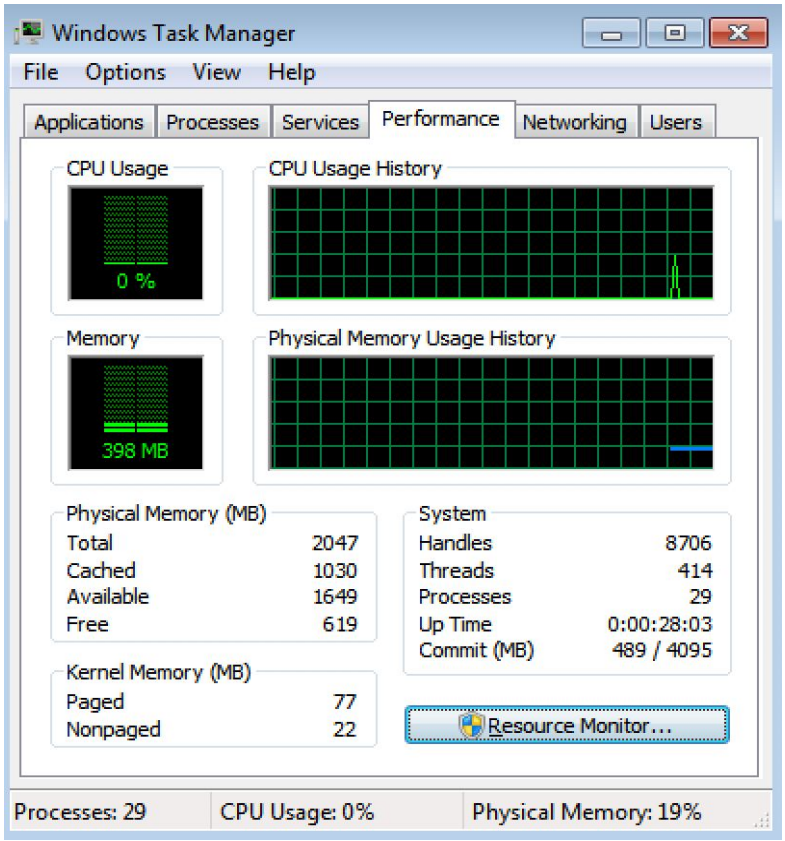

Fig 4.2.2 CPU usage status before attack

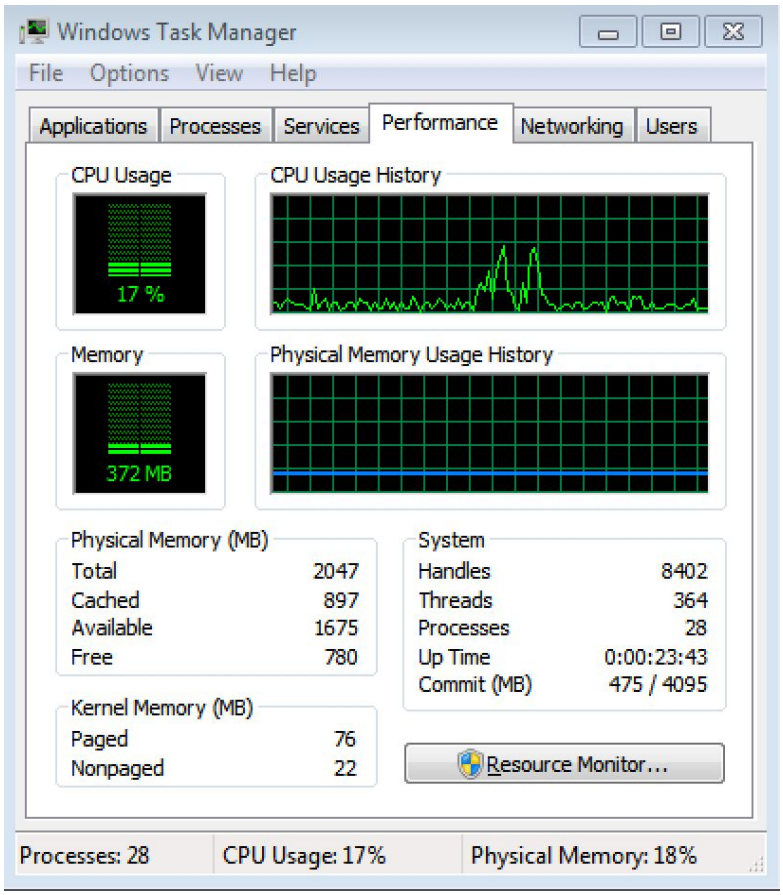

Fig 4.2.3 CPU usage status after attack

2. DNS Spoofing:

DNS Spoofing (sometimes referred to as DNS Cache Poisoning) is an attack whereby a host with no authority is directing a Domain Name Server (DNS) and all of its requests. This basically means that an attacker could redirect all DNS requests, and thus all traffic, to his (or her) machine, manipulating it in a malicious way and possibly stealing data that passes across. We have performed the ARP poisoning using the ettercap tool of Kali Linux. There are many plugins which come by default with EtterCap. Once such plugin is called as DNSSpoof. We have used that plugin to test the DNS spoofing.

This is a type of MITM (Man In The Middle) attack, where we, the attacker, can get in between the victim and the network. In reality, we are actually making the victim host use our custom DNS config file instead of their own. In this file, we can map any particular domain name/IP address to our own IP address. These are the results after performing DNS Spoofing:

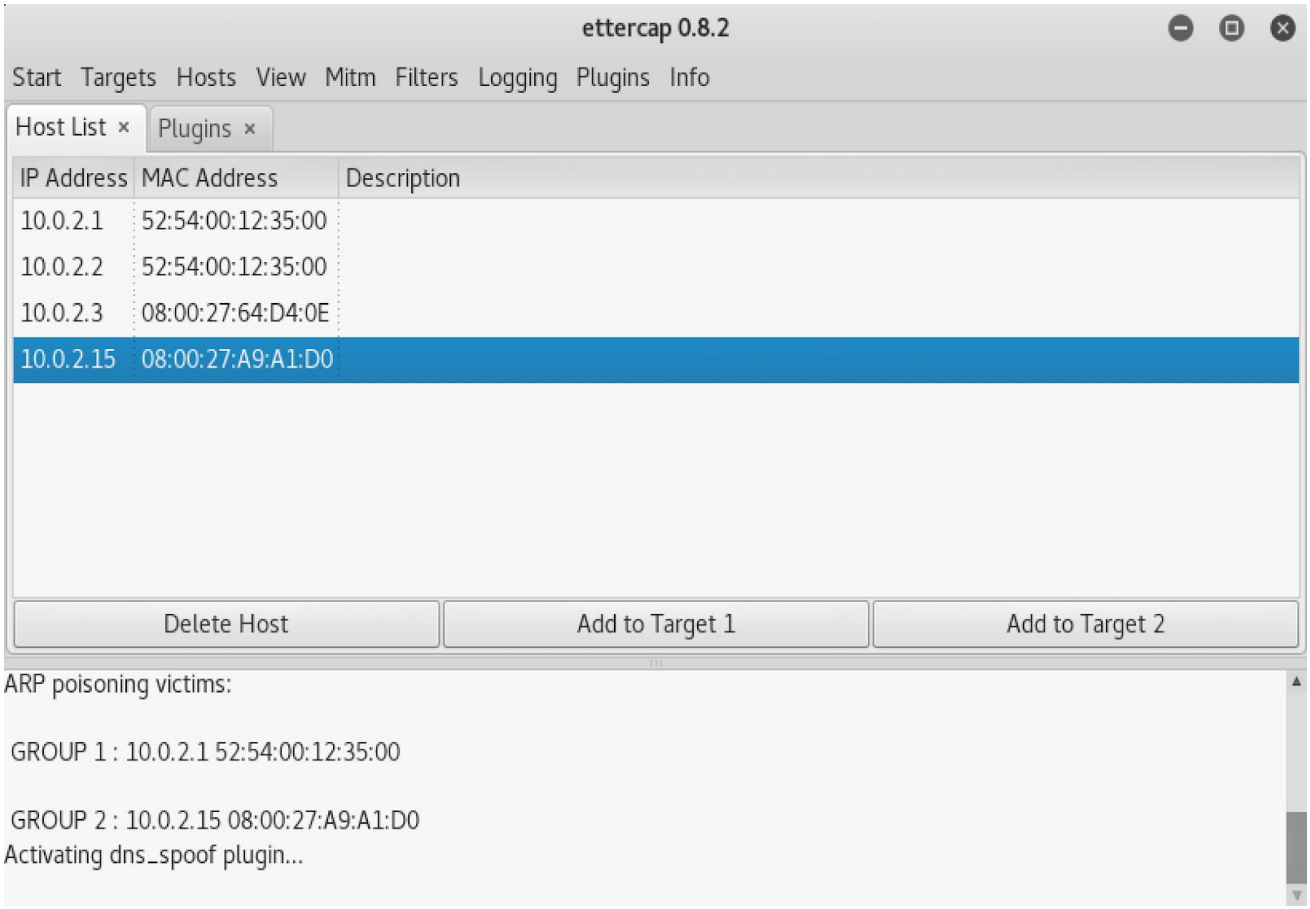

Fig 4.2.4 The victim IP and gateway added as targets for ARP poisoning

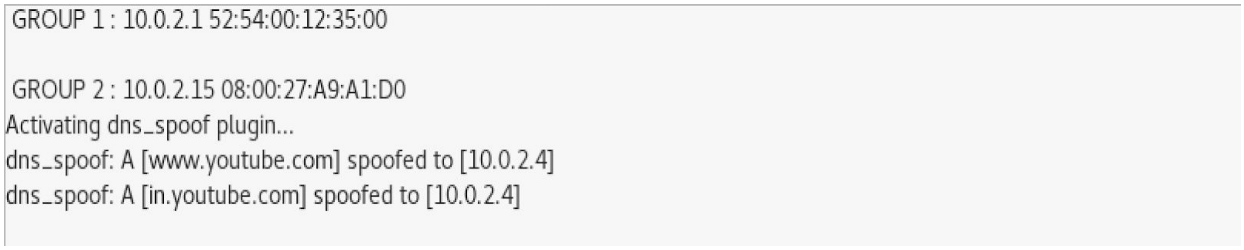

Fig 4.2.5 Results after successful spoofing

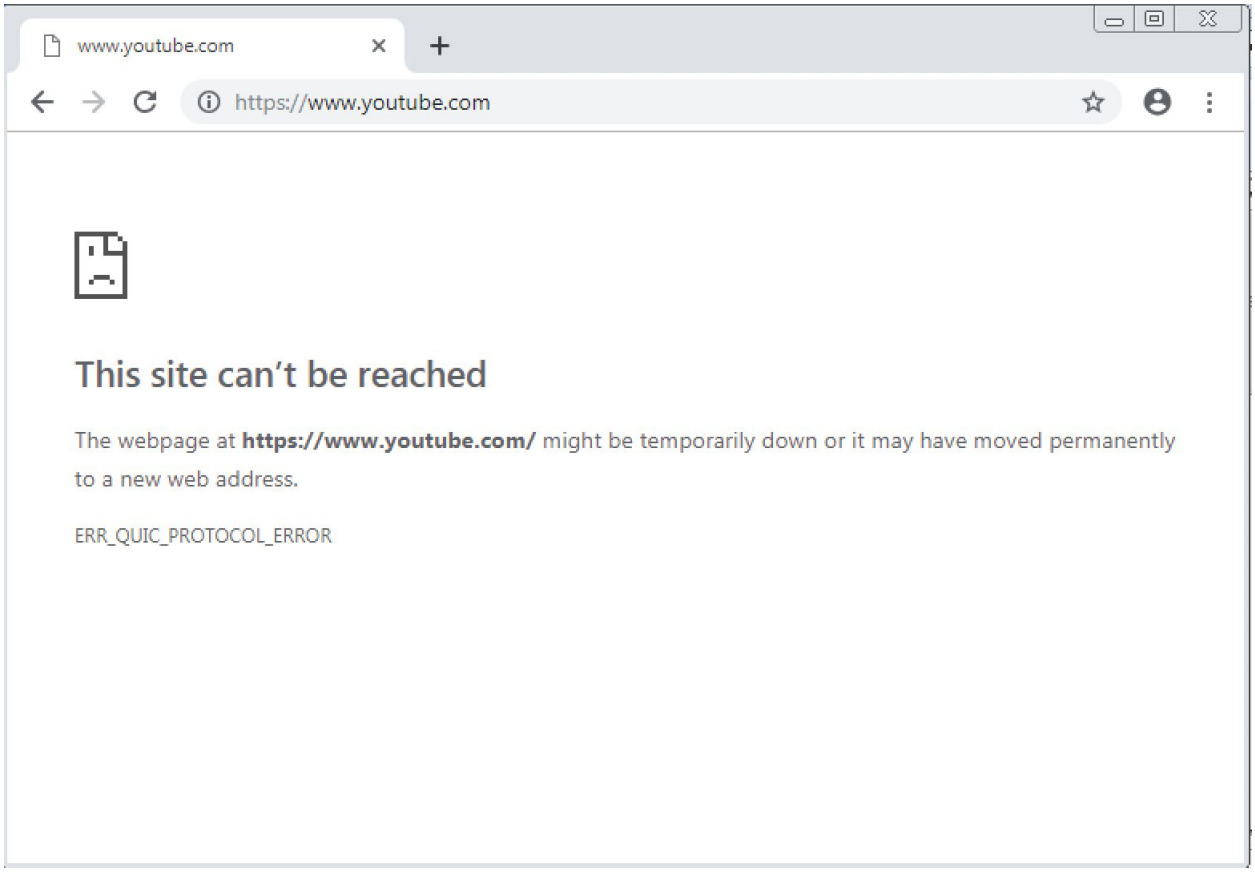

Fig 4.2.6 Case 1: Behaviour of Google Chrome after spoofing

We encounter this behaviour due to a default setting in the Google Chrome browser, according to which HTTP Strict Transport Security is turned on. HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections and never via the insecure HTTP protocol.

On the other hand, the Internet Explorer browser is fairly old and it doesn't have this feature. So in conclusion, we can either redirect the user to our page or stop the services entirely for that webpage.

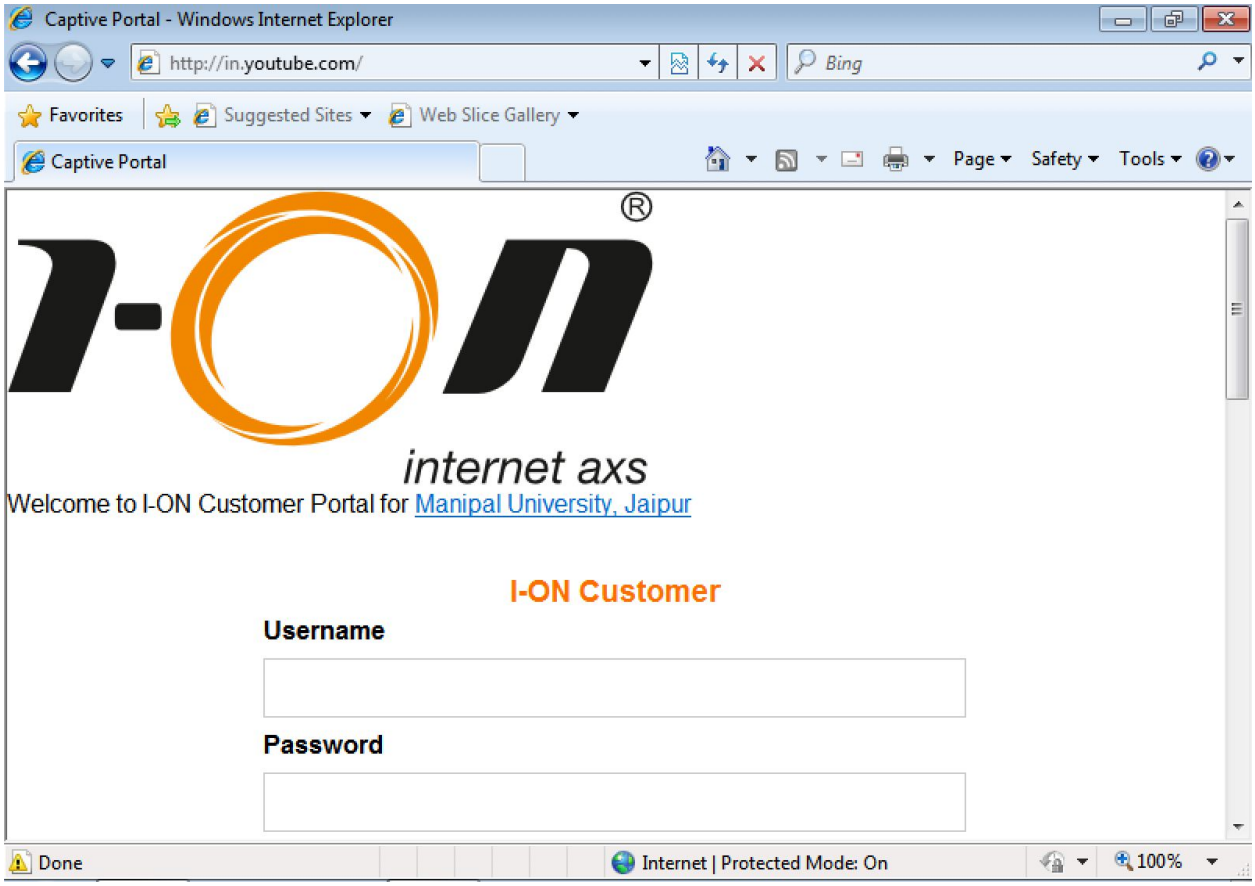

Fig 4.2.7 Case 2: Phishing site opens after DNS Spoofing

3. SSH Brute force attack:

Hydra is a popular tool for launching brute force attacks on login credentials. Hydra has options for attacking logins on a variety of different protocols. SSH is present on any Linux or Unix server and is usually the primary way admins use to access and manage their systems. Brute force attacks work by testing every possible combination that could be used as the password by the user and then testing it to see if it is the correct password. To see if the password is correct or not it check for any errors in the response from the server.

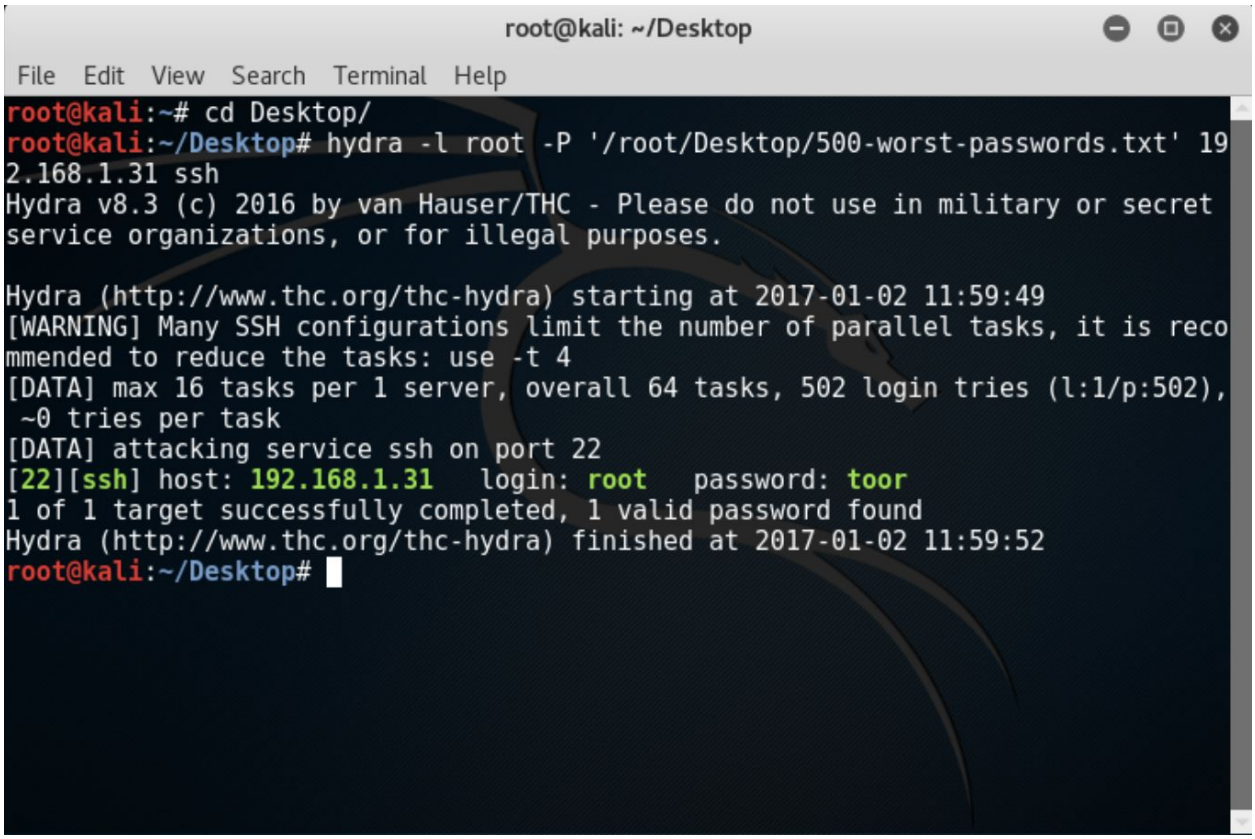

Fig 4.2.8 Password successfully cracked using hydra

Prevention:

1. Change the default port number: Usually SSH runs on port 22 which is open. A good practice is to change this by editing the config file located at /etc/ssh/sshd_configIn.
2. Use Key Value pairs: SSH keys are resilient to such attacks and virtually impossible to decrypt. An SSH key pair consists of two long series of characters: a private key which is kept secret, and a public key which can be safely shared. Their purpose is similar to passwords, and they allow you to automatically establish an SSH session without the need to type in a password.
3. Disable Password login: If you start using SSH keys, you can stop using password authentication. Edit the file located at vi /etc/ssh/sshd_config. Change PasswordAuthentication to PasswordAuthentication_No.

4. **Birthday attack:**

Birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes). This attack can be used abuse communication between two or more parties.

Birthday attacks are based on a unique problem with hashing algorithms based on a concept called the Birthday Paradox. This puzzle is based on the fact that in a room of 183 people, there would be a 50 percent chance of one of them sharing your birthday. However, if you wanted a 50 percent chance of finding any two people who had matching birthdays, you would surprisingly only need 23 people in the room. For hashing functions, this means that it is much easier to find any two matches if you don't care which two they are. It is possible to precompute hashes for a given password length to determine if any collisions occur.

The DES ciphers (and triple-DES) only have a 64-bit block size. This enables an attacker to run JavaScript in a browser and send large amounts of traffic during the same TLS connection, creating a collision. With this collision, the attacker is able to retrieve information from a session cookie. The triple-DES cipher is supported by a vast majority of HTTPS servers and all major web browsers—around 600 of the most visited websites. Fortunately, most browsers opt to use AES rather than triple-DES when making an HTTPS connection.

Prevention:

- Disable any triple-DES cipher on servers that still support it
- Upgrade old servers that do not support stronger ciphers than DES or RC4

4.3 Individual contribution of project members:

1. **Cyber attacks:**

Out of the four attacks that have been implemented by us, each person has performed two.

- ➔ DOS attack and SSH Brute force attack have been researched, implemented, performed and compiled by Prerit.
- ➔ DNS spoofing and Birthday attack have been researched, implemented, performed and compiled by Rhythm.

- ❖ **Phishing attack:** A high performance & responsive fraudulent website was created for this attack wherein we divided the work of web development into front end and back end.
- ➔ Prerit worked on the jQuery, PHP Fetch API and Javascript part of the website. This included making sure the the error code sent in the promise was 200. Also, ensuring that the data was being sent in a json format and it was being perfectly parsed.
- ➔ Rhythm worked on HTML, PHP and Javascript part of the website. This included making sure the page looks like the ION page and appending the username password combinations to a .txt file located in our root directory.

2. Cyber forensics:

Cyber forensics is the research part of our project. We read various research papers and searched the web to do this task. We learned about the Windows Registry structure and how it can help us to trace evidence that might have been left by the cyber attacker. We demonstrate our findings below:

By clicking Start\Run and typing 'legedit' on Windows, we can see Windows registry logical view from Register Editor, Windows default register editor. Each folder in the left key pane is a registry key and the right panes show the key's value. Subkeys are used to show the relationship between a key and the keys nested below it. Windows uses symbolic link to link a key to a different path which allows the same key and its values to appear at two different paths. There are 5 root keys in Windows registry :

Name	Abbreviation
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC

Table 4.3.1 Registry keys

Registry Editor only shows the logical structure of the registry. Physically, registry is not stored in a single file in the hard drive. Windows stores registry in a few separated binary files called hives (Microsoft, 2005a). For each hives file, Windows creates additional supporting files that contain backup copy of the respective hives to restore the hives during failed system boot. Only HKLM and HKU has corresponding hives (since the rest are symbolic links). However, none of 5 root keys are directly associated to a hive file. Table 1 shows registry path and their corresponding hives on disk. All hives in HKLM are stored in %SYSTEMROOT%\System32\config\(%SYSTEMROOT% usually refers to C: \WINDOWS). HKLM\HARDWARE is a dynamic hive that is created each time the system boots and it is created and managed entirely in memory. HKU\.DEFAULT hive file correspond to %SYSTEMROOT% \System32 \config\default. HKU\SID hive file is stored in user home directory, which is %USERPROFILE% \NTUSER.DAT, while HKU\SID_CLASSES hive file correspond to %USERPROFILE%\Local Settings \Application Data\Microsoft\Windows\UsrClass.dat.

5. Conclusion

After successfully completing our research cum application based project on penetration testing and cyber forensics, we conclude that there are many attacks which are very old and still a majority of computers are vulnerable to them. A major example is the SSH Brute Force attack. We also understand how cyber security scientists take use of the Windows Registry to look for traces after an attack has occured. Apart from this, the user should be careful and notice for fishy attributes of a webpage so he doesn’t fall in the trap of the phishing attack.

6. References

- Carvey, H. (2001, August 15). NT/2K Incident Response Tools. Retrieved September 26, 2005, from http://www.securityfocus.com/infocus/1294
- Carvey, H. (2004).Windows Forensics and Incident Recovery. United State of America: Addison Wesley. Carvey, H. (2005a). Windows Forensics and Incident Recovery ñ Tools. Retrieved September 29, 2005, from http://www.windows-ir.com/tools.html
- https://www.null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699/
- Javed, M. and Paxson, V. Detecting Stealthy, Distributed SSH Brute-Forcing from https://seclab.cs.ucsb.edu/media/uploads/papers/dist-ssh-det.ccs13.pdf