

MODUL PRAKTIKUM 2022

KEAMANAN SISTEM INFORMASI

MODUL 1

Virtualization &
Computer Security

ASISTEN

Ananda Anggie Nur Aini	ENJI
Andi Sayid Muhammad Qoyyum	ANDI
Arya Bimo Bagas Penggalih	BIMO
Faris Aufar Putra	PTRA
Farras Naim	RAAS
Fie Alfain Nuril Haque	ALFA
Fitria Nikmatul Hidayah	WPIN
M. Alwi Zein	ZEIN
Maulana Malik Ibrahim	IBRA
Milenia Ari Oktaviana	ARII
Muhammad Hafiz Hawarizmi	VISS
Muliya Dewi	MYDE
Ni Made Meliana Listyawati	MELI
Nurul Annisaa	NASA
Rizal Indera	INRA
Ryan Supriadi Ramadhan	RYAN
Syarah Tazkiatun Nupus	AZKI
Wiratama Putra Prakosa	RAKO

I. Tujuan Praktikum

- 1.1 Praktikan dapat mengetahui dan memahami konsep Hypervisor
- 1.2 Praktikan mampu memahami tentang malware, trojan, dan ransomware

II. Alat dan Bahan

- 2.1 PC/Laptop
- 2.2 ISO Windows 8.1 Pro
- 2.3 ISO Windows Server 2012 R2
- 2.4 VMWare Workstation 15.5
- 2.5 Angry IP Scanner
- 2.6 PuTTY
- 2.7 Flashdisk

III. Landasan Teori

3.1 Hypervisor

3.1.1 Definisi Hypervisor

Hypervisor adalah sebuah teknik virtualisasi yang memungkinkan beberapa operating system untuk berjalan bersamaan pada sebuah host. Dikatakan teknik virtualisasi karena OS yang ada bukanlah sebuah OS yang sesungguhnya, hanya sebuah virtual machine saja. Tugas dari hypervisor adalah untuk mengatur setiap operating system tersebut sesuai dengan gilirannya agar tidak mengganggu satu dengan yang lainnya. Terkadang, hypervisor juga disebut sebagai Virtual Machine Management (VMM), sesuai dengan tugasnya dalam mengatur beberapa virtual machine.

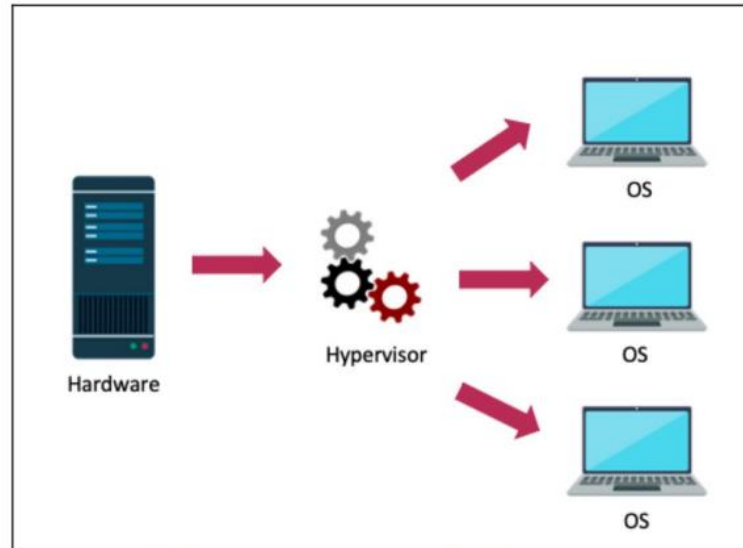
Pada setiap jenis komputer, seperti cluster computing, grid computing, PC ataupun mainframe, memiliki OS yang berbeda satu sama lain karena memiliki sistem yang juga berbeda. Setiap OS tersebut didesain sesuai dengan kebutuhan dari sistem masing-masing. Untuk hypervisor sendiri, didesain lebih mirip OS untuk mainframe dari pada Windows OS. Hal ini dikarenakan sebuah hypervisor, harus bisa mengatur beberapa sistem sekaligus, layaknya sebuah host melayani beberapa client pada mainframe.

3.1.2 Jenis - jenis Hypervisor

Secara umum Hypervisor dibagi menjadi 2 jenis, yaitu sebagai berikut:

1. Native (Baramental) Architecture (Hypervisor Tipe1)

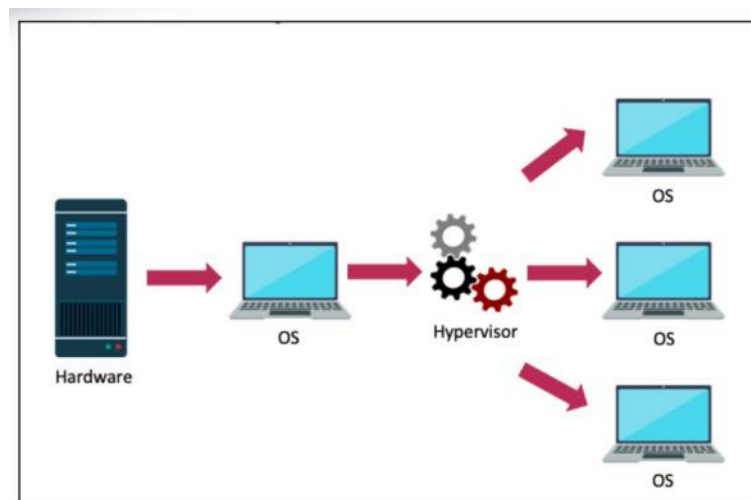
Hypervisor asli berjalan langsung di mesin host, dan berbagi sumber daya keluar (seperti memori dan perangkat) antara mesin tamu. Contoh hypervisor tipe 1 adalah VMware ESX/ESXi, Microsoft Hyper-V, Oracle VM, dan KernelBased Virtual Machine (KVM).



Gambar 3.1 Native (Baremetal) Architecture

2. Hosted Architecture (Hypervisor Tipe 2)

Hypervisor yang ada pada host dijalankan sebagai aplikasi di dalam suatu sistem operasi, dan mendukung mesin virtual yang berjalan sebagai proses individu. Hypervisor tipe 2 adalah VMware Server, VMware Workstation/Player, Virtual Box, dan Parallels Desktop.



Gambar 3.2 Hosted Architecture

3.1.3 Jenis Software Hypervisor

Ada berbagai macam software hypervisor, diantaranya yaitu:

1. VMware Workstation

VMware Workstation merupakan software virtual machine yang memungkinkan user untuk dapat menjalankan satu atau lebih operating system dalam waktu yang bersamaan tanpa mengganggu data yang ada pada operating system utama. VMware Workstation memiliki beberapa keunggulan, yaitu:

1. Dapat melakukan backup data dalam skala besar
2. Dapat melakukan screen capture
3. Dapat melakukan penggunaan aplikasi berat pada OS bayangan
4. Full virtualisasi
5. Memungkinkan untuk 64 bit
6. Support DAS, USB, SSD for swap, RDM, dll.

2. Microsoft Hyper-V

Hyper-V adalah sebuah role yang ada di Windows Server 2008 R2. Menyediakan tools dan services yang bisa digunakan untuk membuat sebuah server virtualisasi. Virtualisasi ini bisa digunakan bermacam-macam pencapaian bisnis untuk meningkatkan efisiensi dan mengurangi pengeluaran. Virtualisasi ini sangat bermanfaat karena kita bisa membuat dan memanagemen virtual machines, dimana kita bisa menjalankan banyak sistem operasi pada satu komputer dan menutup sistem operasi tersebut dengan yang lainnya. Hyper-V disebut virtualisasi berbasis Hypervisor. Hypervisor bisa disebut perangkat lunak atau firmware yang membuat mesin virtual.

Keunggulan Microsoft Hyper-V antara lain:

1. Membuat VM yang dapat menggunakan SMP (symmetric multiprocessing) untuk mengakses dua, empat, atau delapan core pada processor
2. Membuat VM yang dapat menggunakan lebih dari 1 TB physical memory

3. Memiliki tools untuk melakukan migrasi virtual server workload ke virtualisasi Windows Server
4. Membuat dan mengatur child partisi untuk operating system (32-bit dan 64-bit)

3. Kernel-Based Virtual Machine (KVM)

Kernel-Based Virtual Machine (KVM) adalah salah satu teknologi virtualisasi (hypervisor) yang dikembangkan oleh Linux. KVM merupakan sebuah solusi untuk melakukan virtualisasi pada Linux dengan perangkat keras type x86 (64-bit). KVM diimplementasikan sebagai modul kernel loadable yang mengubah kernel Linux menjadi bare metal hypervisor. Ada dua prinsip desain utama yang diadopsi oleh KVM dengan tujuan agar KVM menjadi hypervisor dengan kinerja tinggi dan melampaui opensource hypervisors lainnya.

Keunggulan Kernel-Based Virtual Machine (KVM) antara lain:

1. Mampu merancang solusi hypervisor yang optimal
2. KVM tidak perlu mengimplementasikan fitur yang telah disediakan oleh perangkat keras

3.2 Malware, Trojan, Ransomware

3.2.1 Malware

Malware (Malicious Software) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

Malware dapat menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data/informasi. Hal yang pada umumnya terjadi penyebab malware adalah mengunduh software dari tempat ilegal yang disisipkan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit,

spyware, adware yang tidak jujur, serta software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

1. Computer Viruses

Computer viruses adalah program yang dirancang untuk mereplikasi dan menyebar di antara komputer, biasanya dilakukan dengan cara "menginfeksi" aplikasi yang dapat dieksekusi atau kode program tertentu. Ada beberapa jenis virus yang diklasifikasikan berdasarkan cara virus tersebut menginfeksi komputer, yaitu sebagai berikut:

1. Boot sector viruses, virus ini menyerang informasi sektor boot, tabel partisi, dan terkadang sistem file.
2. Program viruses, berupa urutan kode yang dapat memasukkan diri mereka ke dalam program yang dapat dieksekusi. Ketika aplikasi dijalankan, kode virus menjadi aktif.
3. Script viruses, sebagian besar target dari script viruses ini yaitu memanfaatkan kelemahan pada interpreter. Interpreter yaitu semacam software yang mampu mengeksekusi kode program lalu menerjemahkannya ke dalam bahasa mesin, sehingga mesin dapat melakukan instruksi sesuai dengan apa yang diminta.
4. Macro viruses, jenis virus ini biasanya memengaruhi dokumen Microsoft Office.
5. Multipartite viruses, virus ini menggunakan sektor boot dan metode propagasi atau penyebaran dalam menginfeksi suatu file yang dapat dieksekusi.

2. Worm

Worm adalah virus yang biasanya bertempat pada memori yang dapat mereplikasi sumber daya jaringan. Worm biasanya menargetkan semacam kerentanan dalam aplikasi jaringan, mengkonsumsi bandwidth jaringan secara berlebih. Worm juga dapat merusak sistem operasi atau aplikasi server seperti melakukan serangan Denial of Service.

3. Logic Bomb

Beberapa virus tidak terpicu secara otomatis, seperti logic bomb yang merupakan salah satu jenis malware yang menjalankan fungsinya pada sebuah rentang waktu tertentu. Seperti bom yang memiliki rentang waktu tertentu untuk meledak. Logic bomb baru akan aktif pada rentang waktu tertentu sesuai dengan waktu atau tanggal yang telah dikonfigurasi sebelumnya.

3.2.2 Trojan



Gambar 3.3 Trojan Horse

Trojan Horse atau yang lebih dikenal dengan Trojan adalah salah satu tipe virus atau malware yang menyerang komputer dengan menyamar sebagai salah satu software. Virus Trojan sering digunakan oleh pencuri cyber dan hacker untuk mendapatkan akses ke perangkat yang telah terinfeksi oleh virus ini. Virus ini sering menyamar sebagai sebuah software atau file yang berguna bagi user, dapat membantu user dan kadang menyamar sebagai sebuah software atau file yang bersifat menghibur user sehingga user tidak merasa bahwa perangkatnya sudah terserang virus ini.

Trojan tidak memiliki kemampuan untuk menggandakan diri seperti virus komputer lainnya, tetapi Trojan mampu membantu virus lain untuk masuk menginfeksi sebuah perangkat karena fungsinya yang bisa memberi akses kepada pemberi Trojan tersebut. Hal yang membedakan trojan dengan malware lainnya seperti virus atau worm, yaitu sebagai berikut:

1. Trojan memiliki sifat stealth dalam operasinya dan seringkali berbentuk menyerupai program tersebut tidak berbahaya, sementara virus atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem mengalami crash
2. Trojan dapat dikendalikan dari jauh oleh attacker
3. Trojan mempunyai kemampuan untuk mengirimkan alamat IP korban ke attacker, misalnya melalui media ICQ (I Seek You) atau pun IRC (Internet Relay Chat)

3.2.3 Ransomware

Ransomware adalah salah satu jenis malware yang bertujuan untuk meminta tebusan kepada korban. Ransomware, sesuai dengan namanya, ransom = tebusan (dalam bahasa Inggris), jenis malware ini bertujuan untuk memeras korban yang komputernya terinfeksi ransomware dengan meminta sejumlah uang sebagai tebusan. Bagi yang sering berselancar di internet, tentu akan sering bertemu dengan malware ransomware. Karena biasanya, malware ini muncul saat kita mengunduh suatu file atau mengunjungi website tertentu. Terlebih link website yang kurang aman untuk dikunjungi.

Secara umum ada dua jenis ransomware, yaitu sebagai berikut:

1. Locker Ransomware (Non- Enkripsi)

Locker Ransomware menginfeksi korban dengan menutup akses (lockscreen) ke dalam resources yang ada di komputernya. Setelah layar terkunci, pelaku akan meminta sejumlah tebusan kepada korban, agar hak akses korban dapat diberikan kembali.

2. Crypto Ransomware (Enkripsi)

Crypto Ransomware merupakan jenis yang paling digunakan oleh pelaku kejahatan siber. Crypto Ransomware akan mengenkripsi file- file penting dalam komputer, lalu pelaku akan meminta uang tebusan untuk mendapatkan kunci deskripsinya.

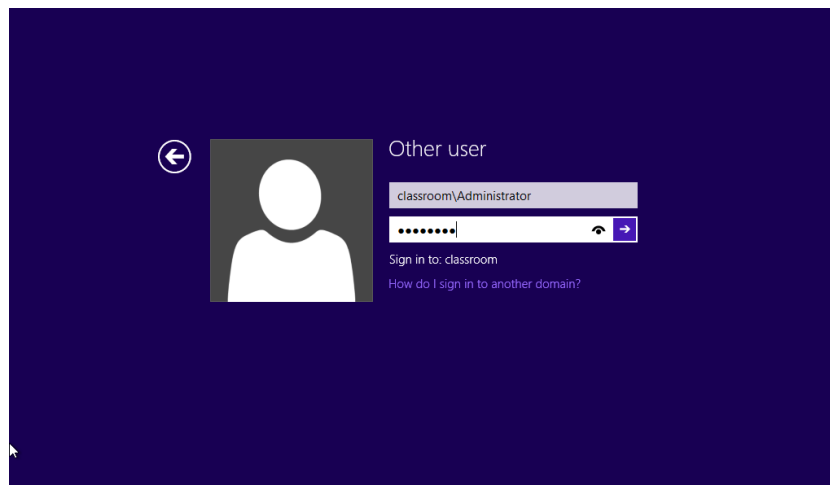
IV. Lab Praktik

4.1 Trojan and Malware protection

4.1.1 Mengaktifkan Trojan

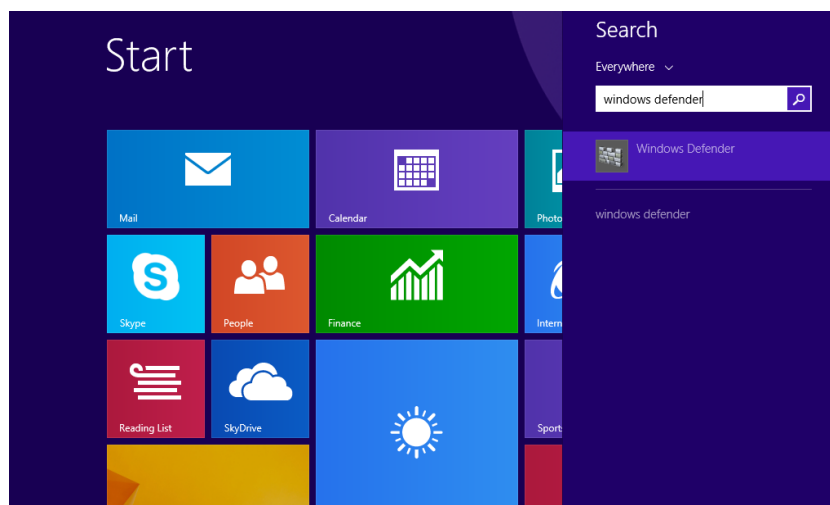
Pada Lab Praktik ini, **VM ROGUE** mencoba melakukan sebuah eksploitasi terhadap *trojan* yang sudah dijalankan oleh **VM CLIENT**.

1. Jalankan **VM Client** dan klik **Other user**, *login* menggunakan *username* “classroom\Administrator” dan *password* “Pa\$\$w0rd”.



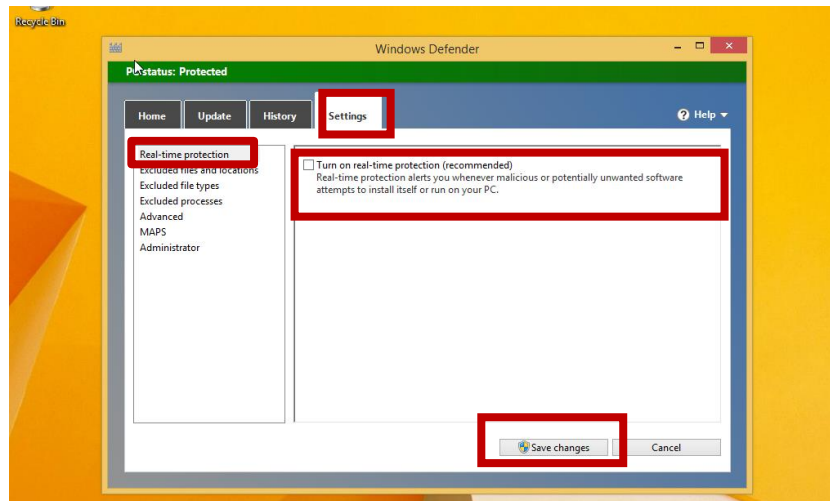
Gambar 4.1 VM Client

2. Buka **Windows Defender**.



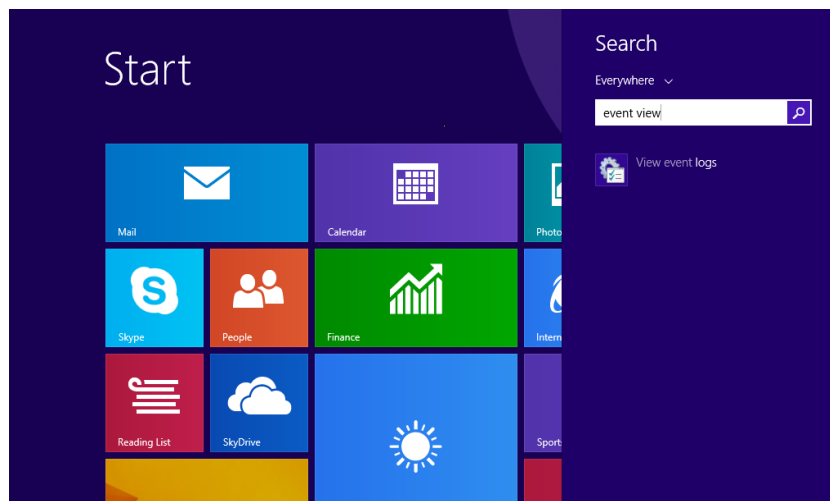
Gambar 4.2 Windows Defender

3. Pada **Windows Defender**, matikan fitur *real-time protection* yang bisa diakses pada tab *Settings* > *Real Time Protection* > *Unchecklist "Turn On Real Time Protection"* > *Save Changes*.



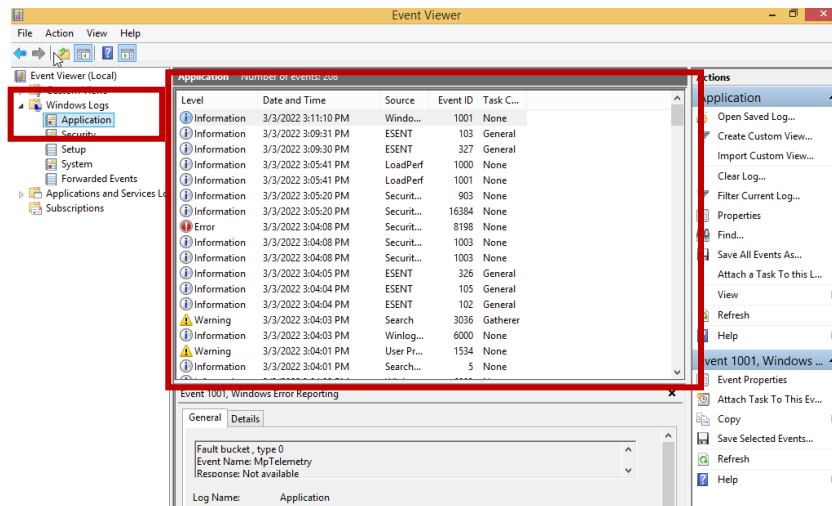
Gambar 4.3 Windows Defender

4. Buka **Event Viewer** untuk melihat kondisi aktivitas awal yang terjadi pada **VM CLIENT**.



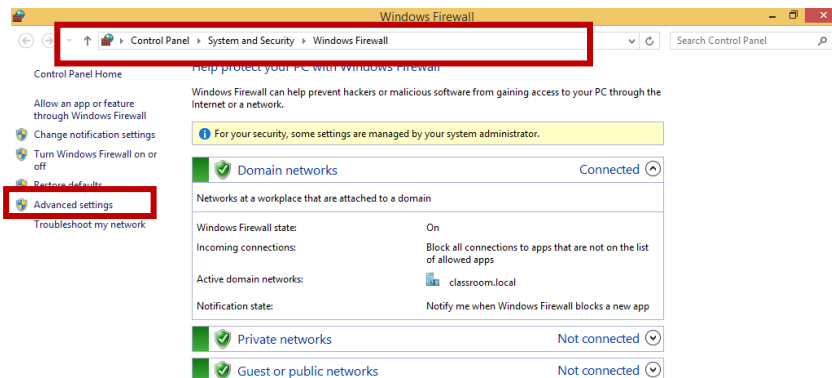
Gambar 4.4 Event Viewer

5. Pada **Event Viewer**, buka **Windows Logs**, lalu klik **Application**. Perhatikan event logs yang ada, tidak ditemukan adanya sesuatu yang mencurigakan.



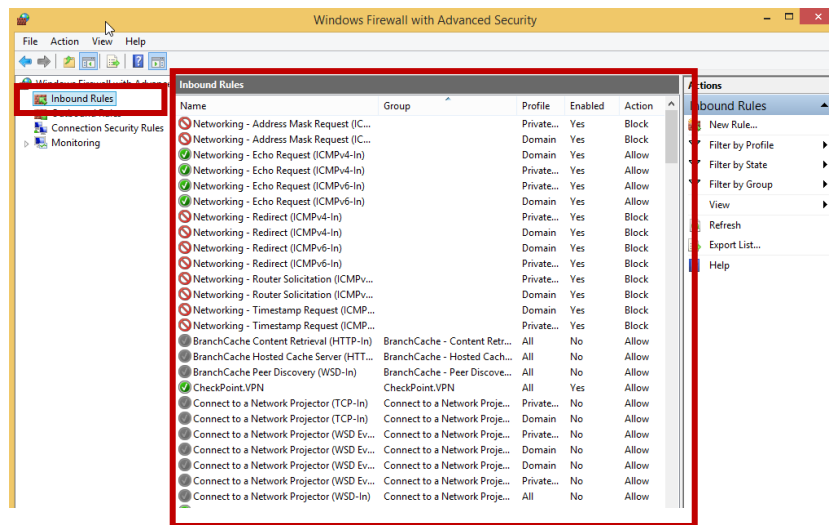
Gambar 4.5 Windows Logs

6. Selanjutnya buka **Windows Firewall**, lalu klik *Advanced settings*.



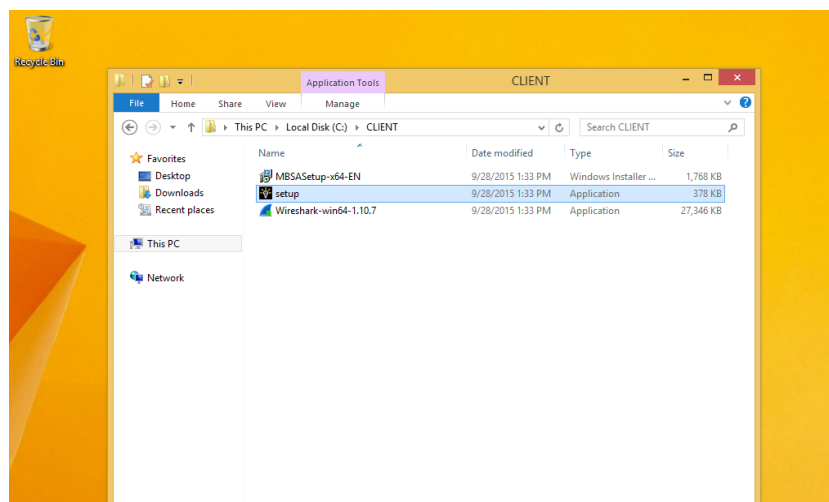
Gambar 4.6 Windows Firewall

7. Klik **Inbound Rules**, perhatikan *Information Rules*. Belum terdapat sesuatu yang mencurigakan.



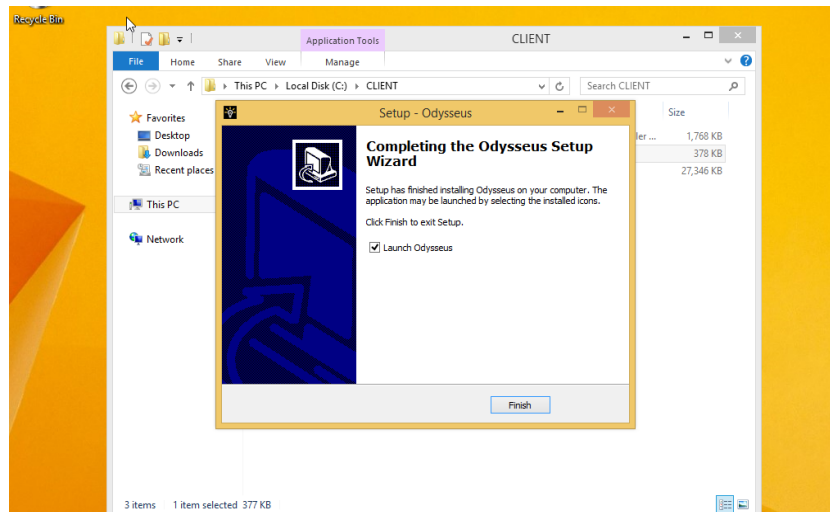
Gambar 4.7 Inbound Rules

8. Selanjutnya, buka direktori **CLIENT** pada *drive C:* dan jalankan **setup.exe**.



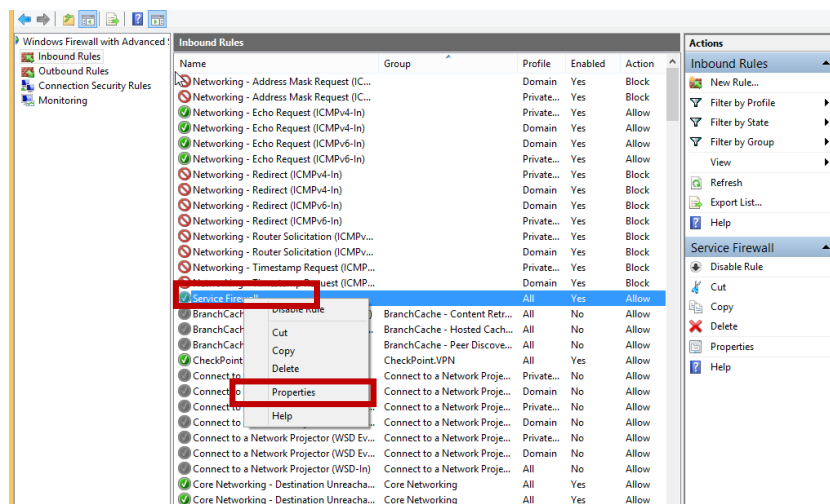
Gambar 4.8 Direktori Client

9. Ikuti langkah instalasi hingga selesai seperti menginstal aplikasi pada umumnya dengan menekan tombol *next* hingga **Finish**.



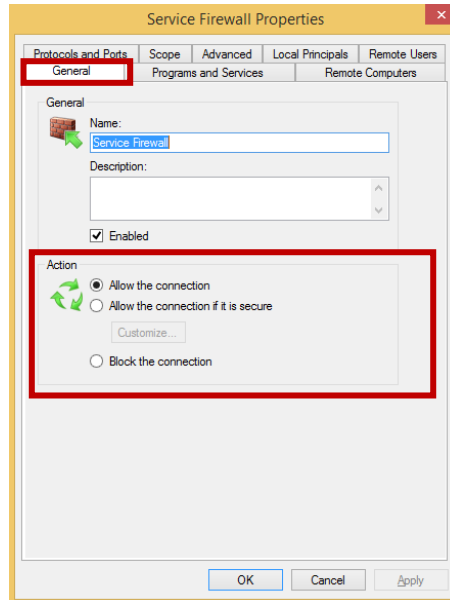
Gambar 4.9 Instalasi

10. Kembali ke jendela **Windows Firewall**; **Inbound Rules**, setelah dicek terlihat sebuah rule baru yang diizinkan yaitu **“Service Firewall”**. Lakukan pemeriksaan lebih lanjut dengan melihat *Properties* dari *rule* dengan klik kanan pada *rule* tersebut.



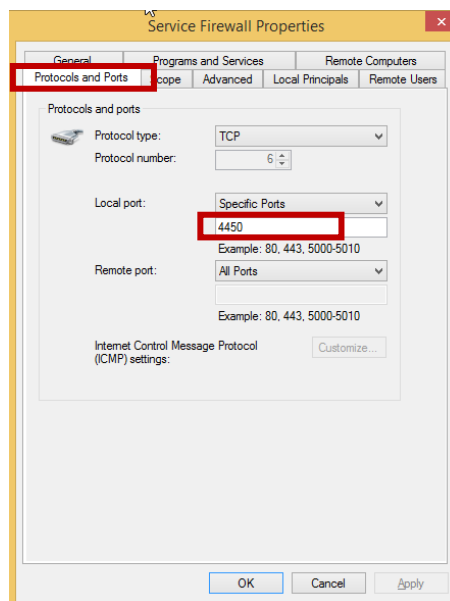
Gambar 4.10 Windows Firewall

11. Pada jendela *Properties* terlihat pada tab **General** bagian *Action* terpilih **Allow the connection** yang membuat rule dapat mengizinkan koneksi melewati *firewall*.



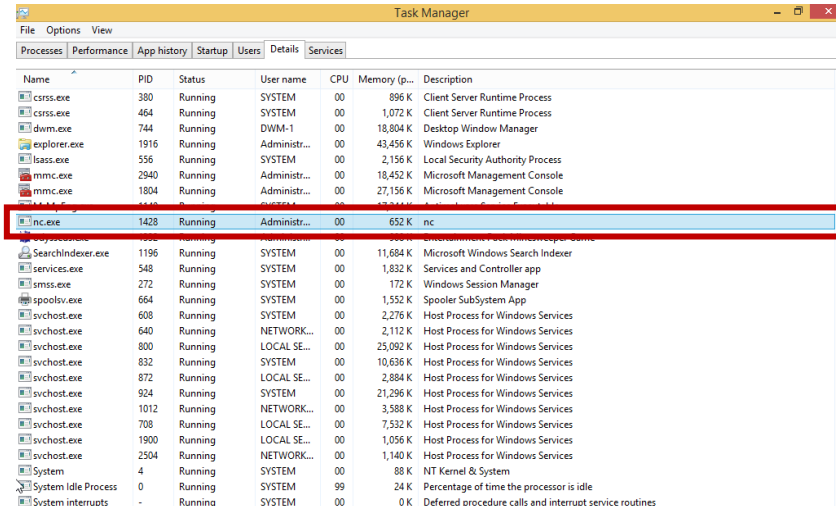
Gambar 4.11 Koneksi Firewall

12. Selanjutnya pada tab ***Protocols and Ports***, terlihat bahwa *port* yang digunakan adalah 4450.



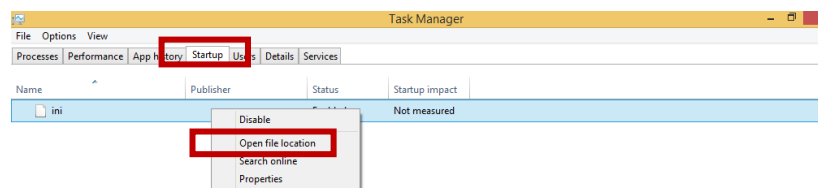
Gambar 4.12 Protocols and Ports

13. Buka *Task Manager* lalu masuk ke tab **Details**, dan terlihat terdapat proses **nc.exe** yang mencurigakan karena tidak memiliki deskripsi proses yang jelas.



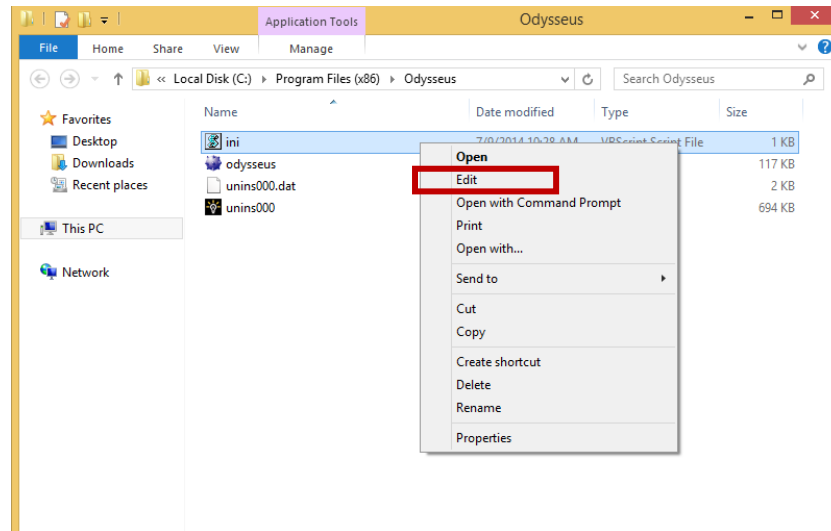
Gambar 4.13 Task Manager

14. Pindah pada tab **Startup**. Terdapat program bernama “ini”, lalu klik kanan pada “ini” dan pilih **Open file location**. Setelah masuk ke lokasi dari *file* tersebut, klik kanan pada *file*, pilih **Edit**.



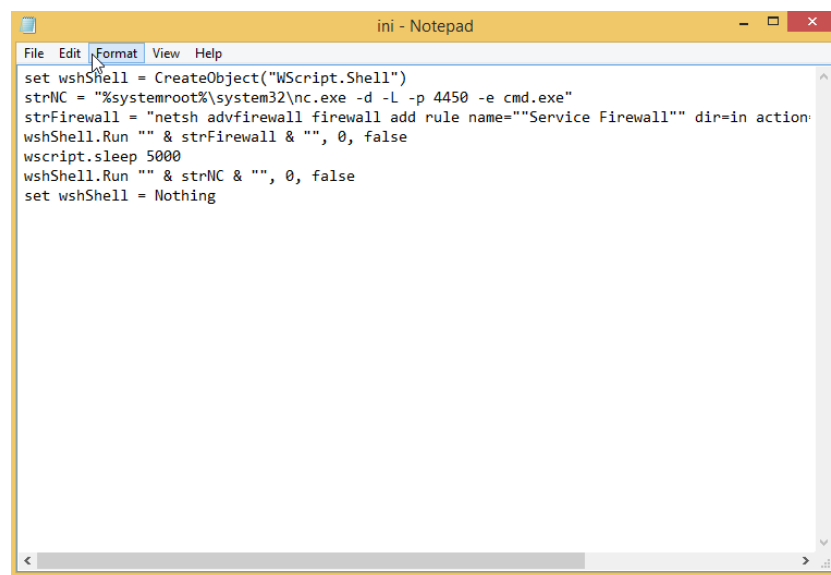
Gambar 4.14 Tab Startup

15. Setelah masuk ke lokasi dari *file* tersebut, klik kanan pada *file*, pilih **Edit**.



Gambar 4.15 File

16. Ketika **VM CLIENT** melakukan instalasi dan menjalankan program **Odysseus**, **VM CLIENT** juga tanpa disadari menjalankan sebuah *script* yang mengaktifkan *backdoor* dengan cara membuat *rule* bernama **“Service Firewall”** yang mengizinkan akses ke *port* 4450 pada **VM CLIENT**. *Script* tersebut adalah *file* bernama “ini” seperti gambar di bawah.

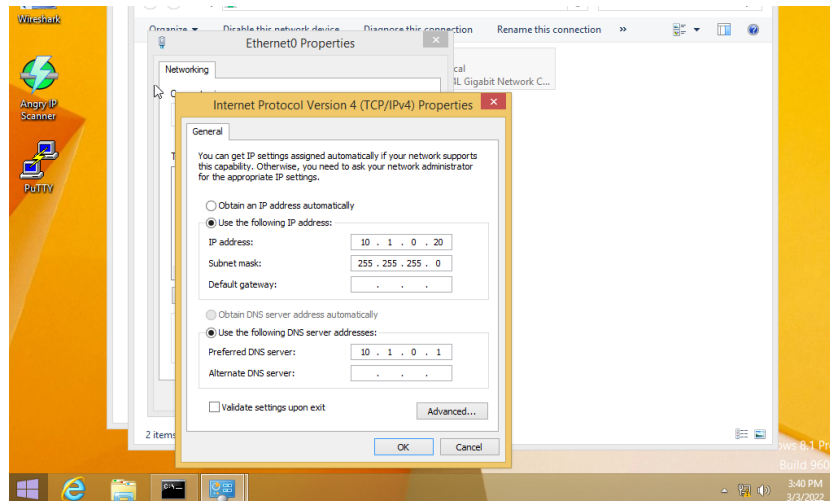


Gambar 4.16 Script

4.1.2 Mengeksploitasi Trojan

Pada skenario ini, **VM ROGUE** mencoba melakukan sebuah eksploitasi terhadap *trojan* yang sudah dijalankan oleh **VM CLIENT**.

1. Jalankan **VM ROGUE**, konfigurasi IP *address* seperti gambar di bawah.



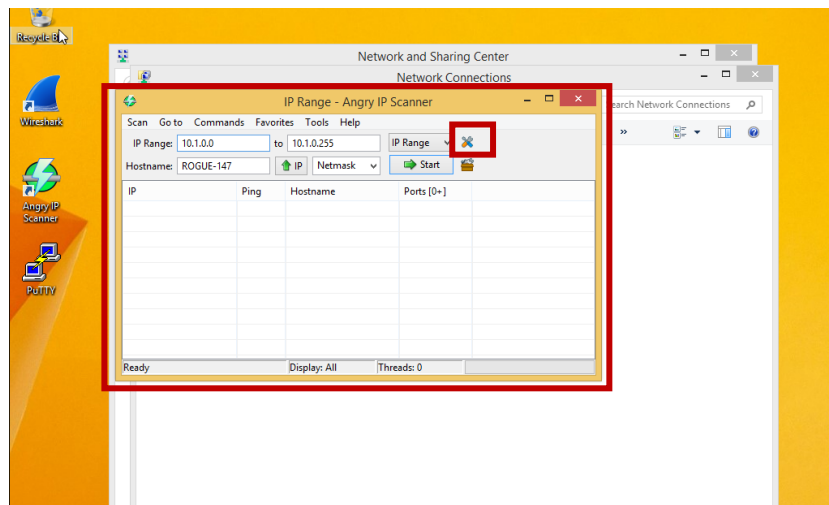
Gambar 4.17 Konfigurasi IP Address

2. Buka dan jalankan aplikasi **Angry IP Scanner**.



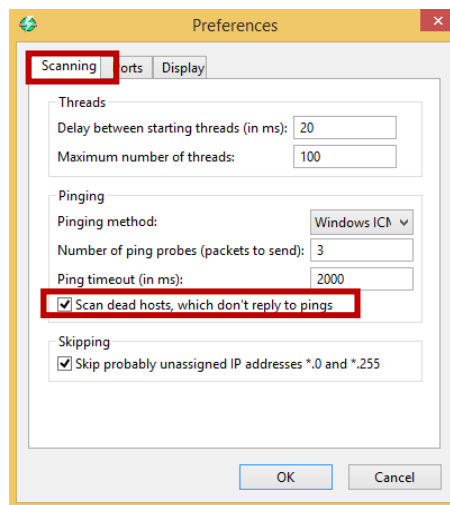
Gambar 4.18 Angry IP Scanner

3. Lalu klik *Preferences*.



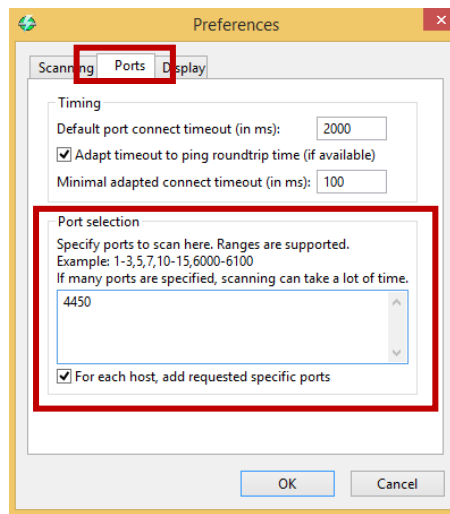
Gambar 4.19 IP range

4. Buka tab *Scanning*, beri tanda centang pada opsi “*Scan dead hosts...*”.



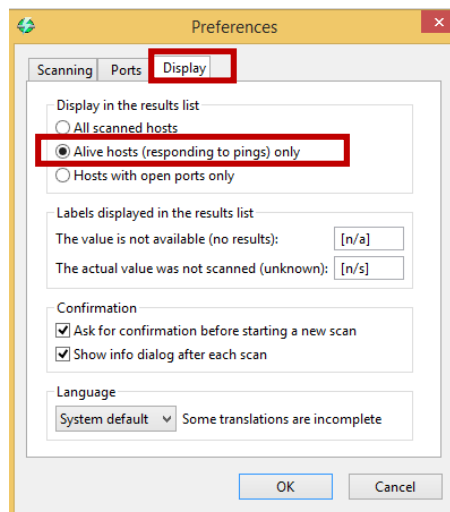
Gambar 4.20 Scanning

5. Selanjutnya buka tab **Ports**, masukkan port 4450 pada *Port selection*.



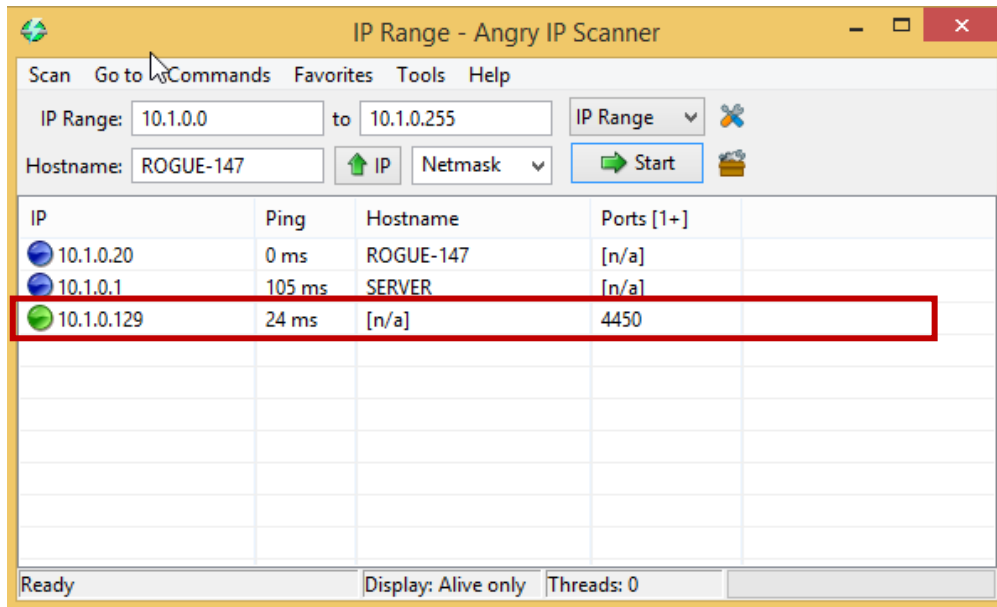
Gambar 4.21 Ports

6. Pindah ke tab **Display**, pada bagian “*Display in the result list*”, pilih “*Alive hosts*”.
Lalu klik OK.



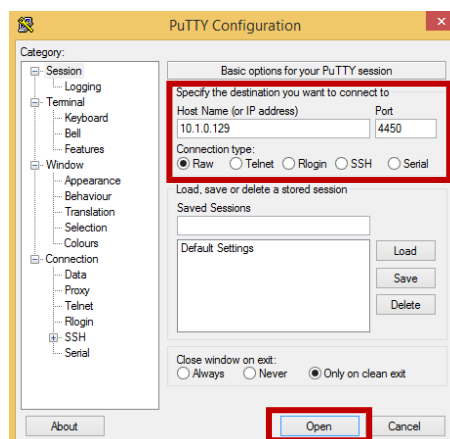
Gambar 4.22 Display

7. Lakukan *scan* pada *range* alamat IP **10.1.0.0 - 10.1.0.255**, lalu klik **Start**. Terdapat tiga hasil *scanning*, di mana dua hasil memiliki *hostname* namun tidak berwarna hijau karena *port* 4450 tidak terbuka. Pada IP **VM CLIENT** terdapat *port* terbuka yaitu 4450, sehingga dapat diasumsikan hasil tersebut merupakan **VM CLIENT**.



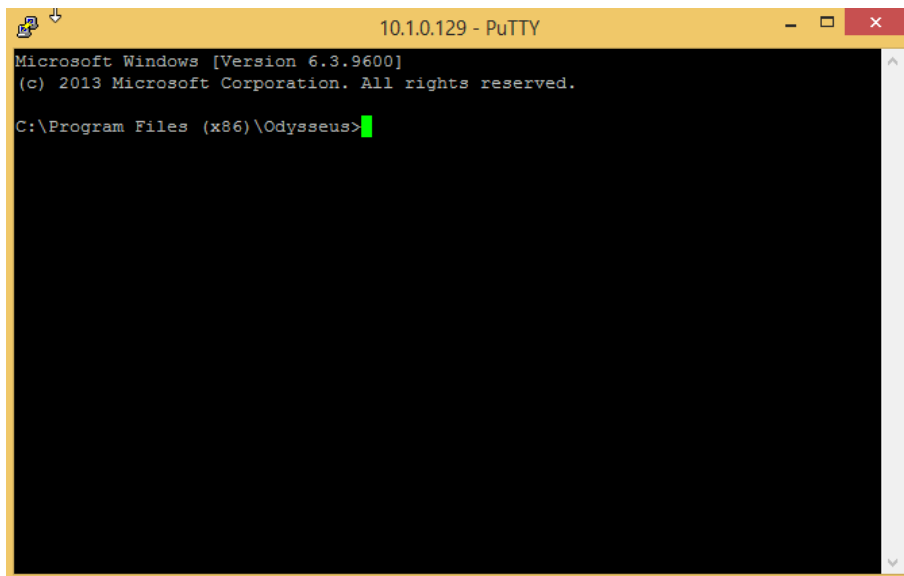
Gambar 4.23 Scan Range

8. Selanjutnya, lakukan *remote access* pada **VM CLIENT** dengan menggunakan PuTTY. Jalankan PuTTY dan masukkan alamat IP dari **VM CLIENT** dengan *port* 4450 dan pilih *connection type* “**Raw**”, lalu klik **Open**.



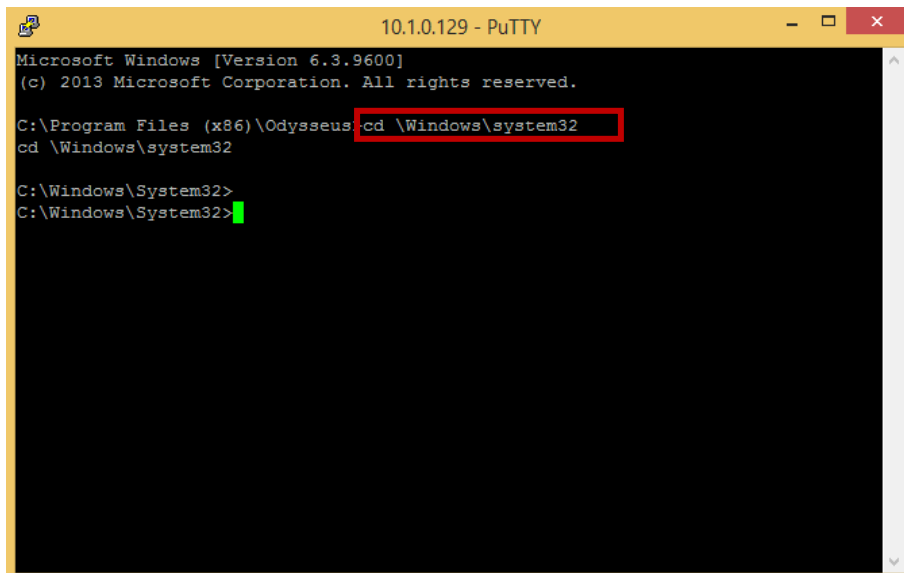
Gambar 4.24 Remote Access PuTTY

9. Jika berhasil masuk **VM CLIENT** maka akan seperti gambar di bawah.



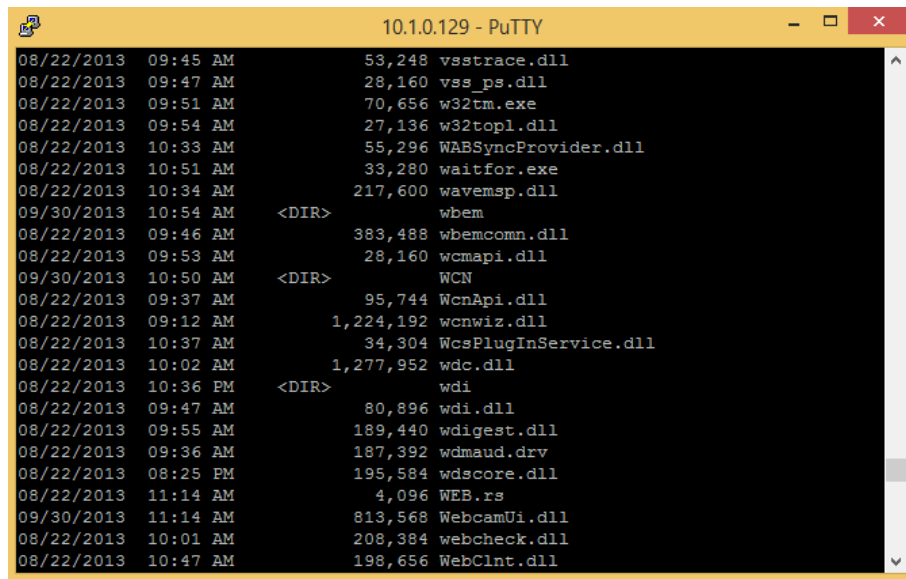
Gambar 4.25 VM CLIENT

10. Selanjutnya, pindah ke direktori lain dengan *command* :
`cd \Windows\system32`



Gambar 4.26 Command Direktori

11. Lalu jalankan command: `dir` untuk melihat isi direktori tersebut.



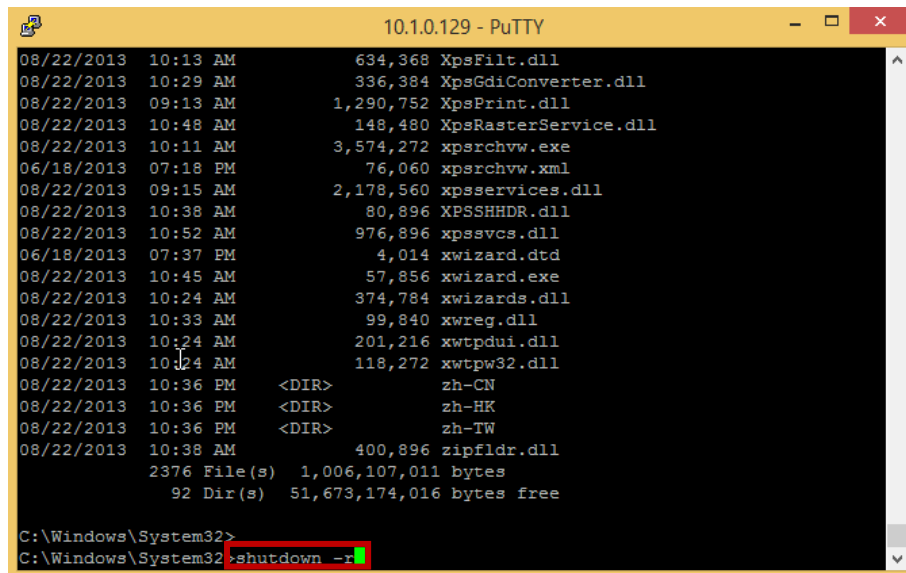
```

08/22/2013 09:45 AM          53,248 vsstrace.dll
08/22/2013 09:47 AM          28,160 vss_ps.dll
08/22/2013 09:51 AM          70,656 w32tm.exe
08/22/2013 09:54 AM          27,136 w32topl.dll
08/22/2013 10:33 AM          55,296 WABSyncProvider.dll
08/22/2013 10:51 AM          33,280 waitfor.exe
08/22/2013 10:34 AM          217,600 wavemsp.dll
09/30/2013 10:54 AM          <DIR>          wbem
08/22/2013 09:46 AM          383,488 wbemcomn.dll
08/22/2013 09:53 AM          28,160 wcmapi.dll
09/30/2013 10:50 AM          <DIR>          WCN
08/22/2013 09:37 AM          95,744 WcnApi.dll
08/22/2013 09:12 AM         1,224,192 wcnwiz.dll
08/22/2013 10:37 AM          34,304 WcsPlugInService.dll
08/22/2013 10:02 AM         1,277,952 wdc.dll
08/22/2013 10:36 PM          <DIR>          wdi
08/22/2013 09:47 AM          80,896 wdi.dll
08/22/2013 09:55 AM          189,440 wdigest.dll
08/22/2013 09:36 AM          187,392 wdmaud.drv
08/22/2013 08:25 PM          195,584 wdscore.dll
08/22/2013 11:14 AM           4,096 WEB.rs
09/30/2013 11:14 AM          813,568 WebcamUi.dll
08/22/2013 10:01 AM          208,384 webcheck.dll
08/22/2013 10:47 AM          198,656 WebClnt.dll

```

Gambar 4.27 Command Direktori

12. Masukkan command: `shutdown -r` untuk me-restart **VM CLIENT**. Kemudian kembali ke **VM CLIENT**.



```

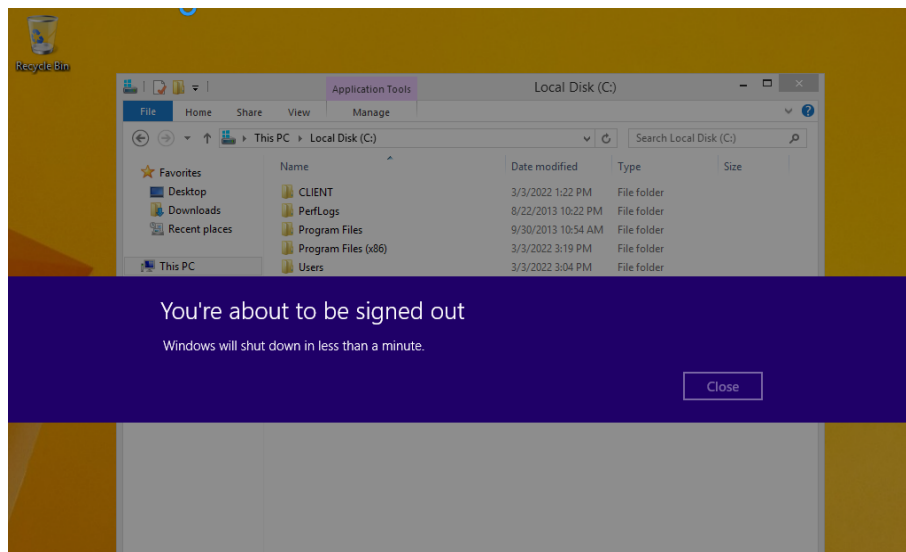
08/22/2013 10:13 AM          634,368 XpsFilt.dll
08/22/2013 10:29 AM          336,384 XpsGdiConverter.dll
08/22/2013 09:13 AM         1,290,752 XpsPrint.dll
08/22/2013 10:48 AM          148,480 XpsRasterService.dll
08/22/2013 10:11 AM          3,574,272 xpsrchvw.exe
06/18/2013 07:18 PM           76,060 xpsrchvw.xml
08/22/2013 09:15 AM          2,178,560 xpsservices.dll
08/22/2013 10:38 AM           80,896 XPSSSHDR.dll
08/22/2013 10:52 AM          976,896 xpsvc.dll
06/18/2013 07:37 PM           4,014 xwizard.dtd
08/22/2013 10:45 AM          57,856 xwizard.exe
08/22/2013 10:24 AM          374,784 xwizards.dll
08/22/2013 10:33 AM           99,840 xwreg.dll
08/22/2013 10:24 AM          201,216 xwtpd.dll
08/22/2013 10:24 AM          118,272 xwtpw32.dll
08/22/2013 10:36 PM          <DIR>          zh-CN
08/22/2013 10:36 PM          <DIR>          zh-HK
08/22/2013 10:36 PM          <DIR>          zh-TW
08/22/2013 10:38 AM          400,896 zipfldr.dll
2376 File(s)  1,006,107,011 bytes
92 Dir(s)    51,673,174,016 bytes free

C:\Windows\System32>
C:\Windows\System32>shutdown -r

```

Gambar 4.28 Command Direktori

13. **VM CLIENT** akan melakukan *restart* secara otomatis, dan koneksi *remote* PuTTY pada **VM ROGUE** akan terputus.

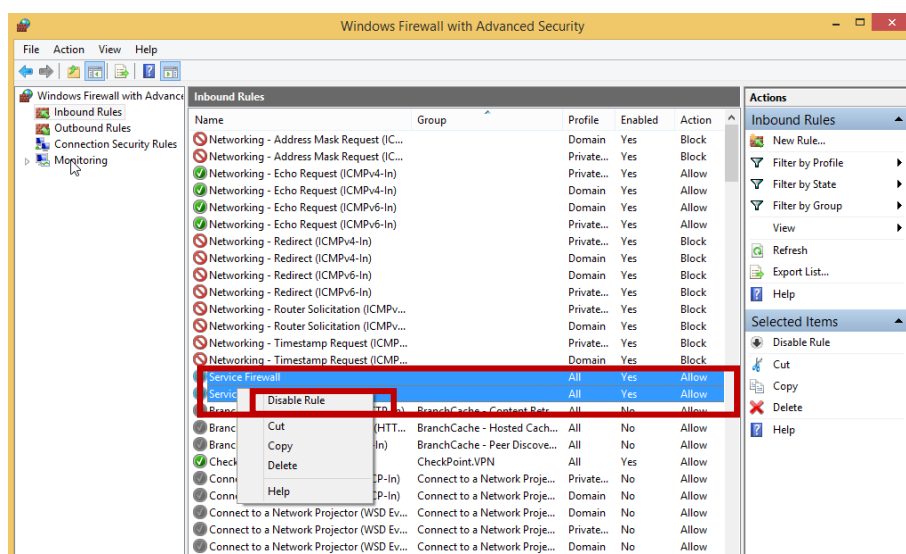


Gambar 4.29 Restart VM CLIENT

4.1.3 Memblokir Trojan

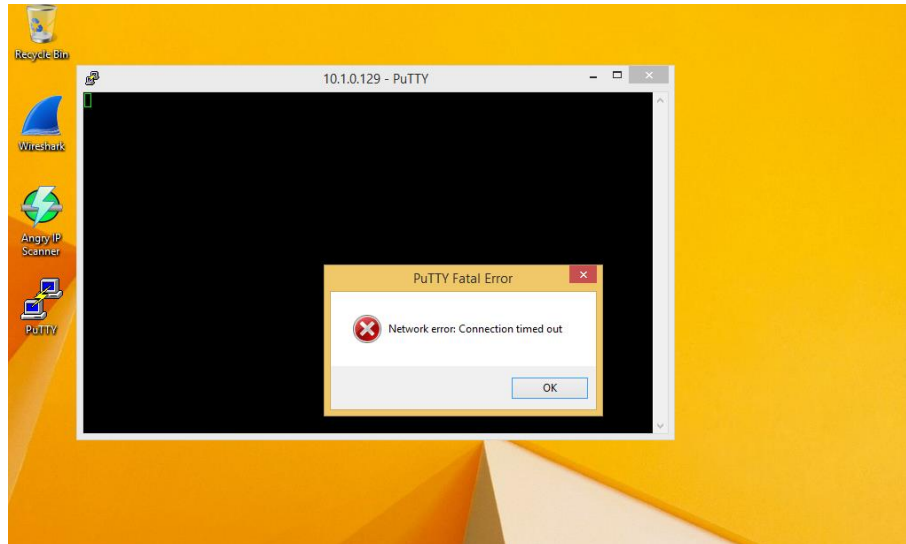
Pada skenario kali ini akan melakukan *blocking* terhadap *trojan* pada **VM CLIENT**.

1. Pada **VM CLIENT**, buka **Windows Firewall**, klik **advanced settings** dan pilih **Inbound Rules**. *Disable* semua *rule* yang bernama “**Service Firewall**” agar tidak ada yang bisa melakukan *remote access* melalui *port* 4450. Lakukan dengan cara klik kanan pada *rule* lalu pilih **Disable Rule**.



Gambar 4.30 Windows Firewall

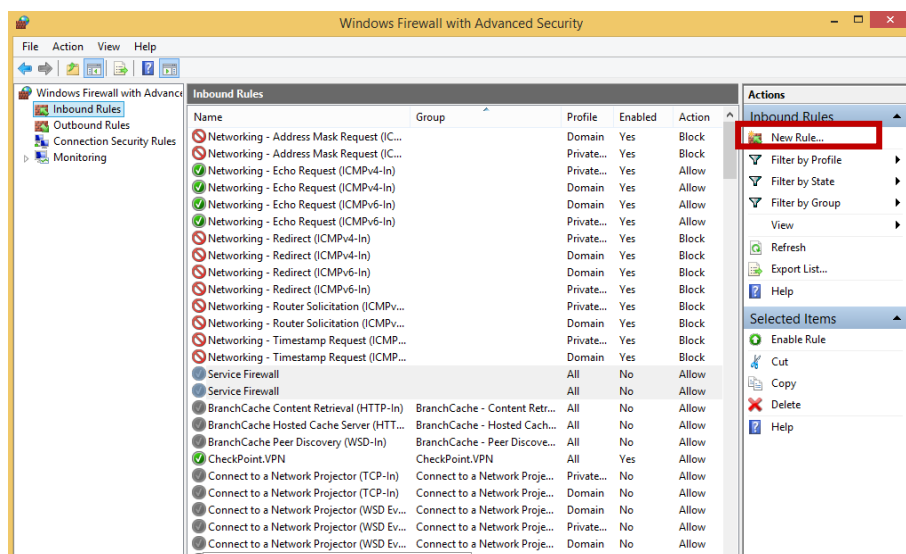
2. Buka **VM ROGUE** dan aplikasi PuTTY. Lakukan *remote access* pada **VM CLIENT**. Maka hasilnya akan *error* karena akses yang diberikan sudah tidak ada (*disabled*).



Gambar 4.31 VM ROGUE

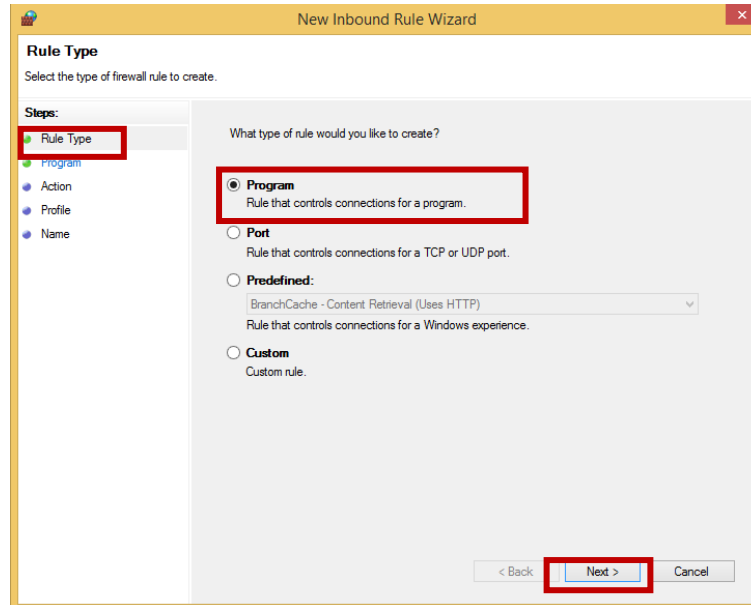
Cara tersebut hanya *temporary*, dikarenakan ketika **VM CLIENT** dimatikan dan dinyalakan kembali maka *rule* “**Service Firewall**” akan muncul kembali dan **VM ROGUE** dapat melakukan eksploitasi (*remote access*) lagi.

3. Selanjutnya, buat sebuah *rule* baru untuk memblokir secara permanen. Pada **Inbound Rules**, klik **New Rule**.



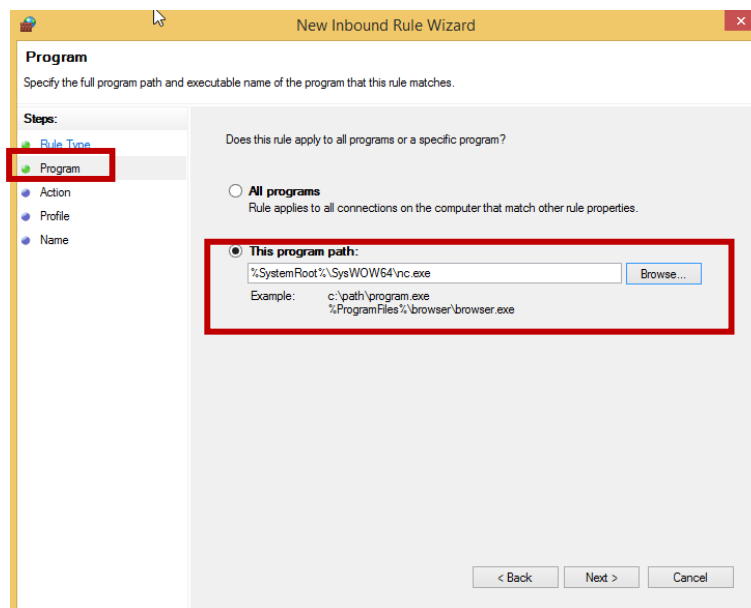
Gambar 4.32 Membuat Rule Baru

4. Pilih Program lalu klik *Next*.



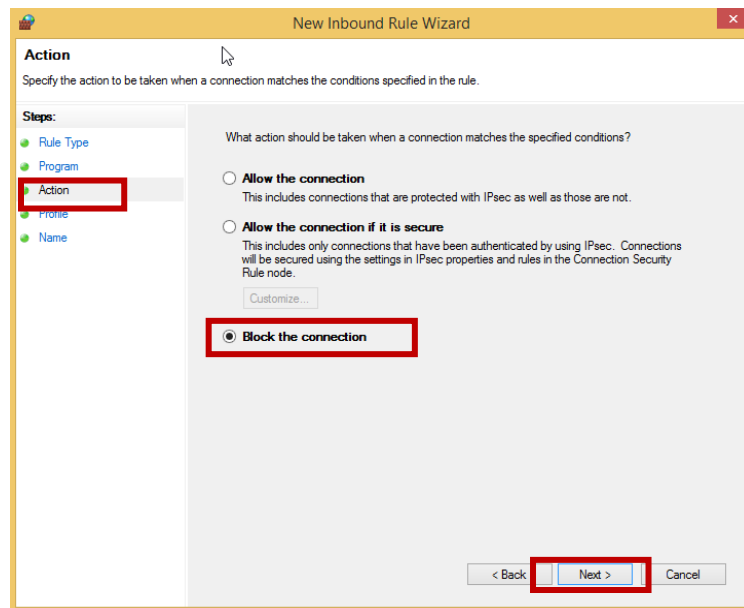
Gambar 4.33 Pilih Program

5. Pilih *this program path* lalu *browse* program **nc.exe** atau isi dengan **C:\Windows\SysWOW64\nc.exe**, lalu klik *Next*.



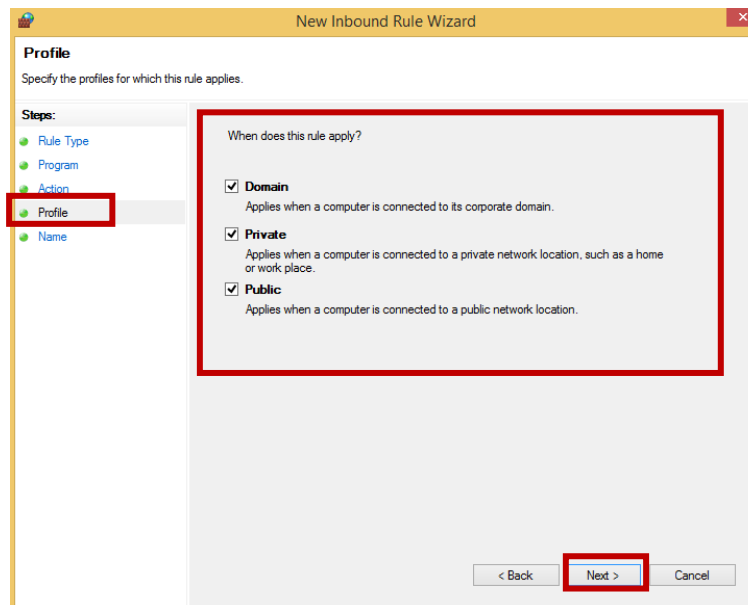
Gambar 4.34 Pilih This Program Path

6. Lalu pilih ***Block the connection***, dan klik ***Next***.



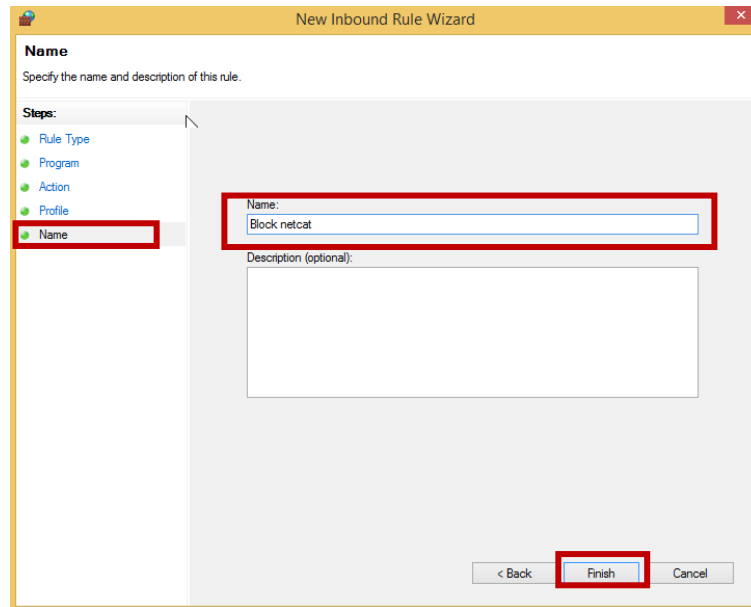
Gambar 4.35 Pilih Block the connection

7. Centang semua pilihan, lalu klik ***Next***.



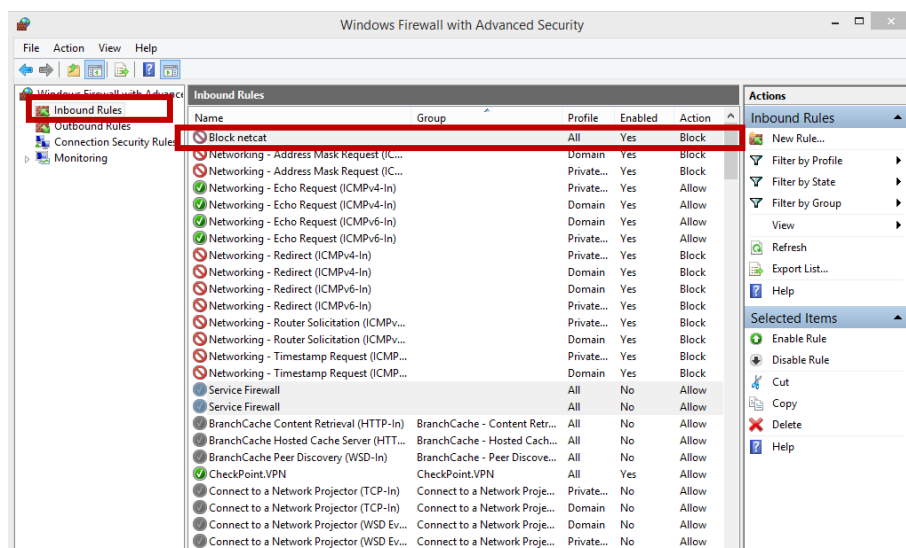
Gambar 4.36 Centang semua pilihan

8. Kemudian pada kolom *Name* beri nama *rule* tersebut dengan nama “**Block Netcat**” dan berikan deskripsi pada kolom *Description*, lalu klik **Finish**.



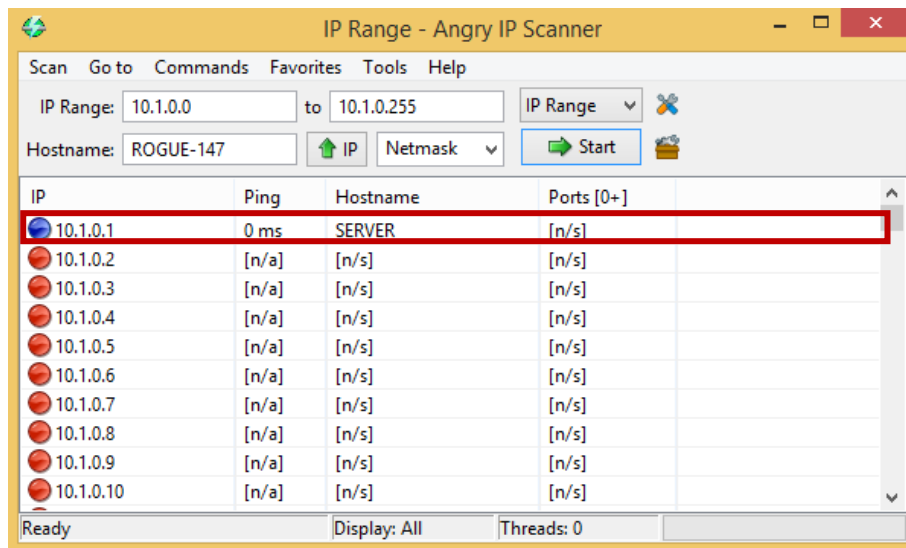
Gambar 4.37 Nama rule

9. Berikut adalah tampilan setelah *rule* dibuat.



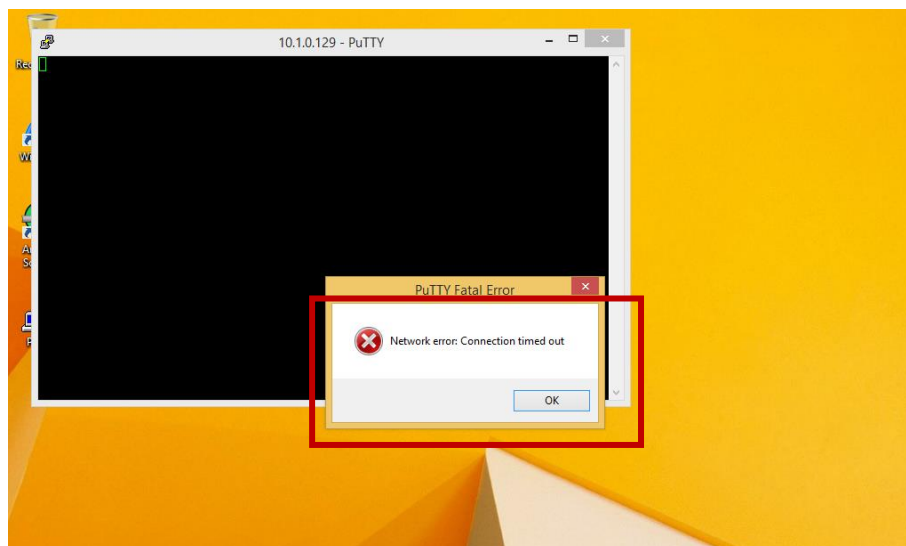
Gambar 4.38 Tampilan setelah rule dibuat

10. Buka kembali **VM ROGUE** dan jalankan aplikasi **Angry IP Scanner**, lakukan *scan* seperti sebelumnya, maka hasilnya tidak ada *port* yang terbuka seperti sebelumnya.



Gambar 4.39 Angry IP Scanner

11. Ketika **VM ROGUE** ingin melakukan eksploitasi kembali terhadap **VM CLIENT** dengan menggunakan **PuTTY** maka hasilnya akan *error* karena akses (*port*) tidak tersedia lagi.

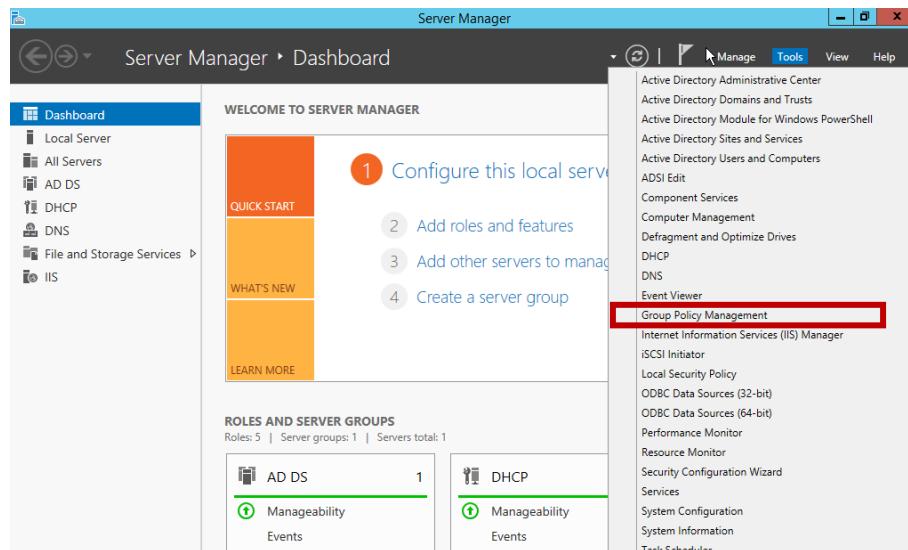


Gambar 4.40 VM CLIENT

4.1.4 Deploying Malware Protection

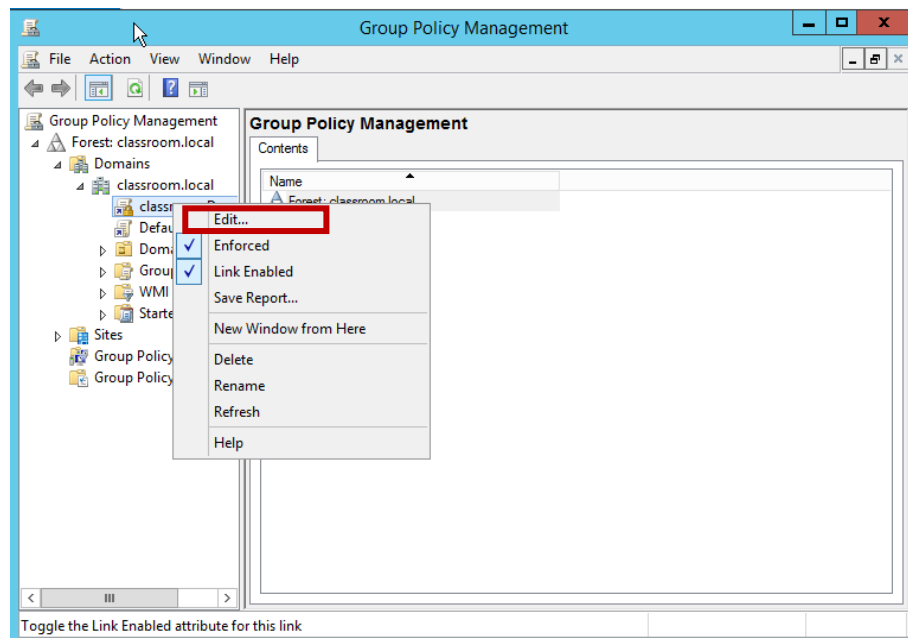
Pada skenario kali ini akan melakukan aktivasi fitur *malware protection* yang ada pada **VM SERVER**.

1. Buka **VM SERVER**, pada Server Manager, klik **Tools > Group Policy Management**.



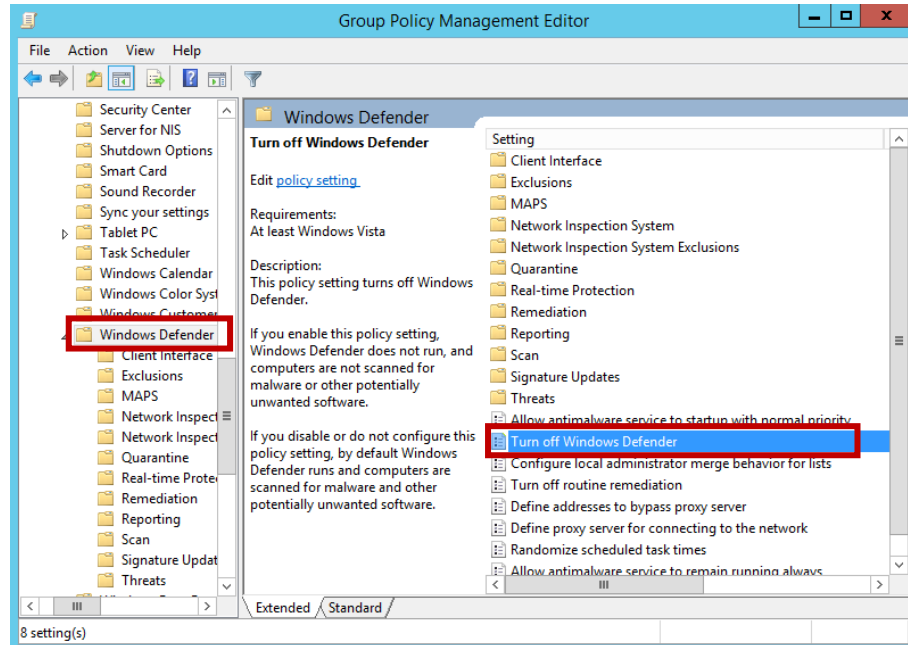
Gambar 4.41 VM SERVER

2. Pada navigation bar di sebelah kiri, buka **Forest: classroom.local > Domains > classroom.local > classroom Domain Policy**, klik kanan > **Edit**.



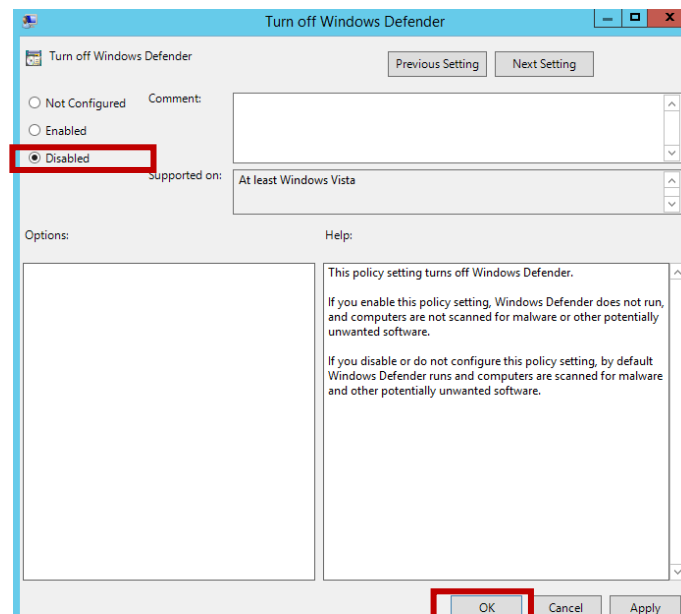
Gambar 4.42 Group Policy Management

3. Pada navigasi sebelah kiri buka **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender**. Lalu pilih dan klik dua kali pada **Turn Off Windows Defender**.



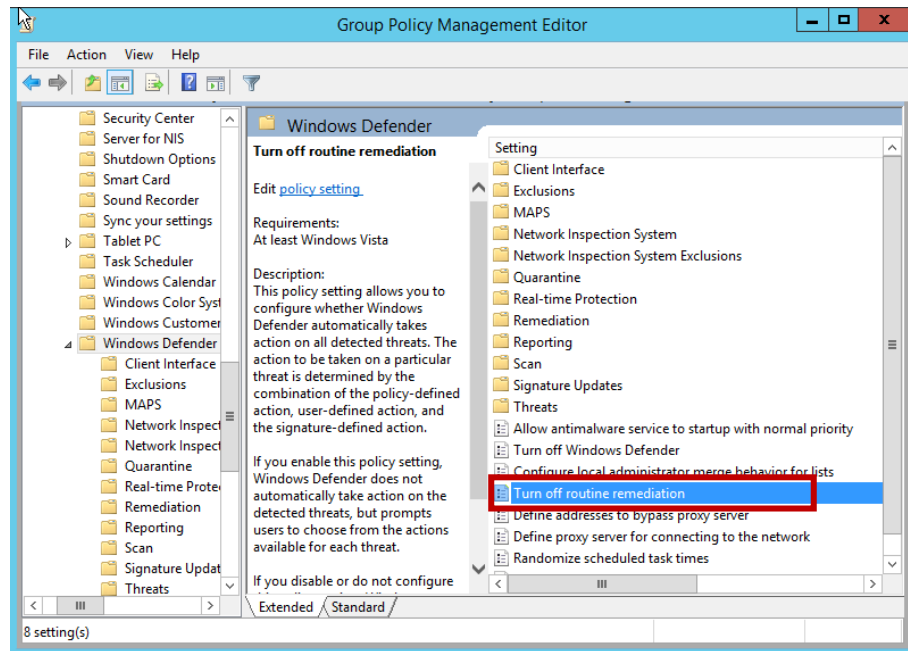
Gambar 4.43 Group Policy Management Editor

4. Pada bagian kiri pilih **Disabled**, lalu klik **OK**.



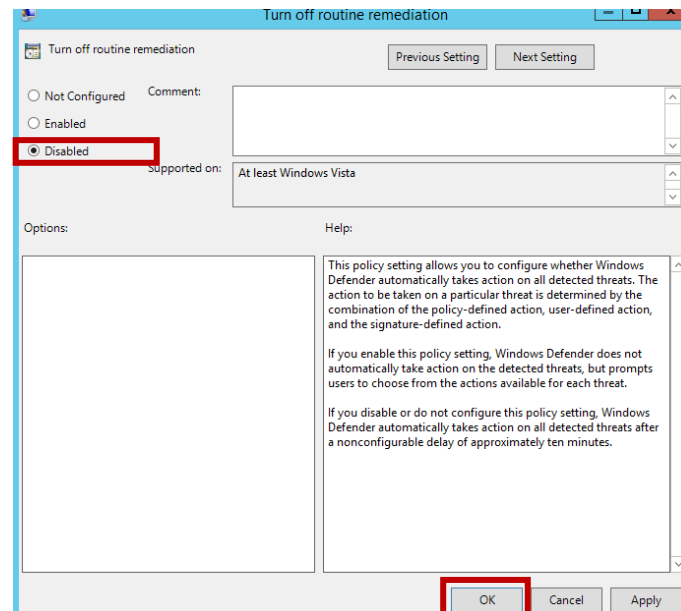
Gambar 4.44 Turn off Windows Defender

5. Selanjutnya pilih **Turn Off Routine Remediation**.



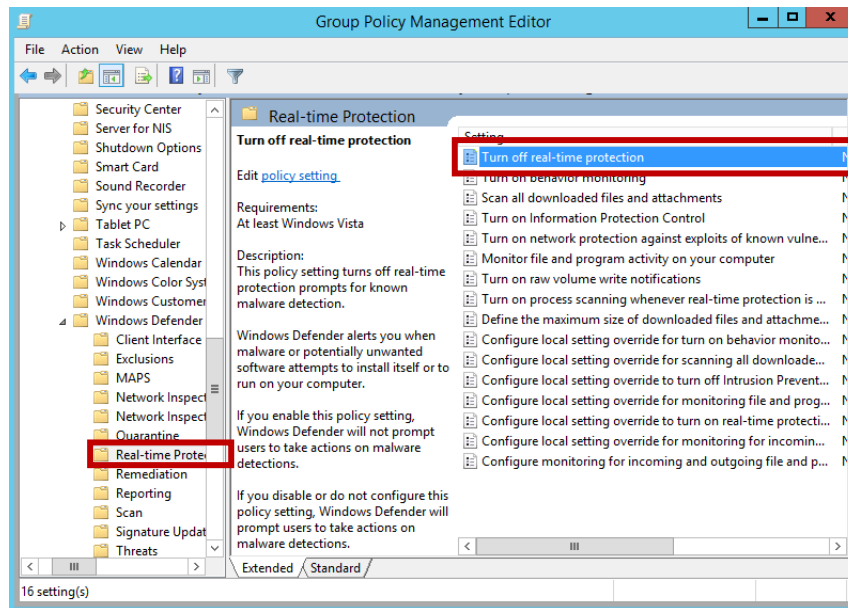
Gambar 4.45 Turn off Routine Remediation

6. Pada bagian kiri pilih **Disabled**, lalu klik **OK**.



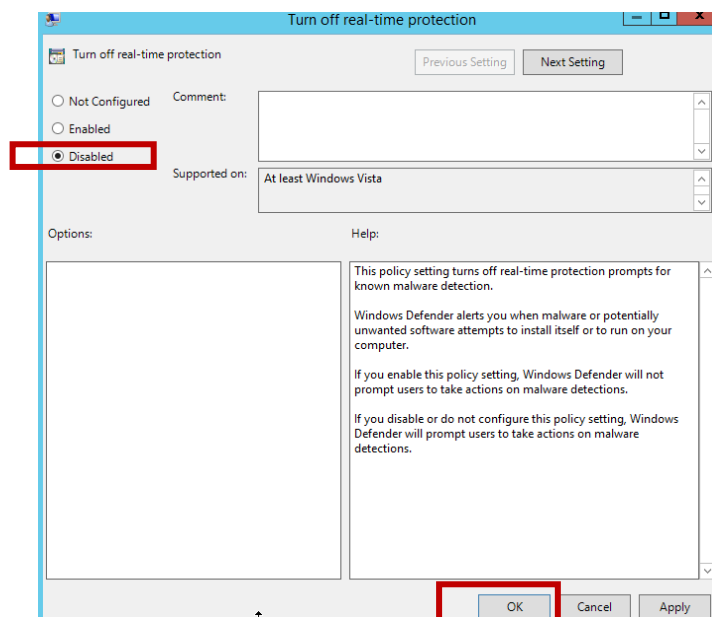
Gambar 4.46 Disabled Routine Remediation

7. Pada *navigation bar* di sebelah kiri klik **Real-time Protection**. Lalu pilih **Turn Off Real-time Protection**.



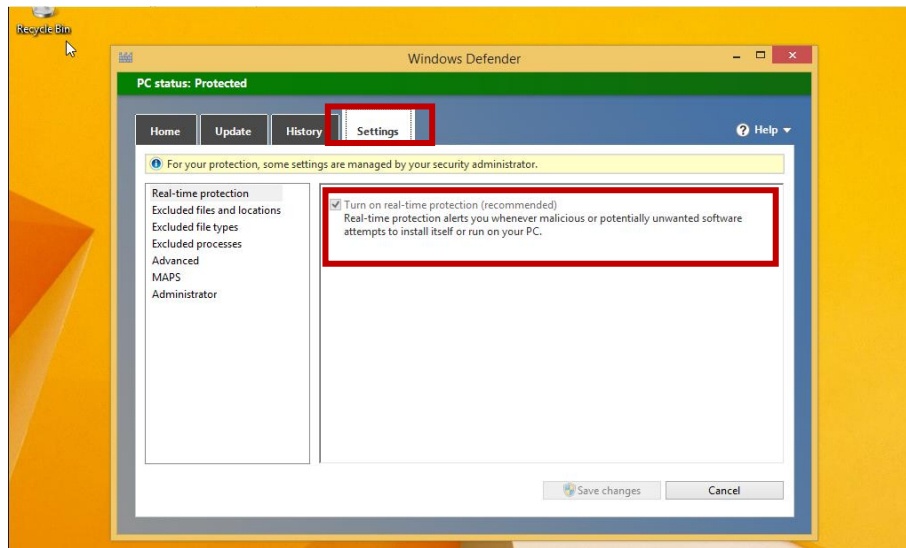
Gambar 4.47 Turn off Real-time Protection

8. Pada bagian kiri pilih **Disabled**, lalu klik **OK**.



Gambar 4.48 Disabled Real-time Protection

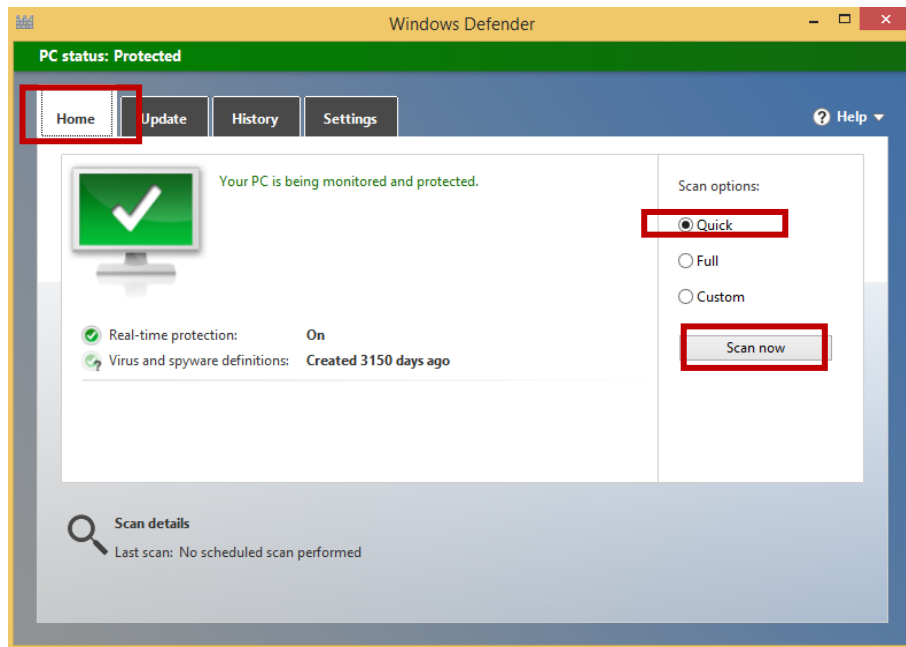
9. Kemudian **restart VM CLIENT**, lalu buka **Windows Defender** pada **VM CLIENT**. Buka **tab Settings**, akan terlihat bahwa **Windows Defender** yang sebelumnya mati sekarang sudah aktif dan tidak dapat dimatikan oleh **VM CLIENT** secara manual tanpa izin Administrator **VM SERVER**.



Gambar 4.49 Restart VM CLIENT

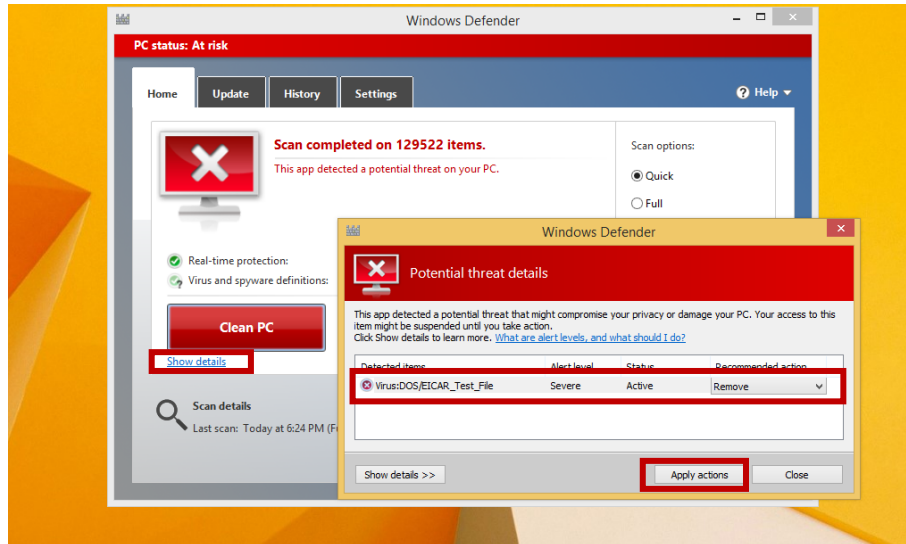
4.1.5 Menggunakan Antivirus

1. Buka **Windows Defender** pada **VM CLIENT**. Pindah ke tab **Home** dan lakukan *quick scan*. Pada bagian kanan *scan options*, pilih **Quick** dan klik **Scan now**.



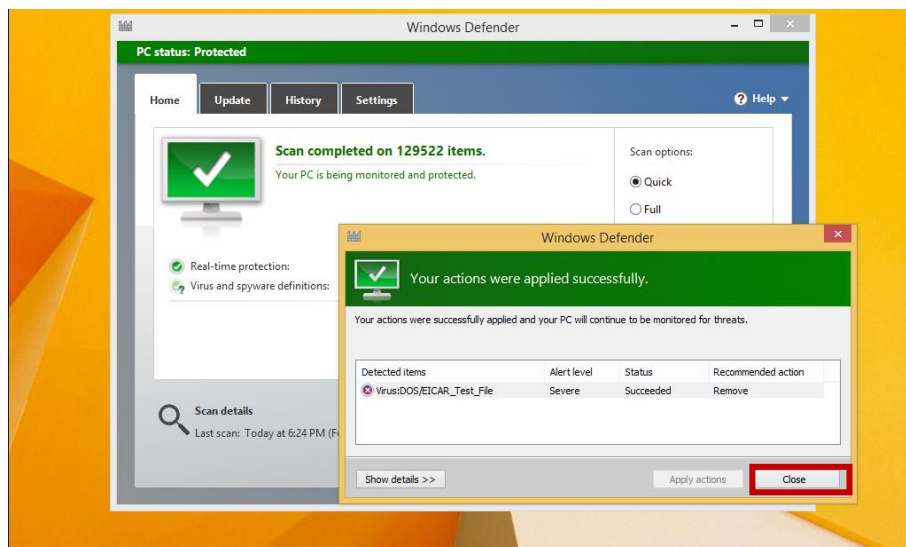
Gambar 4.50 Windows Defender

2. Setelah selesai scan, maka akan ditemukan virus **EICAR_Test_File** yang ter-install bersama trojan saat melakukan instalasi **Odysseus**. Pada kolom *recommendation action* pilih **Remove** lalu klik **Apply actions**.



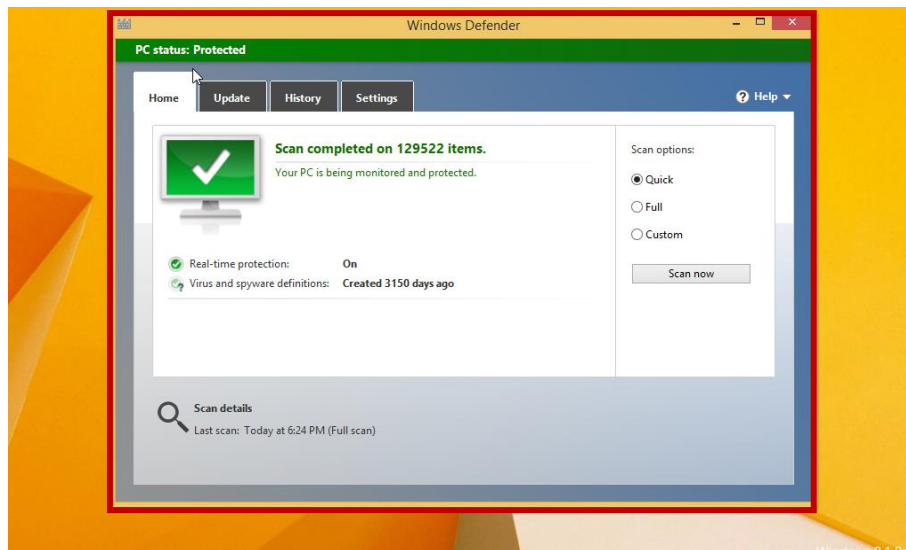
Gambar 4.51 Windows Defender

3. Klik **Close**.



Gambar 4.52 Windows Defender

4. Setelah virus berhasil dihapus maka status akan kembali *protected*.



Gambar 4.53 Windows Defender

V. Daftar Pustaka

1. Laboratorium Sistem Operasi dan Jaringan Komputer. (2021). *Modul Praktikum Keamanan Sistem Informasi 2021*. Bandung, Laboratorium Sistem Operasi dan Jaringan Komputer.