ვირტუალური კიბერ ლაბორატორიის აწყობა

შესავალი

გატეხის (ჰაკინგის) მეთოდების შესასწავლად პრაქტიკული მეცადინეობები არის აუცილებელი. ალბათ გვახსოვს, რომ გატეხა მხოლოდ მაშინ არის კანონიერი, თუ მას ან ჩვენს ინფრასტრუქტურაზე ვაწარმოებთ, ან მფლობელის წერილობითი ნებართვა გვაქვს. იმისთვის, რომ კანონის ფარგლებში დავრჩეთ, მოსახერხებელ გამოსავალს წარმოადგენს კიბერუსაფრთხოების ვირტუალური ლაბორატორიის მომზადება.

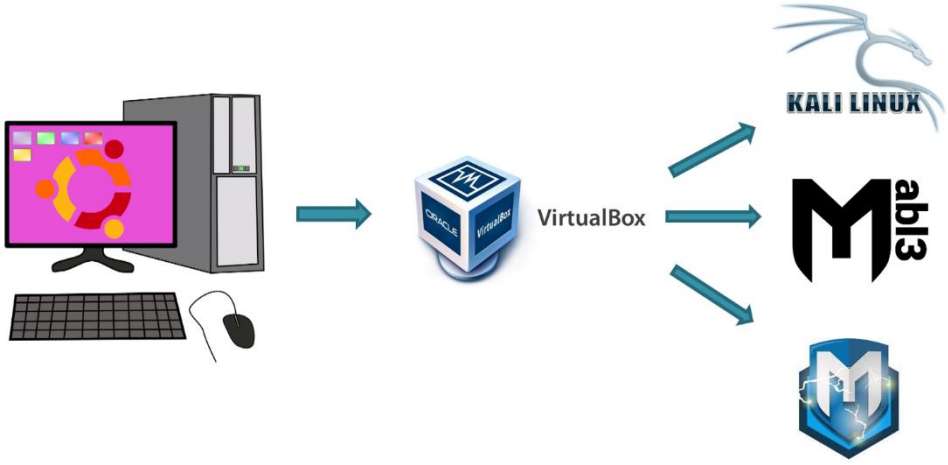
კიბერუსაფრთხოების ლაბორატორია შეიძლება მთლიანად აიწყოს ვირტუალურ გარემოში და თან ზუსტად ასახავდეს ფიზიკურ გარემოს. აქედან გამომდინარე, ვირტუალურ გარემოში ჩატარებული ყველა ექსპერიმენტი ძალაში იქნება რეალურ ინფრასტრუქტურაზეც.

ვირტუალურ ლაბორატორიას სხვა კარგი მხარეებიც აქვს - მომენტალურად შეგვიძლია დავამატოთ კომპიუტერები და ასევე სწრაფად შეგვიძლია წავშალოთ როცა აღარ დაგვჭირდება. ფაქტობრივად, ერთი (ან რამდენიმე) ყოჩაღი კომპიუტერით ჩვენ მთელი ინფრასტრუქტურა შეიძლება შევქმნათ თავისი ქსელებით და კომპიუტერებით.

ვირტუალური ლაბორატორიის ასაწყობად ჩვენს კომპიუტერზე დავაყენოთ VirtualBox.

VirtualBox არის უფასო და ღია კოდის ვირტუალიზაციის პროგრამა, რომელიც შემუშავებულია Oracle-ის მიერ. ის საშუალებას გვაძლევს, რომ გავუშვათ მრავალი ვირტუალური მანქანა (VM) ერთ ფიზიკურ კომპიუტერზე. თითოეული ვირტუალური მანქანა არის დამოუკიდებელი კომპიუტერი თავისი ოპერაციული სისტემით და პროგრამული უზრუნველყოფით.

VirtualBox-ში შევქმნით ვირტუალურ კომპიუტერებს და სათანადო ქსელურ ინფრასტრუქტურას.



Virtual Box-ში შევქმნათ `KaliLinux`-ის ვირტუალური კომპიუტერი, `Metasploitable 2` და `Metasploitable 3` კომპიუტერები და მოვათავსოთ ისინი ერთიან ქსელში.

Metasploitable კომპიუტერი წარმოადგენს სისუსტეებით განზრახ გაჯერებულ კომპიუტერს, რომელიც ჩვენი KaliLinux-ის სამიზნე იქნება დაუცველობების გამოვლენისთვის და მათი გამოყენებით უსაფრთხოების ხელყოფისთვის.

აღწერილი გარემოს შექმნის ყველა ნაბიჯი ქვემოთ არის განხილული დაწვრილებით.

ოპერაციული სისტემის განახლება

მნიშვნელოვანი სამუშაოს წინ, ყოველთვის გირჩევთ კომპიუტერის ოპერაციული სისტემის განახლებას. Ubuntu-ს შემთხვევაში განახლება შემდეგი ორი ბრძანებით ხდება:

```
$ sudo apt update
```

```
$ sudo apt upgrade
```

Virtual Box-ის და მისი Extension Pack-ის ინსტალაცია

VirtualBox-ის დაყენება თითქმის ყველა ოპერაციულ სისტემაზე არის შესაძლებელი. ამ მისამართზე არის ოფიციალური დოკუმენტაცია: `https://www.virtualbox.org/wiki/Downloads`

Linux-ზე VirtualBox-ის ინსტალაცია შემდეგი ბრძანებით ხდება:

```
$ sudo apt install virtualbox
```

თუ ეკრანზე შემდეგი შეცდომა გამოვიდა „Failed to start LSB: VirtualBox Linux kernel module“, ეს ნიშნავს, რომ თქვენ `secure boot` უნდა გათიშოთ კომპიუტერზე. გადატვირთეთ კომპიუტერი, შედით BIOS-ის კონფიგურაციაში და გათიშეთ secure boot.

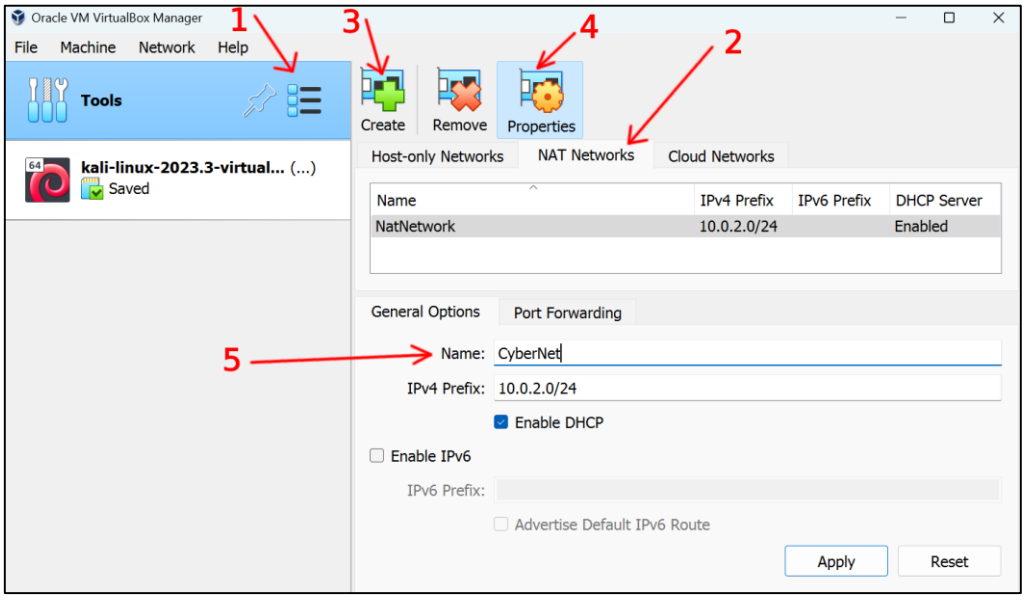
იმისთვის, რომ VirtualBox-ის ფუნქციონალობა სრულად გამოვიყენოთ, მისი გაფართოების ნაკრები (`extension pack`) უნდა დავაყენოთ.

გაფართოების ნაკრები შემდეგი ბრძანებით ყენდება:

```
$ sudo apt install virtualbox-ext-pack
```

Nat Network ქსელის შექმნა Virtual Box-ში

VirtualBox-ში შექმენით ახალი `Nat Network` ქსელი. სწორედ ამ ქსელში გავაერთიანებთ ჩვენი კიბერ ლაბორატორიის კომპიუტერებს. საერთო ქსელში ჩართვა აუცილებელია იმისთვის, რომ კომპიუტერებს ერთმანეთთან ჰქონდეთ წვდომა და შესაძლებელი გახდეს ერთის საშუალებით მეორის გატეხა. ქსელის შესაქმნელად სულ რამდენიმე ღილაკზე მოგვიწევს დაჭერა, იხილეთ შემდეგი სურათი:



ქსელს `CyberNet` დავარქვათ, ისე, როგორც სურათზე არის ნაჩვენები.

Kali Linux-ის გადმოწერა და დაყენება

Kali Linux-ის გადმოსაწერად და VirtualBox-ში მის დასაყენებლად ისარგებლეთ ოფიციალური დოკუმენტაციით: `https://www.kali.org/docs/virtualization/import-premade-virtualbox/`

ოფიციალურ დოკუმენტაციაში Kali Linux-ის ვირტუალურ მანქანას 2 გიგაბაიტი ოპერატიული მეხსიერება აქვს დათმობილი, თუმცა 1-ზეც იმუშავებს და გაითვალისწინეთ თუ თქვენს კომპიუტერს არ აქვს დიდი მეხსიერება.

ასევე გაითვალისწინეთ რომ 1 პროცესორიც სავსებით საკმარისია ამ მანქანისთვის. როგორც დოკუმენტაციიდანაც შეიტყობთ, მომხმარებელი არის `kali`, პაროლიც არის `kali`.

ახლად შექმნილი ვირტუალური მანქანა მოათავსეთ `CyberNet` ქსელში.

Metasploitable 2-ის გადმოწერა და დაყენება

Metasploitable 2 არის ვირტუალური მანქანა რომელიც გამიზნულად აღჭურვილია მრავალი დაუცველობით. იგი გამიზნულია (ძირითადად Metasploit-ის გამოყენებით) შეტევების გასათამაშებლად.

Metasploitable 2-ის გადმოსაწერად და მის დასაყენებლად ისარგებლეთ ოფიციალური დოკუმენტაციით: `https://docs.rapid7.com/metasploit/metasploitable-2/#powering-on-metasploitable-2`

ამ ვირტუალურ მანქანასაც სავსებით ყოფნის 1GB ოპერატიული მეხსიერება და ისიც იმავე Nat Network-ში უნდა მოვათავსოთ.

როგორც დოკუმენტაციიდანაც შეიტყობთ, მომხმარებელი არის `msfadmin`, პაროლიც არის `msfadmin`.

Metasploitable 3-ის დაყენება

Metasploitable 3 არის ვირტუალური მანქანა რომელიც გამიზნულად აღჭურვილია მრავალი დაუცველობით. იგი გამიზნულია (ძირითადად Metasploit-ის გამოყენებით) შეტევების გასათამაშებლად. არსებობს მისი ორი ვერსია, ლინუქსის კომპიუტერი და ვინდოუსის კომპიუტერი.

წინაპირობები

Metasploitable 3-ის დაყენება სტრუქტურულად განსხვავდება Metasploitable 2-ისგან. წინა შემთხვევაში კომპიუტერი უკვე იყო აღჭურვილი პროგრამებით და ჩვენ მხოლოდ მისი გამოწერა და დაყენება გვჭირდებოდა. Metasploitable 3-ის შემთხვევაში, ვინაიდან იგი `Windows Server 2008`-ის ბაზაზეა, მისი გავრცელება ვერ მოხდება VirtualBox-ის ფაილის სახით Microsoft-ის მოთხოვნების გამო. ამიტომ, ჩვენ მოგვიწევს რამდენიმე პროგრამული ხელსაწყოს დაყენება, რომ ჯერ ამ სერვერის სუფთა ვერსია გადმოვწეროთ და შემდეგ დავაყენოთ სათანადო დაუცველი პროგრამები და დავამატოთ საჭირო მომხმარებლები.

Metasploitable 3-ის დაყენებისთვის საჭირო დამხმარე პროგრამული ხელსაწყოებია:

- Packer: `https://www.packer.io/docs/install/index.html`
- Vagrant: `https://www.vagrantup.com/docs/installation/`
- Vagrant Reload Plugin: `https://github.com/aidanns/vagrant-reload#installation`

მივყვეთ სათანადო ოფიციალურ დოკუმენტაციას და დავაყენოთ ზემოთ მოყვანილი პროგრამები.

Metasploitable 3-ის დაყენება

გაითვალისწინეთ, რომ თქვენ უნდა დაარედაქტიროთ `VagrantFile` თუ მხოლოდ ლინუქსის ან მხოლოდ ვინდოუსის მანქანის დაყენება გსურთ.

Linux-ის მომხმარებლებისთვის შემდეგი ბრძანებებია საჭირო:

```
$ mkdir metasploitable3-workspace
$ cd metasploitable3-workspace
$ curl -O https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile && vagrant up
```

Windows-ის მომხმარებლებისთვის შემდეგი ბრძანებებია საჭირო:

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -
OutFile "Vagrantfile"
vagrant up
```

გაითვალისწინეთ, რომ ინსტალაცია საკმაოდ ხანგრძლივია - 2-3 საათი.

Metasploitable 3-ის აწყობა (Building)

ეს ნაბიჯი არ არის საჭირო თუ უკვე გადმოწერეთ და დააყენეთ Metasploitable 3 წინა თავში მოყვანილი ინსტრუქციის მიხედვით.

გადმოწერეთ ან დააკლონირეთ (clone) Metasploitable 3 მისი GitHub-ის რეპოზიტორიიდან `https://github.com/rapid7/metasploitable3/`.

გაითვალისწინეთ რომ თუ Hyper-V გაქვთ გააქტიურებული, უნდა გათიშოთ იგი VirtualBox-ის სრულფასოვანი ფუნქციონირებისთვის.

გაუშვით PowerShell ადმინისტრატორის უფლებებით და გადადით Metasploitable 3-ის ფოლდერში. გაუშვით შემდეგი ბრძანება:

```
Set-ExecutionPolicy Unrestricted
```

ახლა მზად ვართ ავტომატური პროცესის დასაწყებად. უნდა გავუშვათ სკრიპტი, რომელიც გადმოტვირთავს `Windows Server 2008`-ის საცდელ ვერსიას და დააყენებს მასზე საჭირო პროგრამებს.

სკრიპტის მოქმედებაში მოსაყვანად გაუშვით შემდეგი ბრძანება:

```
.\build.ps1 windows2008
```

სკრიპტის მუშაობას დაახლოებით 1 საათი დასჭირდება. ამის მერე გაუშვით შემდეგი ბრძანება:

```
vargant up
```

ამის მერე, Metasploitable 3 დაყენდება VirtualBox-ში.

Metasploitable 3-ის გამართვა

ვირტუალური მანქანის მომხმარებელი არის `vagrant`, პაროლიც არის `vagrant`.

1 ან 2 გიგაბაიტი მიეცით ვირტუალურ მანქანას. ზოგიერთ შემთხვევაში 2 გიგაბაიტი და 2 CPU გარკვეულ პრობლემებს ქმნის.

თავდაპირველად ეკრანის ზომა იქნება მცირე. ეკრანის ზომის გასაზრდელად guest additions CD უნდა ჩადოთ ვირტუალურ მანქანაში (შემდეგი მენიუს დახმარებით Device -> Insert guest additions CD image) და გაუშვათ სათანადო, 64 ბიტიანი პროგრამა.

ზოგიერთ შემთხვევაში ეს პროგრამა ეკიდება. ასეთ დროს, რეკომენდირებულია მხოლოდ 1 პროცესორის მიცემა და 3D acceleration ის გათიშვა ვირტუალური მანქანის დისპლეისთვის.

Ubuntu-ს ვირტუალური მანქანის შექმნა

Ubuntu Linux-ის გადმოწერა და მისი Virtual Box-ზე დაყენება შემდეგი ოფიციალური დოკუმენტაციის მიხედვით უნდა გააკეთოთ: `https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview`

ვირტუალურ მანქანას მინიმუმ 6GB ოპერატიული მეხსიერება დაუყენეთ.

გაითვალისწინეთ, რომ Ubuntu ყენდება iso ფაილიდან, რომლის ზომა 5 გიგაბაიტამდეა. დაყენების პროცესი შემდეგნაირია. ჯერ იქმნება ახალი Ubuntu მანქანა და ოპტიკური დისკით ხდება გადმოწერილი iso ფაილის მიწოდება. როცა მანქანა ჩაირთვება დაიწყება მისი ოპერაციული სისტემის ინსტალაცია iso ფაილიდან. ამ დროს ფაილი უნდა ჩაიტვირთოს ოპერატიულ მეხსიერებაში, რაც მოითხოვს დიდ რესურსს. თუ თქვენს კომპიუტერს ოპერატიული მეხსიერება არ ყოფნის, სისტემის დაყენება რაღაც ეტაპზე გაიჭედება.

ოპერაციული სისტემის დაყენების შემდეგ, ეკრანის ზომა იქნება მცირე. ეკრანის ზომის გასაზრდელად შემდეგი მოქმედებებია საჭირო:

1. გაუშვით ბრძანება: `sudo apt install linux-headers-$(uname -r) build-essential dkms`. თუ არ გაქვთ root-ის უფლებები `su root` ბრძანებით ისარგებლეთ.

ზოგჯერ ვირტუალურ გარემოში დაყენებულ ubuntu-ზე ტერმინალი არ ეშვება. თუ თქვენს შემთხვევაშიც ასე მოხდა, უნდა შეცვალოთ ubuntu-ს ენა. ამისთვის შედით მენიუში (settings -> Language and Region) და English (United States) შეცვალეთ English (United KIngdom)-ით, გამოდით და თავიდან შედით სისტემაში.

2. ვირტუალურ მანქანაში ჩადეთ guest additions CD (შემდეგი მენიუს დახმარებით Device -> Insert guest additions CD image) და გაუშვათ სათანადო სკრიპტი.

3. გადატვირთეთ ვირტუალური მანქანა.

ვირტუალური მანქანისთვის გარე ლოკალურ ქსელზე წვდომის მიცემა

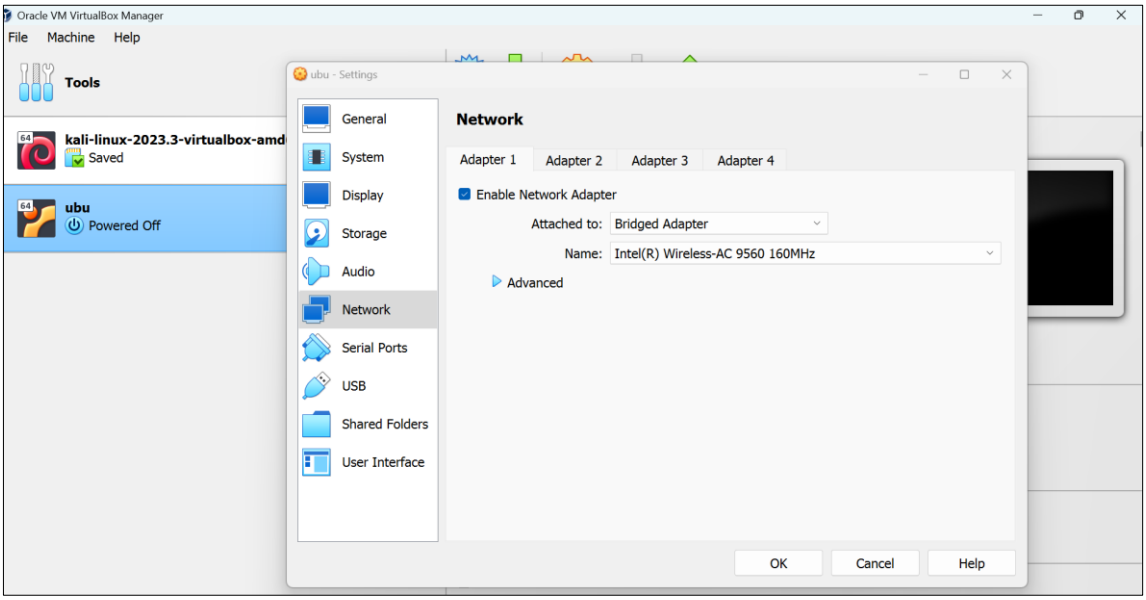
ზოგჯერ საჭიროა, რომ ჩვენს ვირტუალურ მანქანას გარე ლოკალურ ქსელზე ჰქონდეს წვდომა.

ასეთ შემთხვევაში Bridged Networking ინტერფეისით უნდა ვისარგებლოთ. ეს ინტერფეისი თქვენს ვირტუალურ მანქანს საშუალებას მისცემს, რომ იქონიოს გარე LAN ინტერფეისი და ჰქონდეს მინიჭებული IP მისამართი.

გაუშვით VirtualBox და დარწმუნდით, რომ თქვენი ვირტუალური მანქანა დამორთულია.

შედით თქვენი ვირტუალური მანქანის პარამეტრებში (Settings) და აირჩიეთ ქსელის მენიუ (Network).

გამოჩნდება "Adapter 1" თავისი პარამეტრებით. ჩამოსაშლელ მენიუში "Bridged Adapter" აირჩიეთ. "Name"-ს ჩამოსაშლელ მენიუში აირჩიეთ ფიზიკური ადაპტერი რომელიც გსურთ რომ იყოს საზიარო ფიზიკურსა და ვირტუალურ კომპიუტერს შორის. როგორ წესი, ეს შეიძლება იყოს T Wi-Fi ან Ethernet ადაპტერი. "Advanced" სექციის მორგებაც შეგიძლიათ საკუთარ სურვილებზე, თუმცა, რაც უკვე მითითებულია მუშაობს უმეტეს შემთხვევებში.



დაასრულეთ პროცესი "OK" ღილაკზე დაჭერით და ჩართეთ ვირტუალური მანქანა.

ამის შემდეგ თქვენს ვირტუალურ მანქანას გაუჩნდება პირდაპირი წვდომა ლოკალურ ქსელზე. რუთერი მას მიანიჭებს IP ნომერს და შესაძლებელი გახდება სხვა კომპიუტერებთან და ინტერნეტთან კავშირი.

გაითვალისწინეთ, რომ ვირტუალური მანქანას პარამეტრებში მითითებული უნდა ჰქონდეს რომ IP მისამართი აიღოს რუთერიდან. თუ ხელით გაწერთ IP მისამართს, დარწმუნდით, რომ იგივე ქსელის მისამართია, რომელშიც იგი ჩართული აღმოჩნდა.

ქსელში ჩართვის გადასამოწმებლად `ifconfig` ან `ip a` ბრძანებით უნდა ისარგებლოთ. ეკრანზე უნდა იხილოთ IP მისამართი, რომელიც თქვენი ლოკალური ქსელის მისამართების ინტერვალს შეესაბამება.

ბოლო შტრიხები

განაახლეთ Kali Linux და Ubuntu ვირტუალურ მანქანები `sudo apt update` და `sudo apt upgrade` ბრძანებების გამოყენებით.

აიღეთ ყველა ვირტუალური მანქანის ასლი (snapshot). ეს გამოგვადგება მანქანის აღსადგენად დაზიანების შემთხვევაში.