þÿSerious Pentest documention with latest Dradis Framework (2.5.0)

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

A key part of any serious Penetration Test is to provide a comprehensive documentation of all phases - reconnaissance, enumeration, exploitation and finale documentation.

Now you have a fully loaded BT4 Pentest-Weapon, having a well-defined documentation process is another great way to extend the awesome BT4!

Especially in larger engagements it is key to exchange all findings with the whole team in the most effiecent way and therefore I'd like to provide a little howto to use the great dradis information sharing framework.

Dradis core components are based on ruby rails and sqlite3, fully customizable through the plugin API, importing information from key sec-tools like nmap, burb or nikto; simple frontend with essential tools to create your documentation (no fancy, overloaded editor or options, keep it simple and bring it to the point!)

Export engine is also quite interesting, currently HTML and Word export is possible, wherby the Word one is the most interesting one, after you created an initial template with the specific dradis meta-tags, you are ready to go - takes some time, but once done, you have the power to create a quick report after all your tasks you have documented within dradis. Details can be found here:
WordExport templates - dradis

BT4 comes with dradis 2.4 (/pentest/misc/dradis) and 2.5 was just released. Dradis is simple to install and to initialize for the first run, but not really intuitive for novice users, especially performing some automated tasks. Also some confusing options during first-time initialization...

Thefore I've created a shell-script to create a fully custom dradis initialization, just to use the tool and not spent to much time going through the internals to customize it yourself.

Script features:
-fully custom dradis 2.5.0 installation

-script needs to be executed without parameter, but have a look in the script to set some basic parameters

-Simple menue to choose between dradis features (custom ssl cert, view shared pwd, xml parser to see word export teplate meta tags etc)

-Automated import of predefined templates (I've one basic pentest template included)

-Full backup of sqlite3 & dradis environment settings, including using GPG to encrypt it
(for any engagement you should create a new DB - data privacy ;-)

-Import a basic Pentest template (you can set a parameter to define type of template
you'd like to import, currently I've only added a simple one. Maybe ISECOM is a good
reference or http://www.vulnerabilityassessment.c...rationTest.zip)

-Create a custome SSL certificate (dradis runs default only on localhost/https)

INSTALLATION:

1. download http://zerohat.de/_shared_files/drad...ler_1.1.tar.gz
2. unpack & start script
Code:

sudo ./startDradis

3. start with menu option 1

Please, this projects fully relies on community feedback and etd (key developer)
is always looking for feedback - especially from the Pentest community.

Give it a try, any comments/criticism are welcome...

/brtw2003

P.S.: for clarification, just have a look in the actual script - like stated above, never executed blindley any kind of tools, even if it's from so
called 'trusted' sources! The installer includes some useful templates &
the original dradis 2.5.0 source code,feel free to use...
http://pastebin.com/m4e2b8bc

