# Utilization Of Usbdriveby And Social-Engineer Toolkit (SET) For DNS Spoofing Attacks On Windows Operating Systems

**Jimmy, Ahmad Almaarif, Avon Budiono**

**Abstract:** Universal Serial Bus (USB) is one of the mechanisms used by many people with practical plug and play function, making data transfer fast and easy compared to other hardware. Windows has a weakness that is easily exploited on the system. There is one method of attacking social engineering using USB, USBDriveby which can exploit loopholes in Windows for people to change the hosts file and do DNS spoofing by connecting USB to the target computer. The purpose of this study is to design and analyze USBDriveby on Windows. This study is also conducted to determine whether the DNS Spoofing attack on the target computer using USBDriveby can be done. The result is that DNS Spoofing testing using USBDriveby was successfully carried out on windows systems and websites that did not activate HTTP Strict Transport Security (HSTS).

**Index Terms**: USBDriveby, DNS Spoofing, Social Engineering, Operating System, USB-based Attack, HSTS.

## 1 INTRODUCTION

Universal Serial Bus (USB) is a mechanism that is currently used everywhere by enabling plug and play functionality, enabling fast and easy data transfer compared to other hardware. USB offers the flexibility needed by users that can be used for everyday needs. USB is also a mechanism for carrying out highly efficient exploits that are capable of sending, installing and running malware on the system [1]. Social Engineering is a technique of collecting data or important/confidential information from a person by using a human approach through the mechanism of social interaction by exploiting human weaknesses [2]. Social engineering attack concentrates on manipulating user as the weakest chain of computer network systems. Every person who has access to the system is a potential threat and potential victim for social engineering attack. Social Engineering can be used as a technique for attack that is very effective at people who have social relationships. In social life, people interact with one another like borrowing things from new people. A supporting example is that humans have USB as a personal necessity in sending files offline. It can be used for attacks via USB by launching attacks by embedding dangerous files in it, but the user does not realize that the USB is not safe so that the attacker can easily carry out attacks when the USB is connected by the user, and also there have been many warnings to not connect USB that is not their own so as not to be attacked by malicious files. Many people have been hit by USB attacks that can have a minor or fatal impact. An example of attacks using USB is by embedding DNS spoofing, and running programs to steal user data. DNS Spoofing can be conducted using USB and operating system as attack vector. Windows is the most widely used operating system [3]. Unfortunately, it still has security holes that need to be addressed. The weakness used in this study is the ease in adding, changing and deleting files on a computer even by people who are not owners. By using admin privileges in command prompt (CMD) of target computer, the attacker can change the hosts file on the target computer by using USB-based attack method [4]. This study discusses the USB-based attack using Arduino Microcontroller which will be transformed into a USBDriveby. USBDriveby is a device that can conducted DNS spoofing on the target computer via USB. Attack using DNS Spoofing method is a method of hacking that can be categorized as a Man in The Middle Attack (MITM) that can manipulate DNS packets exist in the DNS network itself by changing a domain address into a fake address. Therefore, the attacker can steal the data sent to a website [5]. By using this method, it is expected to know the impact of the attack by changing the hosts file resulting as DNS spoofing. USBDriveby was developed by a security and privacy researcher named Samy Kamkar. This research combined the use of USBDriveby and Social Engineer Toolkit (SET) as attack vector. Social Engineer Toolkit (SET) is used as a tool to manipulate victim to input credential data into fake website. The existence of this research is expected to find out the impact of the USBDriveby and Social Engineer Toolkit (SET) on Windows operating system.


- *Jimmy is an undergraduate student of Information System Program in Telkom University, Bandung, Indonesia. E-mail: jimmy@student.telkomuniversity.com*
- *Ahmad Almaarif is currently a lecturer at Information System Program in Telkom University, Bandung, Indonesia. E-mail: ahmadalmaarif@telkomuniversity.ac.id*
- *Avon Budiono is currently a lecturer at Information System Program in Telkom University, Bandung, Indonesia. E-mail: avonbudiono@telkomuniveristy.co.id*


## 2 LITERATURE REVIEW

### 2.1 DNS Spoofing

DNS spoofing is the term used when a DNS server receives and uses incorrect DNS information from a host that is not authorized to provide that information. DNS spoofing attack uses cache poisoning that put fake data on a server's cache. Spoofing attacks can cause serious security problems for DNS servers. By using spoofing attacks, user will be directed to a fake internet site or e-mail to an unauthorized server created by an attacker [6].

### 2.2 Social Engineering

Social Engineering is a 'theft' technique or the taking of confidential information from a person by using human approach through social interaction mechanism. In other words, social engineering is a technique of obtaining confidential data/information by exploiting human weaknesses. One tool often used to launch social engineering attacks is the Social-Engineer Toolkit. Social-Engineer Toolkit (SET) is a software specifically designed to carry out attacks on human's

psychology by using specific technology techniques.

## 3 DESIGN AND IMPLEMENTATION

Attack process requires certain hardware and software. Therefore, identification of device architecture is necessary, consisting of hardware and software. The specifications used can be seen in Fig 1.

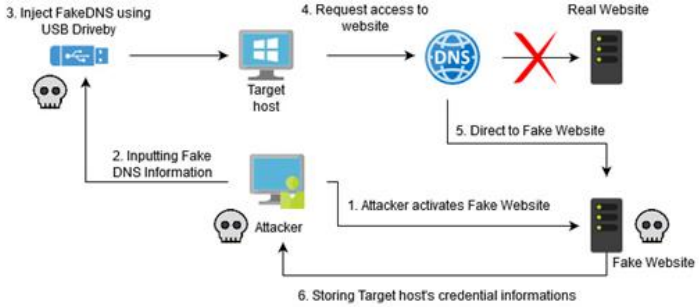


***Fig. 1**. Design of DNS Spoofing Attack using USBDriveby*

Fig. 1 shows an illustration of the attack carried out to do DNS spoofing on the target computer. The attack begins with the attacker activating the fake website which was the clone of the website to be spoofed. Fake DNS information script will be inputted into USBDriveby. Afterwards, The USBDriveby is injected to target computer via the USB port. USBDriveby will work automatically by acting as keyboard input on the target computer. USBDriveby's actions are based on lines of code entered into USBDriveby's itself. At the time victim access a website, the USBDriveby's script will direct the website request to a fake website which was cloned from real website using SET. While the victim input their credential data to fake website, the attacker will also have their data, including their username and password of that website.

### 3.1 Design of USBDriveby

Fig. 2 shows the attack mechanism carried out in this study. The attack was preceded by the attacker activating the fake website which would be used to trick the victims into entering their confidential information. Fake website created using SET. Then USBDriveby will access software command prompt (cmd) with administrator access rights. Then firewall will be deactivated and the pwn.bat file will be created on the victim's computer. This file will be saved in the AppData/Local/Temp folder. The next step, the script on USBDriveby will run the pwn.bat file which functions to change the DNS in the hosts file contained on the victim's computer. The final step is to do DNS Spoofing on the target by directing the target to a fake website that has been created previously.

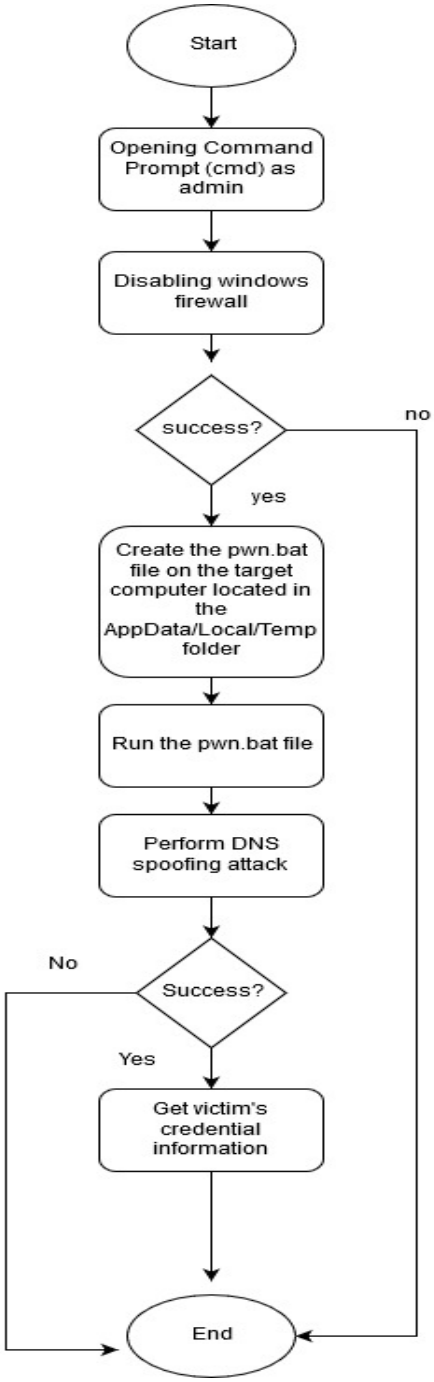


***Fig.2** Flowchart of Attack using USBDriveby*

The general step of the attack can be described as follows.

1) Activate Fake Website

Before attacking a target, the attacker must activate the fake website on web server first.

```
Root@kali:~#setoolkit
Set>1
Set>2
Set:Webattack>3
Set:Webattack>2
Set:Webattack>192.168.1.19
Set:Webattack>targetwebsiteURL
```

2) Disabling Firewall on windows

To attack a target, the attacker must first turn off the firewall on the target computer. It is necessary to carry out activities carried out by the attacker that cannot be read as suspicious.

```
C:\Users\Jims>NetSh Advfirewall set allprofiles state off
```

3) Creating a pwn.bat file on windows

```
Keyboard.println("cd AppData/Local/Temp");
Keyboard.println("echo.>pwn.bat");
Keyboard.println("notepad pwn.bat");
Keyboard.println("@ECHO OFF");
Keyboard.print("ECHO 192.168.1.13 gmail.com >>
C:\\WINDOWS\\SYSTEM32\\DRIVERS\\ETC\\HOSTS");
delay(1000);
Keyboard.press(KEY_LEFT_ALT);
Keyboard.press(KEY_F4);
Keyboard.releaseAll();
```

4) Running pwn.bat file

At this stage, the execution of pwn.bat that was made beforehand is carried out. The file is useful for adding DNS to the hosts file

```
Keyboard.print("pwn.bat");
typeKey(KEY_RETURN);
delay(500);
```

The detailed illustration of attack mechanism is illustrated on Fig.2. USBDriveby will run a script to open cmd with administrator privileges then activate the firewall on the windows operating system. If the firewall is no longer active, the pwn.bat file will be created. This file is useful for changing DNS settings on the victim's computer. In this file, some targeted websites will change their DNS settings. The disadvantage, not all websites can be attacked with this system. Previously, the attacker had cloned a website display that would be used as a medium of attack. Users who are not aware, will enter confidential information such as usernames and passwords on fake websites that are visited.

### 3.2 Testing Scenario

DNS Spoofing is an attack mechanism that is useful for falsifying the IP address of a domain from the original website that will be accessed by the target computer. The DNS Spoofing test was carried out on six websites in the category of social media websites, e-mail, electronic payments, and e-commerce websites. Tests carried out on computers with Windows operating systems by plugging USBDriveby on a computer system. Memory used in this computer is 8GB RAM. After USBDriveby is run, users will be asked to access some of the sites that have been determined. Previously the attacker had cloned and made fake websites for these sites. The website and its categories can be seen in Table 1

***TABLE 1***
*TARGET WEBSITES AND ITS CATEGORY*

| Website | Category |
|---|---|
| A | Social Media |
| B | Email service |
| C | Social Media |
| D | Electronic payment |
| E | e-commerce |
| F | e-commerce |

## IV. RESULT AND DISCUSSION

Testing is conducted by accessing certain site using victim's computer and USBDriveby. On some websites, the user's credential data is successfully obtained as shown in Fig. 3

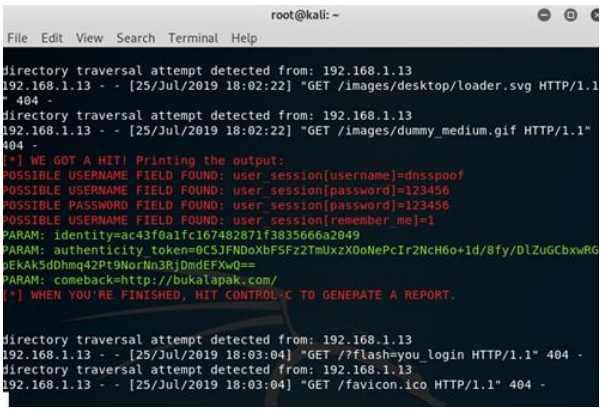


***Fig.3*** *Data obtained by from Fake Websites*

As indicated by Table 2, DNS Spoofing testing using SET and USBDriveby is not always successful. Some websites, especially e-commerce websites that do not use HTTP Strict Transport Security (HSTS), are not secure so they can be easily cloned. HSTS keeps the website protected from downgrade protocols. Most social engineering based website cloning applications still use HTTP on the cloned website so websites that already use HSTS cannot be easily cloned.

***TABLE 2***
*ATTACK RESULT*

| Website | Result | Analysis |
|---|---|---|
| A | unsuccessful | Because the Website is registered as HSTS on a Web browser so the web browser will automatically be forced to use HTTPS. As a result, the website can avoid indications of data theft by hackers. |
| B | unsuccessful | |
| C | unsuccessful | |
| D | unsuccessful | |
| E | Succeed | Because this website is not registered as HSTS on a web browser, so when the website is cloned with an http website, the web browser will not automatically force this website to use HTTPS |
| F | Succeed | |

From the test results it can be concluded that the attack website using Social-Engineer Toolkit with the credential harvest attack method, there are several websites successfully attacked and also some unsuccessful. That is because websites that cannot be successfully attacked use HTTP Strict Transport Security (HSTS) whose function is to force a site to always access the HTTPS protocol that can prevent Man-in-The-Middle attacks such as DNS Spoofing. For websites that are successfully attacked, the website is not registered as HSTS preload in a web browser. USBDriveby attacks by imitating the target computer keyboard. On USBDriveby there is a line of delay code that functions to set the time the system runs the attack steps. If the target device that is attacked responds longer than the delay that has been regulated, then it can result in the performance of an attack carried out by USBDriveby requires a long time and failure can also occur. USBDriveby uses the keyboard function found in the Arduino library. Therefore, the attack will fail if an interruption occurs, such as accidentally pressing certain keys on the keyboard. The attack will fail because USBDriveby does not have a loop to run the attack.

## 4 CONCLUSION

The DNS Spoofing attack using USBDriveby and the Social-Engineer Toolkit can have a major impact on users. If the attack is successful, the user's credential information is threatened and can be misused by the attacker. USB Flash drive devices have weaknesses that are often ignored by users. One threat is the use of USBDriveby to insert malicious scripts that can change users' DNS settings and direct users to fake, fraudulent websites. The way USBDriveby attacks work is done by using the keyboard on the target computer. USBDriveby provides command injection so the keyboard can run the command according to the line of code that has been prepared. USBDriveby has the disadvantage that interruptions can occur if when USBDriveby is run there are other keyboard activities that are run by authorized users. Another disadvantage of this attack is that if a website is targeted to use HSTS, then the attack cannot be carried out. This attack utilizes the Social-Engineer Toolkit that does the cloning. Unfortunately SET can only clone websites using the HTTP protocol so it cannot be done on websites that already use the HSTS protocol.

## REFERENCES

[1] K., Orrey, A Survey of USB Exploit Mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective. Kevin Orrey, MSc. 1–27, 2011.

[2] I., Richardus, Social Engineering E-Artikel Sistem Dan Teknologi Informasi Vol. 999., 2013.

[3] W3schools, OS Statistics, 2019, Accessed on June 28, 2019. [Online]. Available: https://www.w3schools.com/browsers/browsers_os.asp

[4] S., Vouteva, Feasibility and Deployment of Bad USB, 2015.

[5] [5] K., Samy, USBDriveby: exploiting USB in style, 2014, Accessed on Mei 20, 2019. [Online]. Available: https://samy.pl/usbdriveby/

[6] [6] S.P., Singh, & A.R., Maini, Spoofing Attacks of Domain Name System Internet, 2011.