**Table of Content**

[***Vulnerability Description***](#_274jvtdnpb32) ***2***

[*Vulnerability Discovery*](#_ca8rgu9umxao) *2*

[*Remote Desktop Protocol*](#_52k2ccvem1a) *2*

[***Vulnerability Outcome***](#_ez6lpif5mzdf) ***3***

[***Affected Systems***](#_fnz1wblvxu3l) ***4***

[***Access Level***](#_g54c8fopy8sa) ***4***

***Setting Environment***

[***Exploitation Demonstration***](#_u6c6l22t6vbb) ***5***

[***Mitigation Strategies***](#_emdkvziapqof) ***6***

[***Conclusion***](#_tn5f4wemblwe) ***7***

[***Reference***](#_rivsnrvkt3jc) ***8***

# 

# **Vulnerability Description**

## *Vulnerability Discovery*

In May 2019, the United Kingdom Cyber Security Centre discovered a vulnerability in the Remote Desktop Services that exists in the Microsoft Operating Systems. This vulnerability has a full CVSS score of 10. <https://www.cvedetails.com/cve/CVE-2019-0708/>  
  
The CVE-2019-0708 more known as Bluekeep, is a vulnerability that could be exploited via Windows Remote Desktop Protocol. Attackers can exploit this vulnerability by performing a remote code execution by sending a specially crafted code to a system that is unpatched and unprotected. Bluekeep is also a wormable vulnerability.

Microsoft sent a worldwide warning twice, on May 14th and once again on May 30th with more urgency for users to update vulnerable Windows Systems due to the Bluekeep vulnerability.

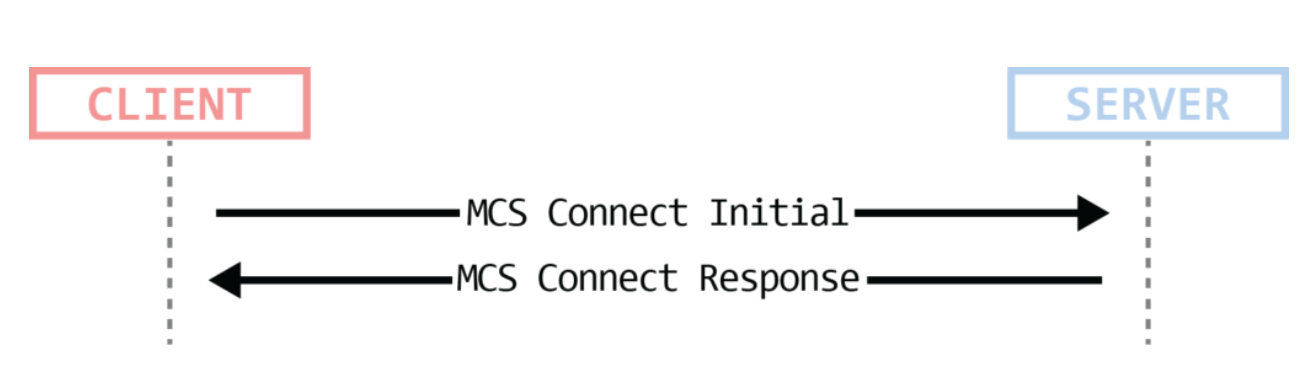
Microsoft released a patch update for all the older Microsoft OS. Patch for unsupported OS like Windows XP were released for the first time in years which indicated a huge warning sign. However, the warning signs were not heeded by enough users which resulted in Microsoft to warrant escalation for update alerts.

The National Security Agency (NSA) then took an unexpected step on 4th June 2019 by publishing an advisory note to warn users on the risk of Bluekeep. NSA warned that the vulnerability could cause a devastating and huge impact. The agency also alerted users to urgently update and patch their systems.

The vulnerability was seen as more serious than expected when the United States government stepped in and issued an “update now” alert through the Cybersecurity and Infrastructure Security Agency (CISA) on June 17th that year.

[*https://www.forbes.com/sites/daveywinder/2019/11/03/windows-bluekeep-attack-that-us-government-warned-about-is-happening-right-now/?sh=450932731a00*](https://www.forbes.com/sites/daveywinder/2019/11/03/windows-bluekeep-attack-that-us-government-warned-about-is-happening-right-now/?sh=450932731a00)

## *Remote Desktop Protocol*

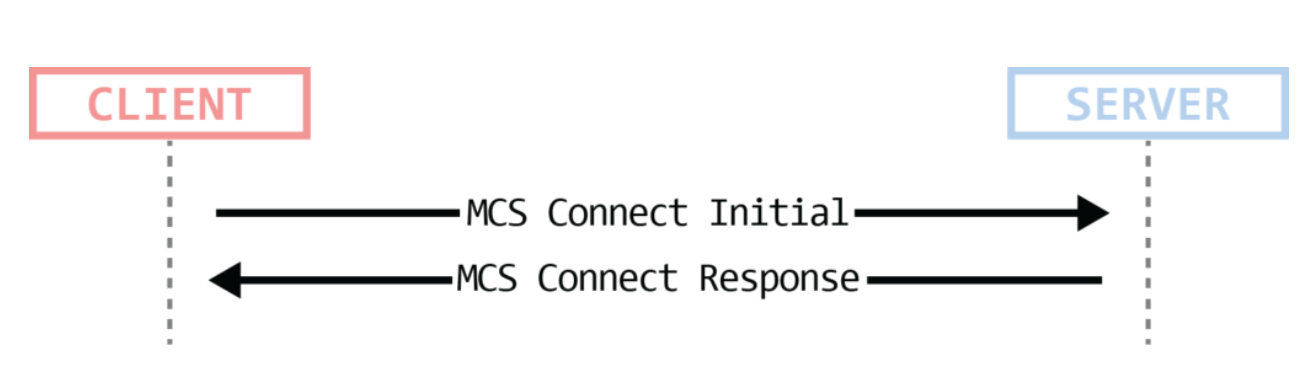


The Remote Desktop Protocol is a widely used service to Windows machines for remote access.

The RDP is a service which enables users to have control of their Windows machine remotely almost like they are working on it locally. The protocol uses the TCP port 3389 by default.   
The RDP protocol establishes a connection between a client and a server by creating data communication channels between them. Virtual channels are bidirectional data pipelines that allow data to be sent back and forth between the two. By default, Windows XP and Server 2003 have 32 virtual channels. As a result of that limitation, dynamic virtual channels were created. Windows attaches the static virtual channel names to numbers within the driver called ‘TermDD.sys’

Channels are referenced to Windows with different names and could be used for different purposes. For example, rdpsnd for sound sharing and cliprdr for clipboard. These channels could be used by clients using the RDP api. RDP reserves channel 31 with the name MS\_T120, by default. However, it does not check the existence of 2 channels with the same names. This is where the vulnerability surfaces.

Attackers could set up the name MS\_T120, with a different channel number which could result in the existing RDP session having the same channel in 2 different places, within the 32 different channels that are available. For example, the malicious MS\_T120 could be on Channel 22 while the default one on Channel 31.



When an attacker sends a specially crafted code to the system via the malicious channel, the TermDD.sys driver would attempt to shut the channel and terminate the RDP session. When the default channel is terminated, the reference pointer for Channel 22 would be cleared. However, a dangling pointer would remain, tied to Channel 31 which would lead to a use-after-free vulnerability. This vulnerability lets an attacker determine the space memory to execute arbitrary code and malicious payloads.

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/>

# **Vulnerability Outcome**

If Bluekeep is successfully exploited, it might have a number of negative consequences.

Approximately 100 million devices are potentially vulnerable to Bluekeep due to the open RDP port. Bluekeep is wormable vulnerability which means it has the ability to self-replicate and affect other computers across the network. This is similar to the EternalBlue exploit which was used in ransomware attacks like WannaCry which affected systems worldwide back in 2017.

This vulnerability also affects mostly older systems which are more vulnerable compared to the newer OS. This is because outdated operating systems are typically not adequately maintained by the vendor, in this instance Microsoft, or by the users. Windows XP is another one of the impacted operating systems which has been out of support for years. This vulnerability, however, is sufficiently serious that Microsoft chose to release a patch even for Windows XP.

Another important effect is that this vulnerability impacts the Remote Desktop Services, which are utilized by millions of machines globally and are particularly prevalent in vital industries such as healthcare and industrial controls.

Bluekeep may possibly have a large impact, comparable to WannaCry, which infected over 200,000 systems globally and had a total economic cost of approximately $4 billion.  
<https://www.youtube.com/watch?v=AkXM2wywMN0>

# **Affected Systems**

This vulnerability has mainly affected systems that run the older versions of Windows Operating Systems.

The OS versions that are affected are:

* Windows 2000
* Windows Server 2003
* Windows Server 2003 R2
* Windows Server 2008
* Windows Server 2008 R2
* Windows XP
* Windows Vista
* Windows 7

The newer operating systems like Windows 8 and 10 are deemed safe as for now.  
<https://us-cert.cisa.gov/ncas/alerts/AA19-168A>

# **Access Level**

If an attacker manages to successfully exploit the vulnerability, he would be able to install programs; read, modify or delete data. As well as creating new accounts with full user rights.  
This would mean the attacker would be able to have full control of the affected system.

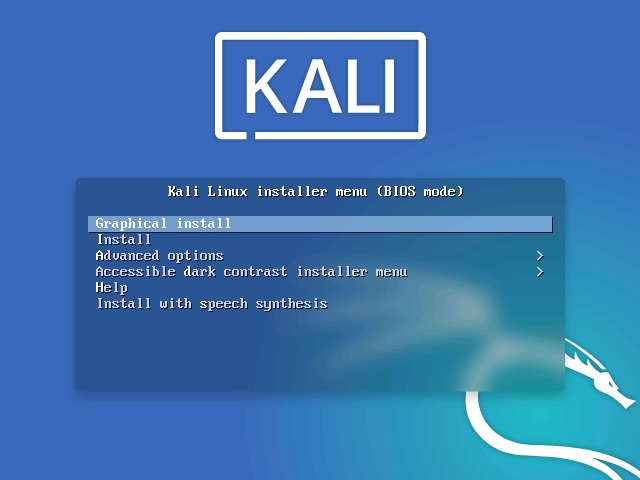
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708>

# **Setting Environment**

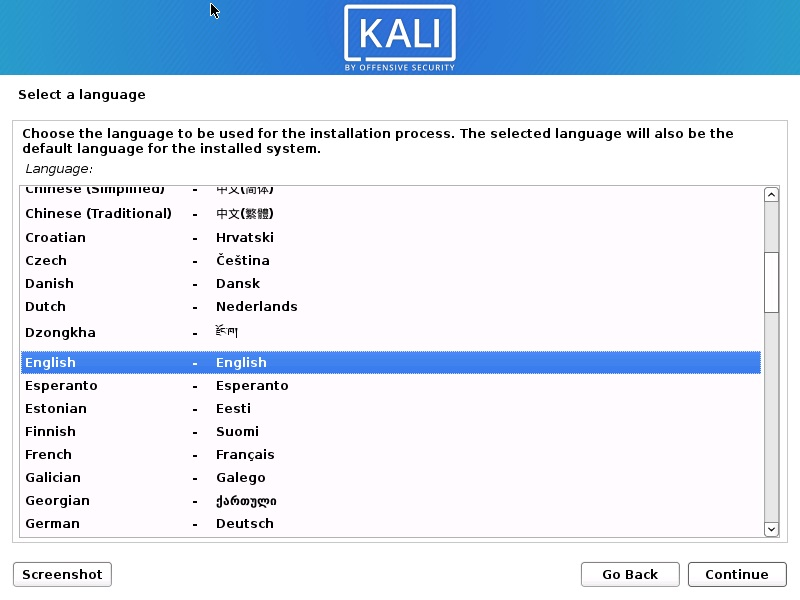
Setting Environment: VRbox

Setting Environment: kali2020

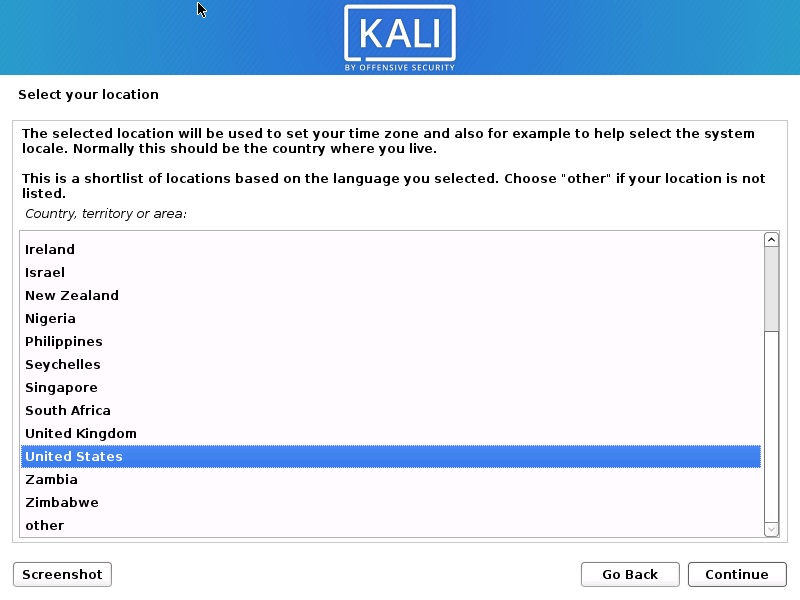
* Select Graphical Install from Boot Menu



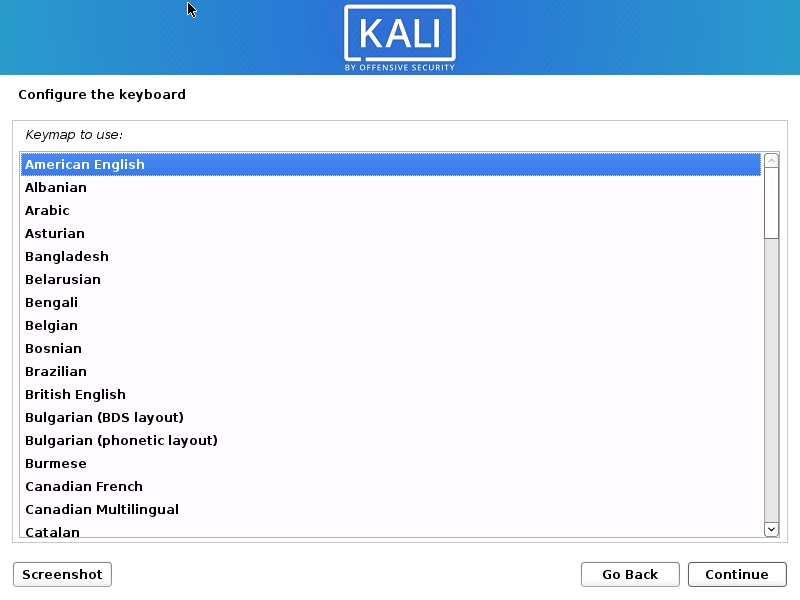
* Select a language



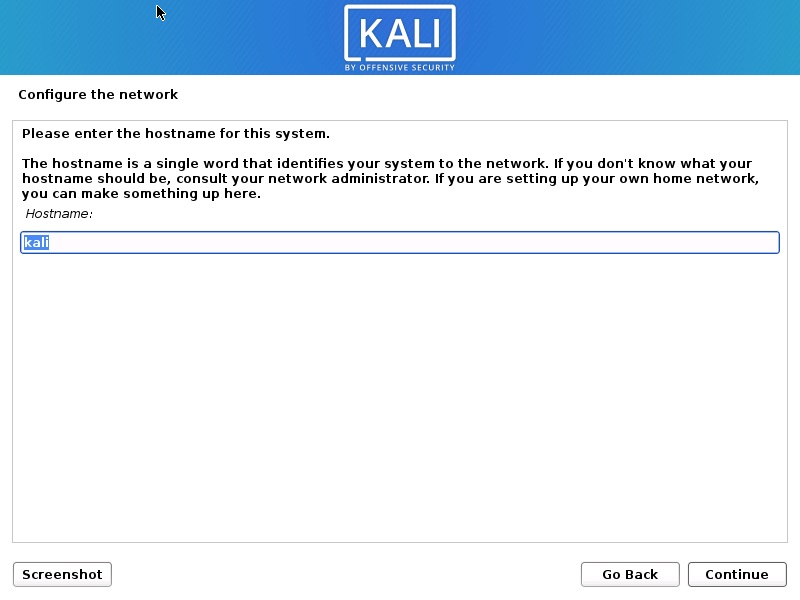
* Select location



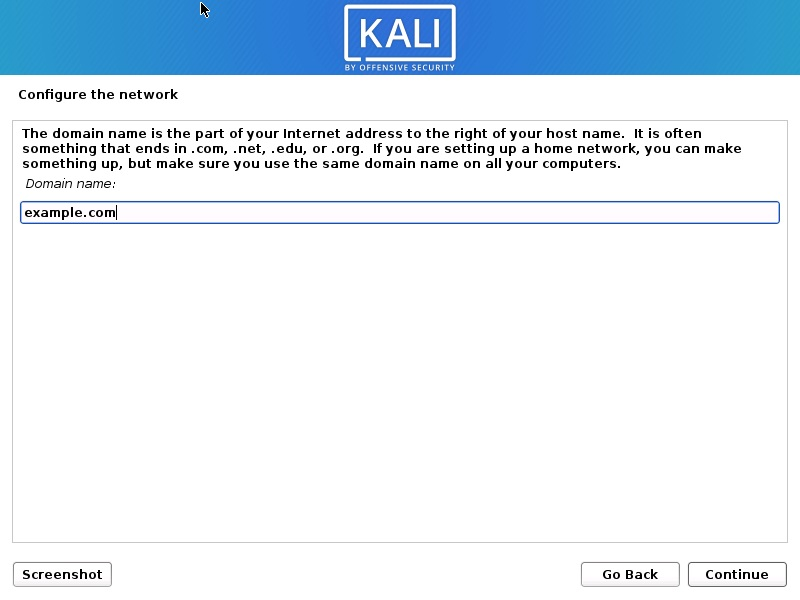
* Configure the keyboard



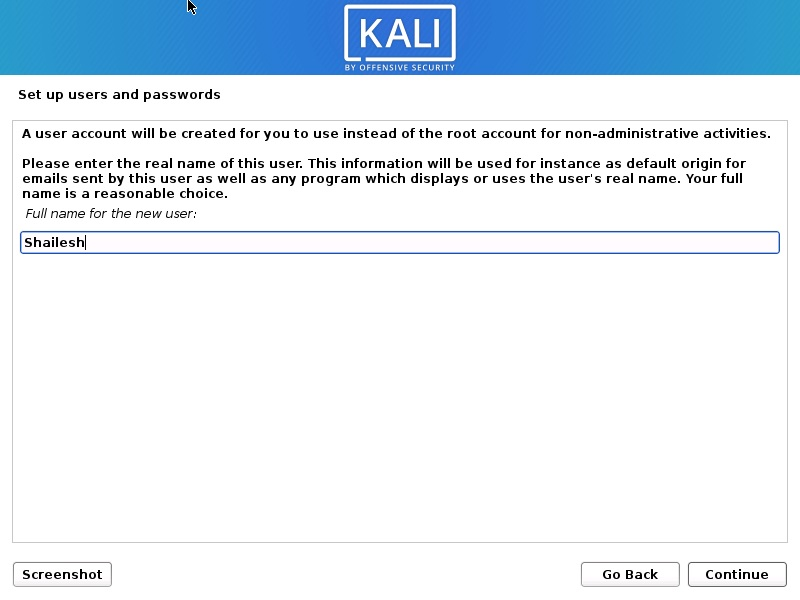
* Network configuration: Host Name



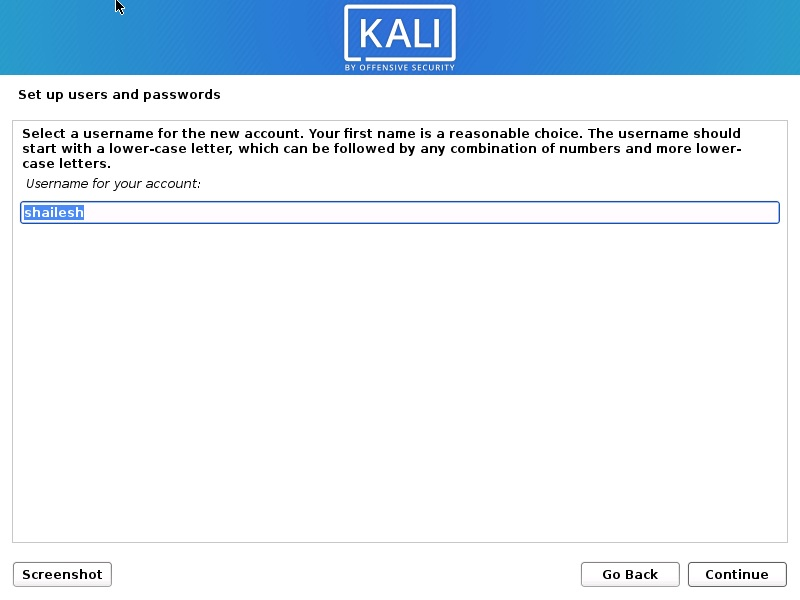
* Network configuration: Domain Name



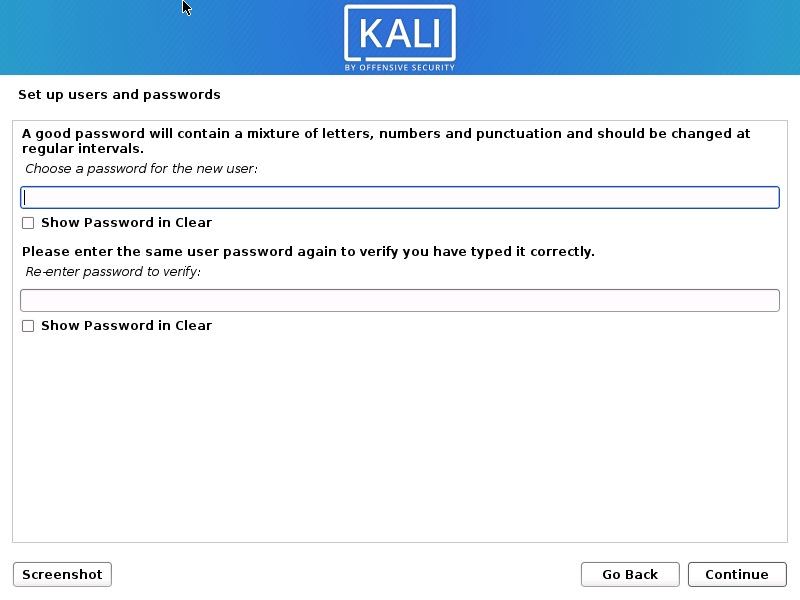
* Set user account



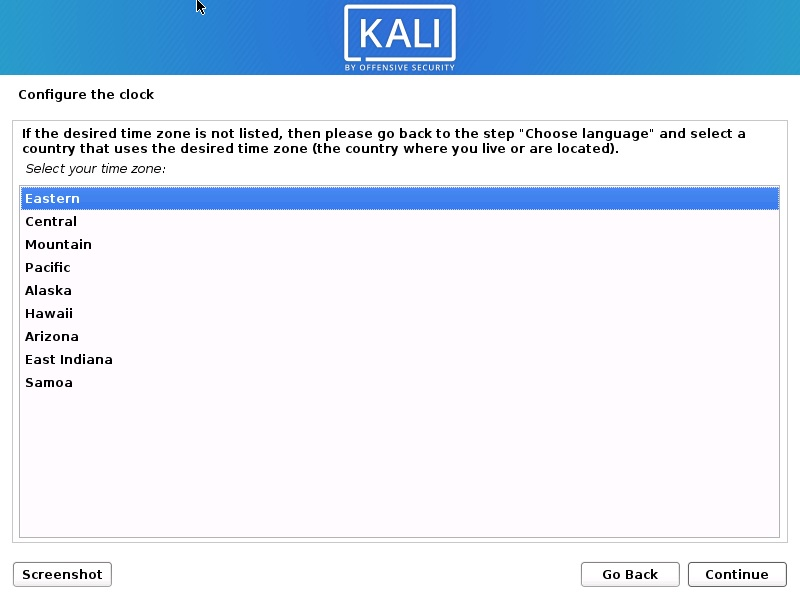
* Set user name



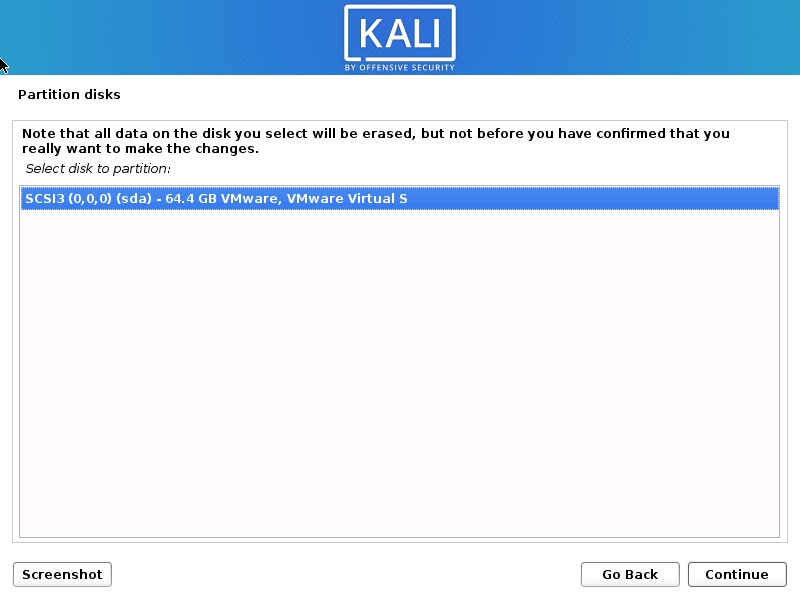
* Set user Password



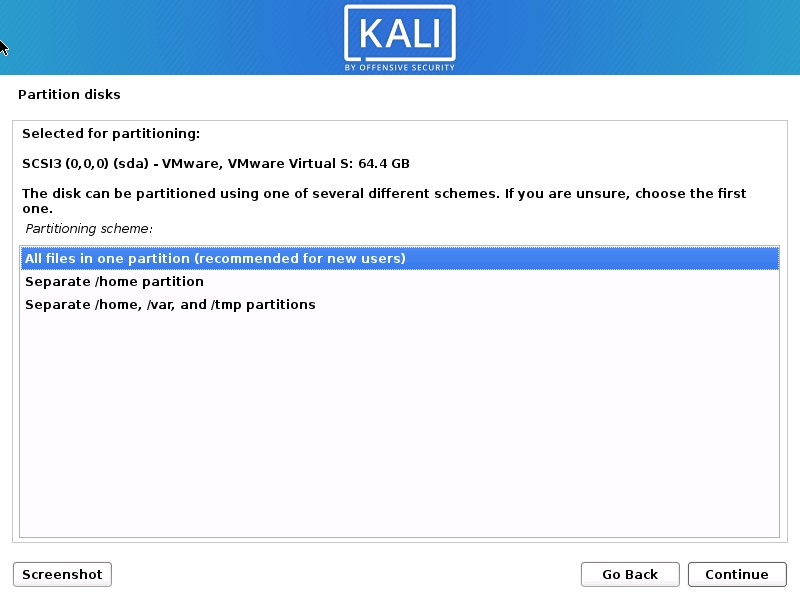
* Time configuration



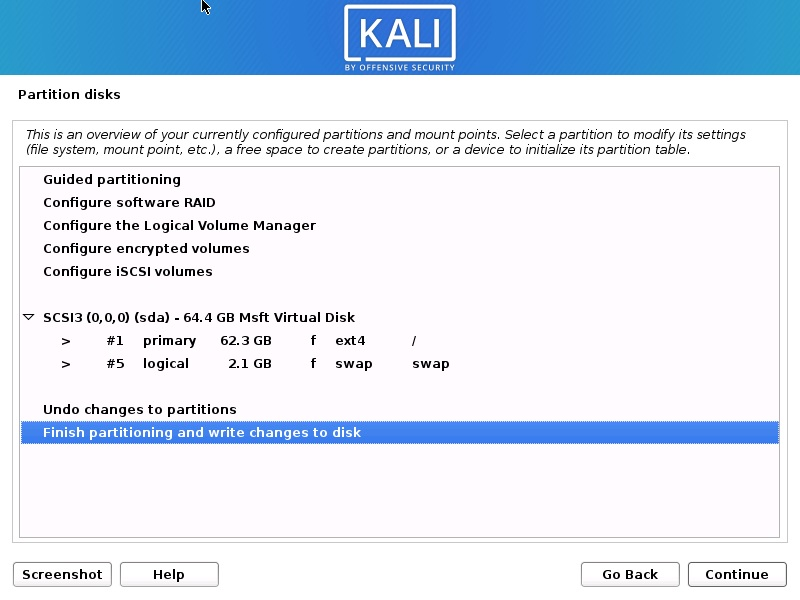
* Partition disk



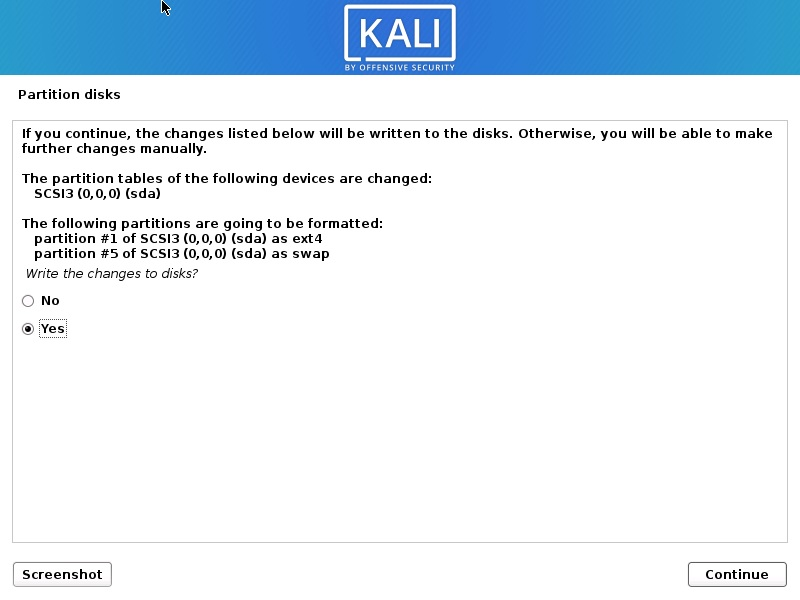
* Select partition scheme



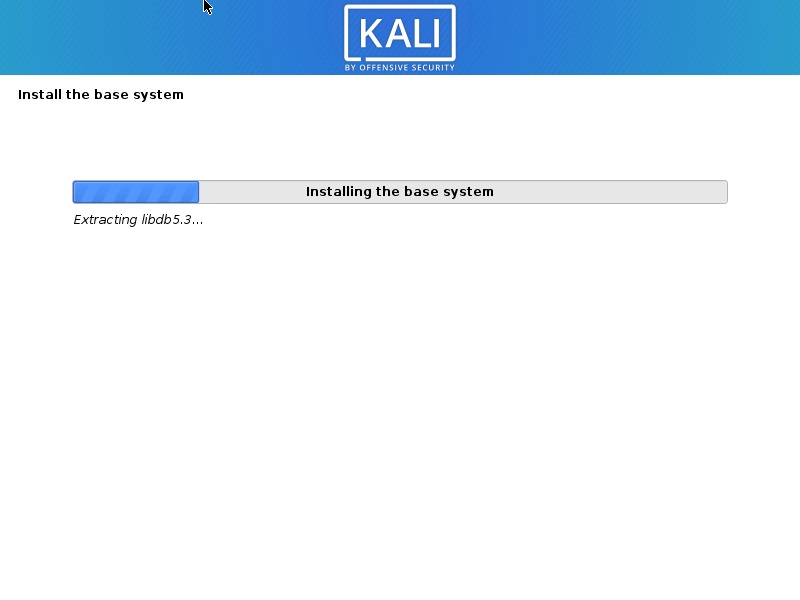
* Disk partition over view



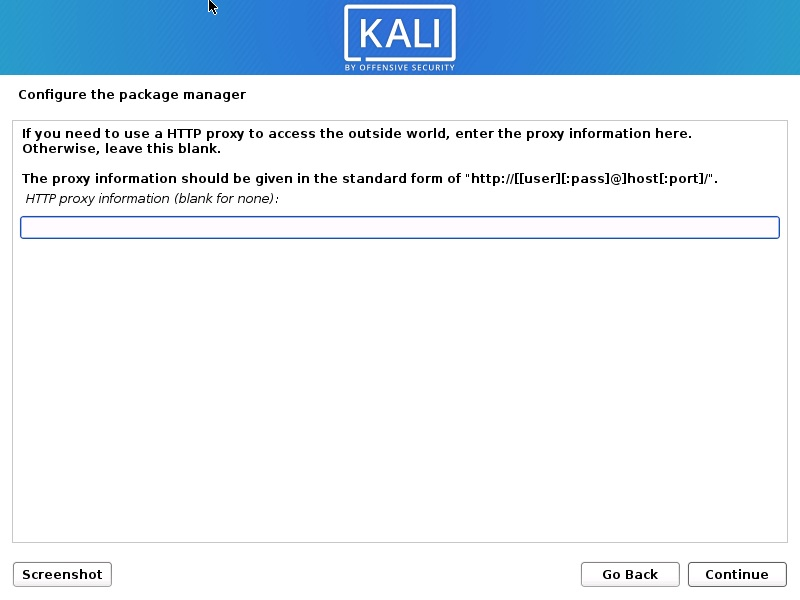
* Disk partition confirmation



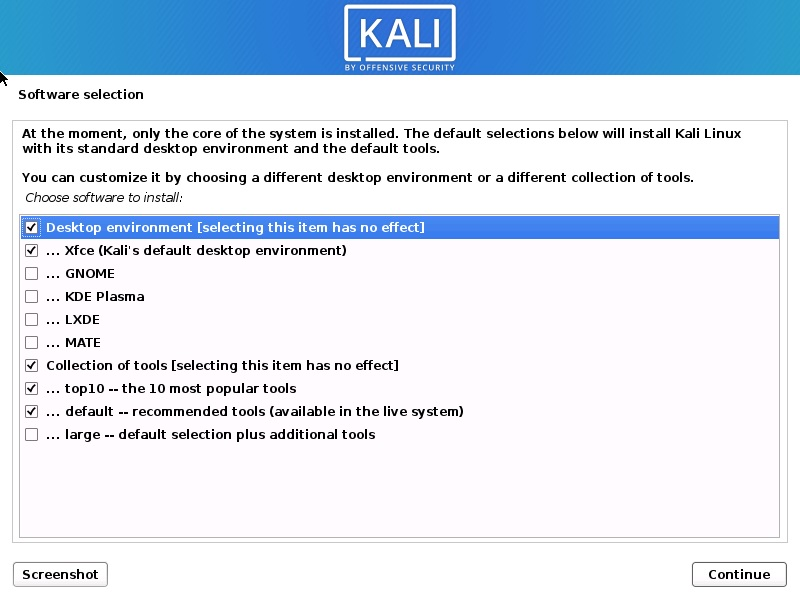
* Start installation



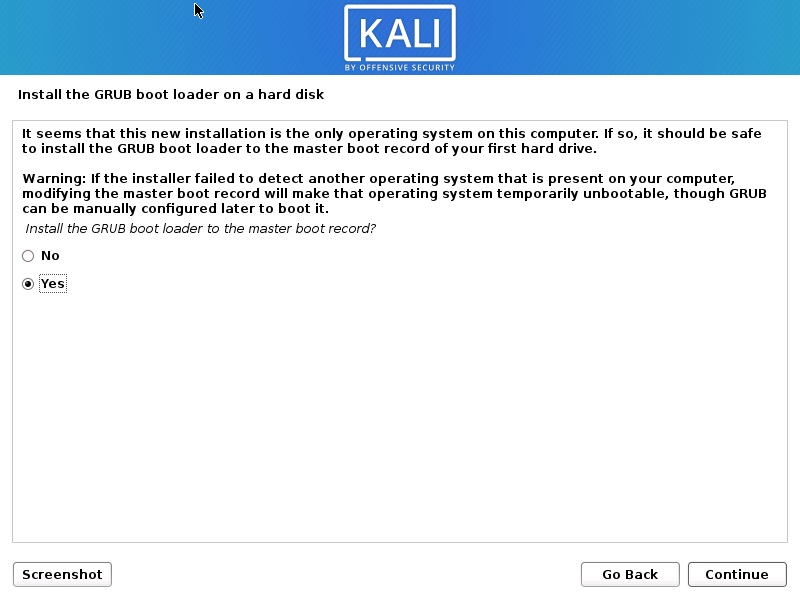
* Configure the package manager



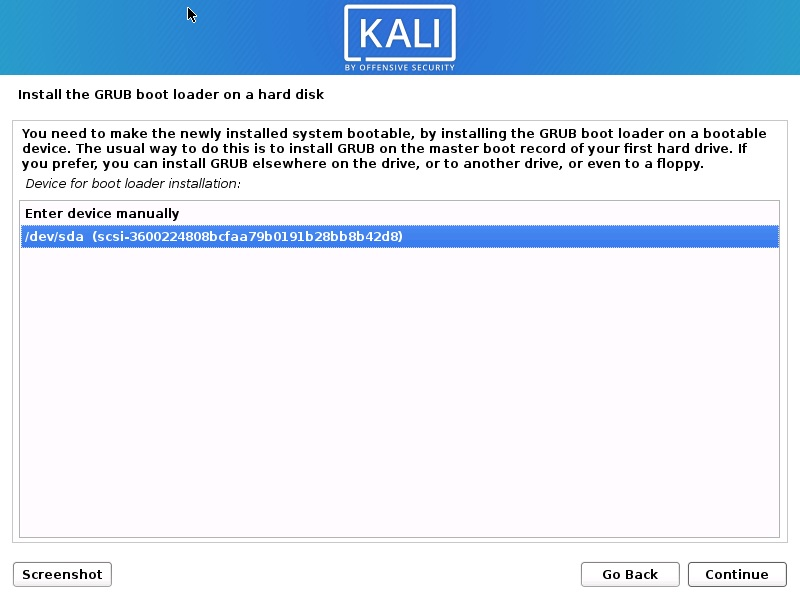
* Software selection



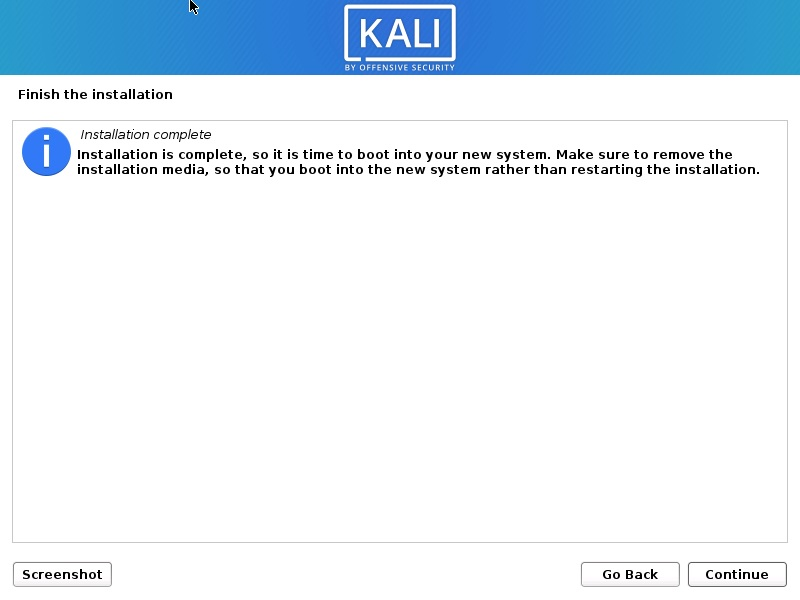
* GRUB boot loader installation



* Select device for GRUB boot loader installation



* Complete installation

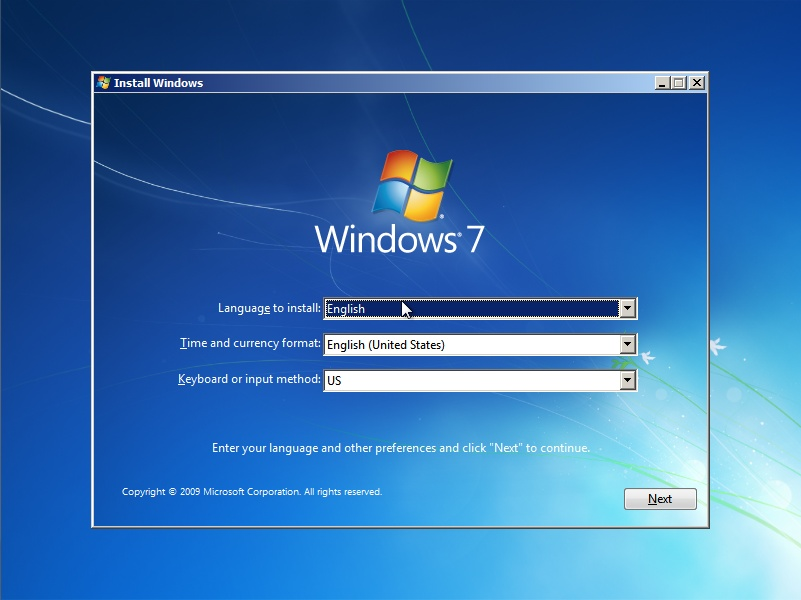


* Complete the process

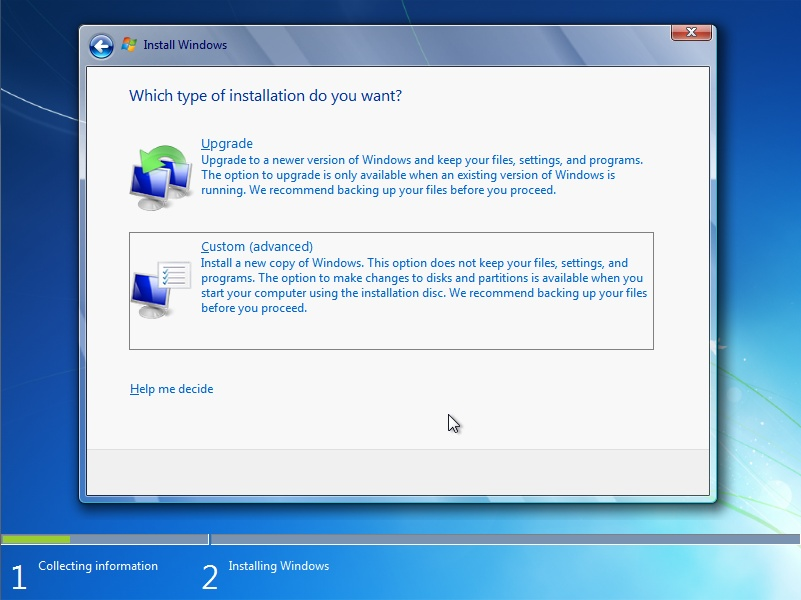


Setting Environment: windows 7

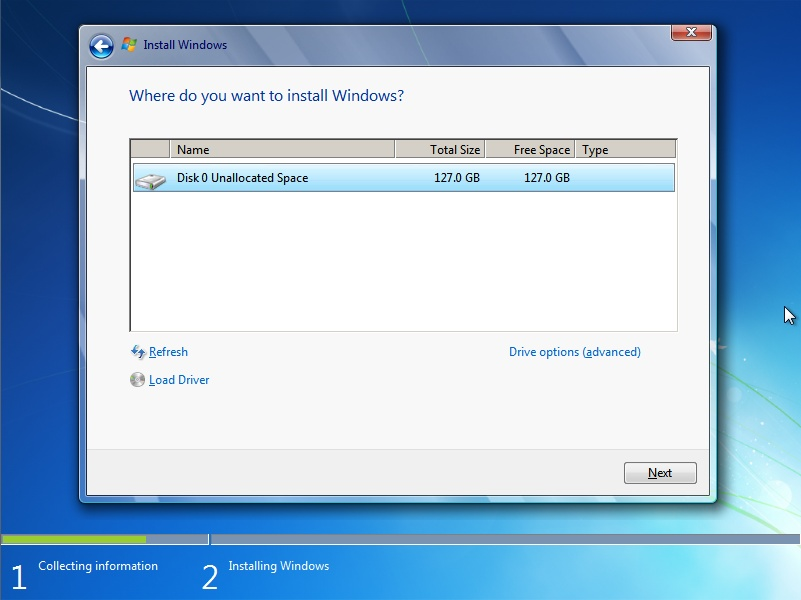
* Set language



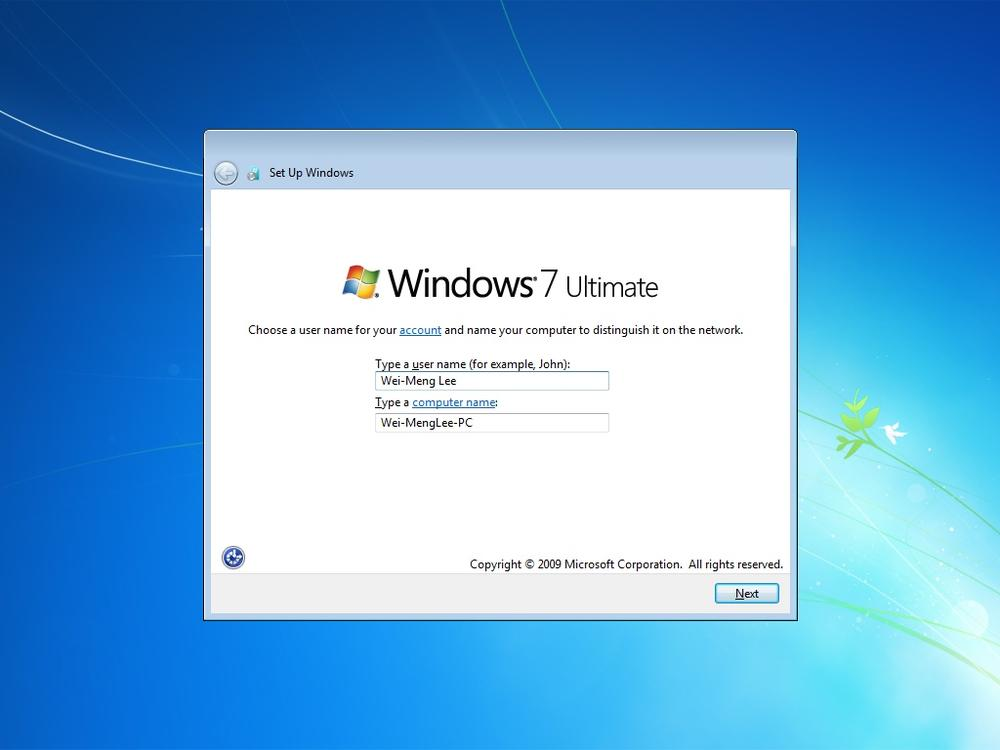
* Select upgrade or fresh installation



* Select the disk for installation



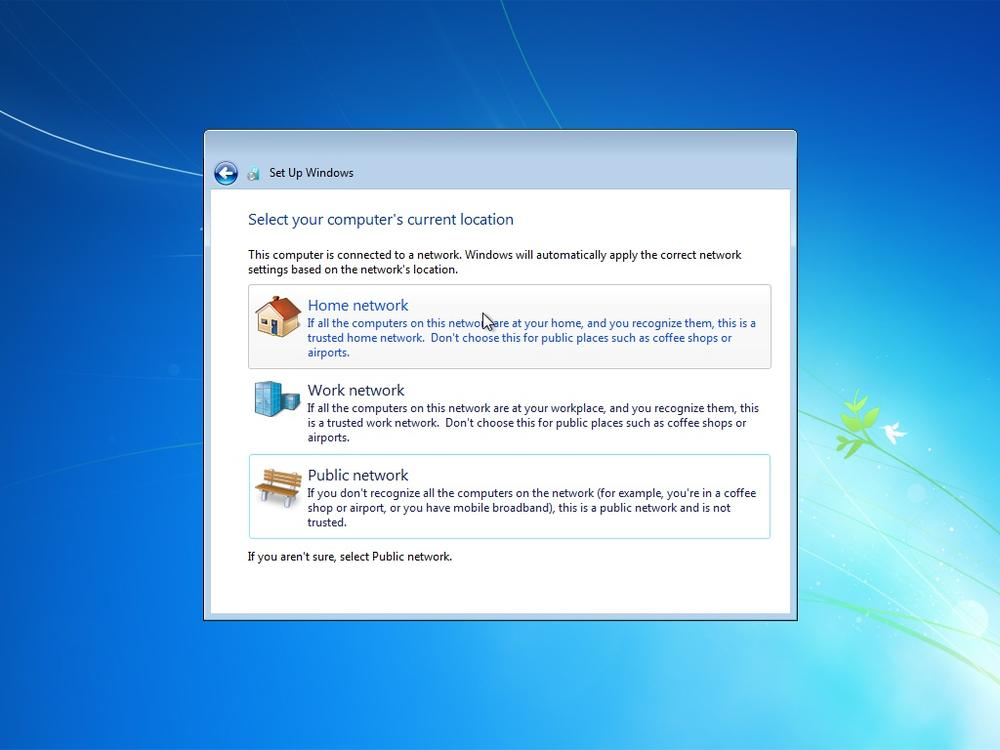
* Set user name for account



* Select update method



* Select current location of computer (installation overs. Next move to network settings)



To replicate a vulnerable Windows OS refer to the following steps:

1. Under firewall settings, head to the advanced options as show in the image below, Fig. X
2. Click inbound rules and scan through all remote options
3. Ensure all remote options are enabled. If these Inbound rules are not enabled, right-click on the rules and enable them as shown in Figure X.

# 

# **Exploitation Demonstration**

# Basically, Virtual box version 6 is used. Attacking client server is kali Linux 2020.2, and the victim server is windows7 Ultimate. Also, open-source packet analysis program 'Wireshark' is used to show the impact specifically.

# 

# 

# First, move to the Bluekeep directory. codes which will use to demonstrate bluekeep are stored in this directory.

# 

# 

# Perform the command ‘git clone https://github.com/Ekultek/BlueKeep’ to download proof of concept code for demonstrating bluekeep vulnerabilities.

# 

# 

# And then log in to the root account to get authority.

# 

# 

# Then, enter Command 'arp-scan'. It is a protocol used to bind an IP address to a physical network address on the client network.

# 

# 

# After finishing scanning, enter command 'nmap -sV -p 3389 ip'. Nmap is for port scanning and 'sV' is used to define service versions. 'p' makes nmap to scan only specified ports and 3389 is Windows RDP port number. Bluekeep only can exploit with this port opened, so this is the process to check the victim. The appeared IP address matches with the victim server’s IP, and it shows that the port is opened.

# 

# Enter the command 'python3 bluekeep\_poc.py -i ip' Python3 is the executing method. It means I will use python version3 to execute the code. and following is file name and victim Pc’s IP.

# 

# 

# Poc file verifies that RDP is enabled on the victim's PC. It Also Checks the packet value. The client can then connect to the port 3389 and can verify SSL/TLS version information. When it attempts SSL/TLS communication during the SSL/TLS connection process, TLS version, cipher List supported by client, and the number information generated by the client server can be checked. The victim server sends a SSL version information, a cipher List supported by the client, and the number information generated by itself to the client server and then sends "Server Hello Done". The victim server also sends its own certificate information to the client. The client generates a pre-master-secret from a random number created by itself and the victim server. It is encrypted and sent to the server via the server's public key. This process generates symmetric keys that are used for encryption. And the client server uses negotiated algorithms and keys for RDP remote requests and SSL/TLS connection requests.

# 

# 

# 

# 

# 

# Enter the commands 'python3 bluekeep\_dos.py -i ip'. Python3 is the executing method. It means I will use python version3 to execute the code. and following is file name and victim Pc’s IP. Dos file is aiming to make a crash on the victim’s server.

# 

# 

# 

# 

# The transmission of RST packets from TCP ports is used when the sender attempts to do something invalid and means that the connection and termination of the communication cannot be done normally.

# 

# 

# It is shown that after executing bluekeep\_dos.py, the victim server shows the blue screen and sends the RST packet to Attacking server.

# 

# 

# **Mitigation Strategies**

There are some mitigation methods to help prevent Bluekeep vulnerability from being exploited.

* Place the Remote Desktop protocol listener behind a two-factor authentication mechanism such as VPN, SSL tunnel or RDP gateway.
* Enable the Network Level Authentication (NLA). This would prevent unauthorized access to the RDP tunnel by requiring users to authenticate before connecting to remote system, which decreases the likelihood of RDP-based worms
* Apply the patch that was released by Microsoft Windows. This would force the MS\_T120 channel to always divert to Channel 31 even if an RDP server requests otherwise.
* Disable the Remote Desktop Services with its link port TCP 3389 when not in use.

<https://www.microsoft.com/security/blog/2019/08/08/protect-against-bluekeep/>

# 

# **Conclusion**

# 

# **Reference**