MODUL PRAKTIKUM MALWARE
NJRAT

A. PENDAHULUAN

Remote Access Trojan ini adalah sebuah trojan yang kita buat dan infeksikan ke korban, yang mana setelah trojan berjalan, kita punya hak akses dan kontrol penuh terhadap komputer infeksi tersebut. Tools yang digunakan yaitu njRAT. Aplikasi njRAT ini dulu sangat berjaya ketika Windows XP masih tenar, namun sayang, sekarang ketenarannya sudah mulai berkurang karena sudah banyak antivirus yang dapat mengenalinya. Bahkan si trojan untuk melakukan RAT nya ketika diupload ke virustotal.com, hanya 4 antivirus yang tidak menganggapnya sebagai sebuah trojan. Dibuat menggunakan bahasa pemrograman berbasis .NET sehingga bagi pengguna Windows XP, ada kemungkinan trojan ini tidak dapat dijalankan karena dibutuhkannya .NET framework. Biasanya pengguna njRAT akan menjual akun korban yang terinfeksi trojan hingga menjual generator trojan dan tutorial penggunaannya. Oke, gambar dibawah ini tampilan ketika njRAT pertama kali diaktifkan. Jangan lupa untuk mendisable antivirus dan firewall.

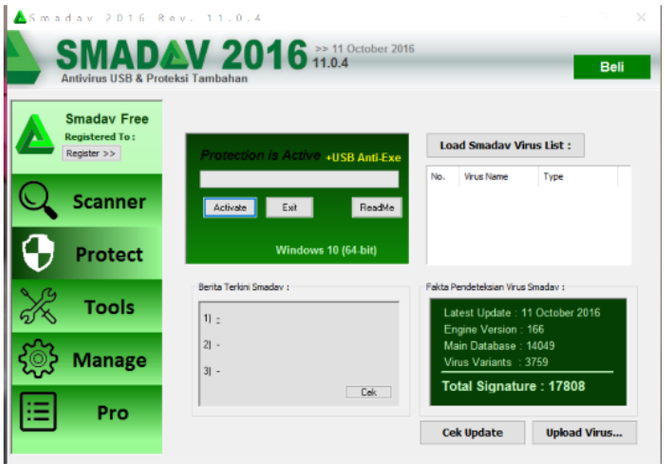
NjRAT adalah salah satu tools hacking untuk OS windows yang digunakan untuk meremote pc satu dengan pc lain.

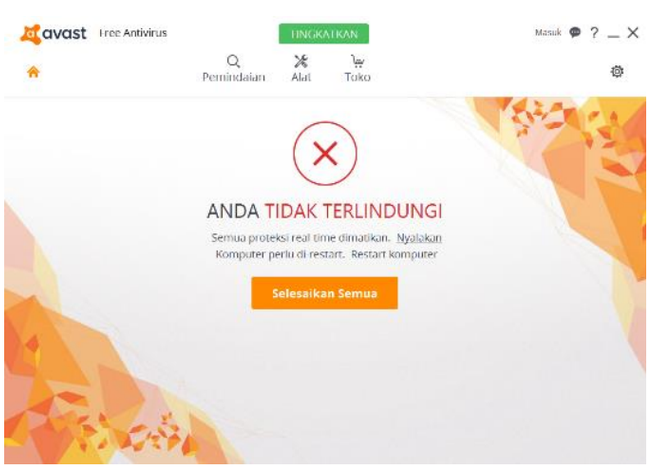
RAT adalah singkatan dari Remote Administrator Tool yang di gunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan seperti :

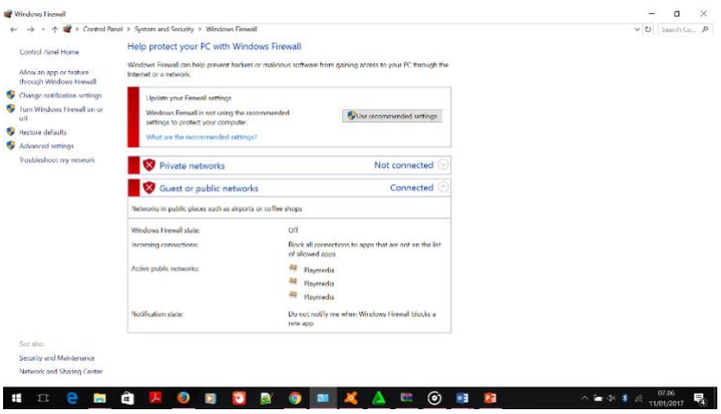
- Screen/camera capture atau control
- File management (download/upload/execute/dll.)
- Shell control (CMD control)
- Computer control (power off/on/log off)
- Registry management (query/add/delete/modify)
- Password management !!

B. LANGKAH PRAKTIKUM

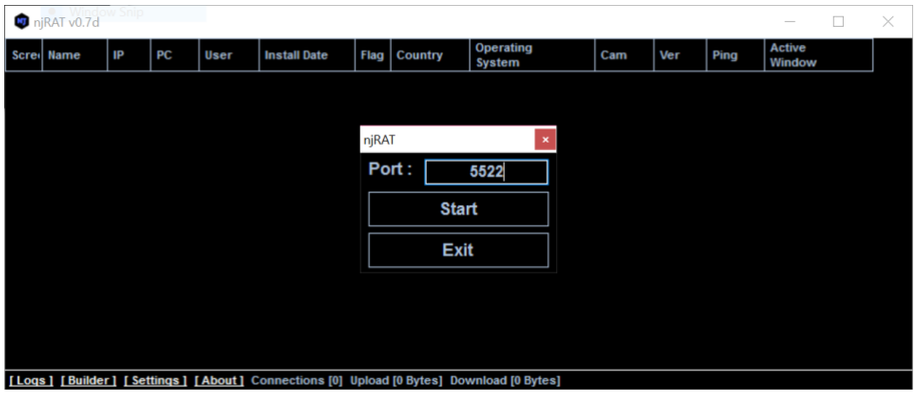
1. Jalankan virtual machine windows
2. Clone VM windows , untuk di jadikan target
3. Pada VM Windows yang dijadikan host matikan semua antivirus dan firewall pada kedua komputer yang digunakan untuk memakai aplikasi njrat ini.



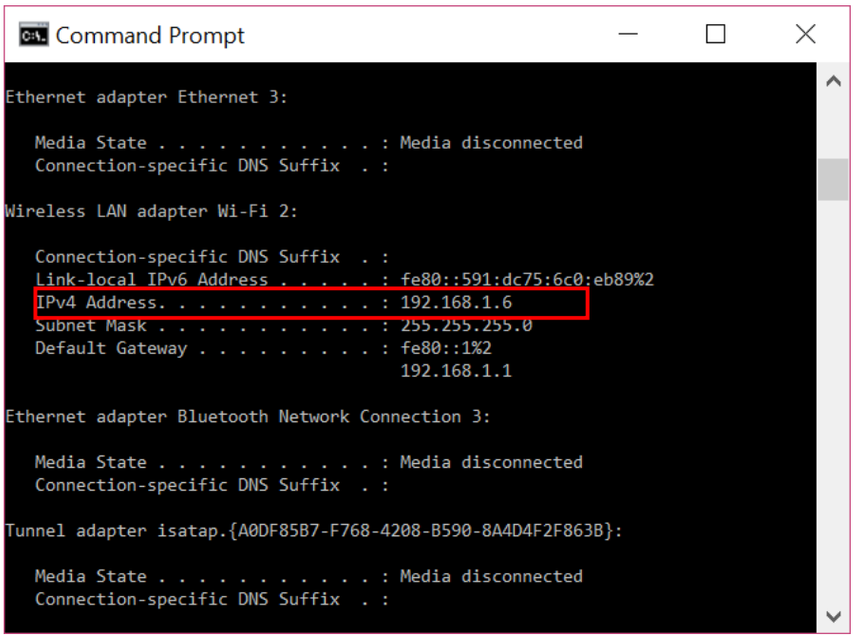




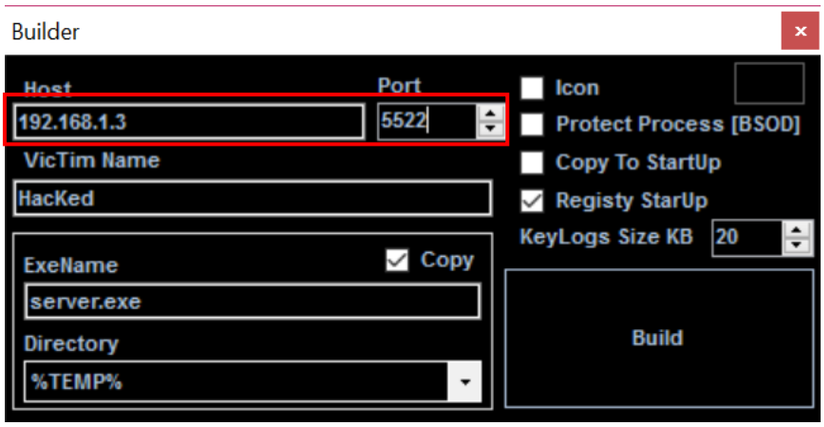
4. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host.
   https://github.com/adarift/njRAT/releases/tag/v0.7D
   Masukkan port yang ingin digunakan 5520



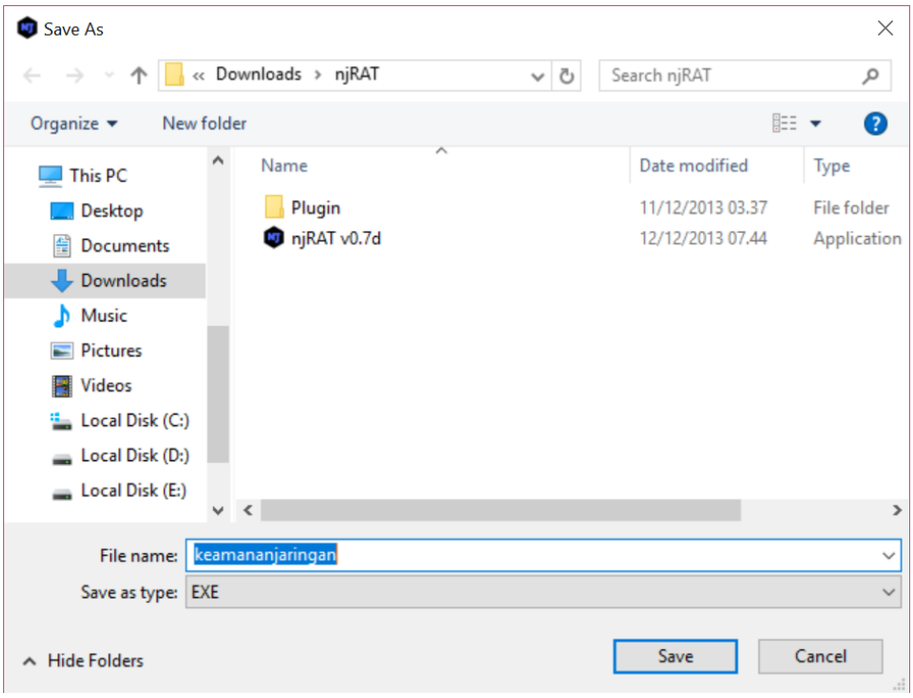
5. Sebelumnya, cek IP Address milik host terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan



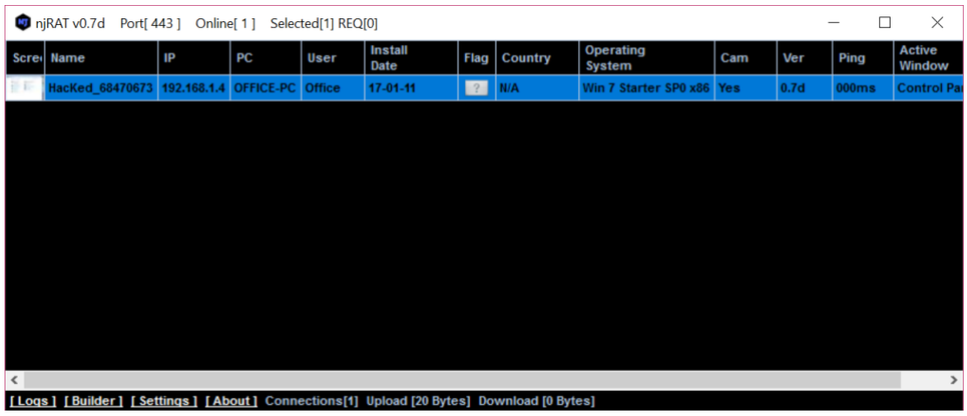
6. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada awal membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol build.



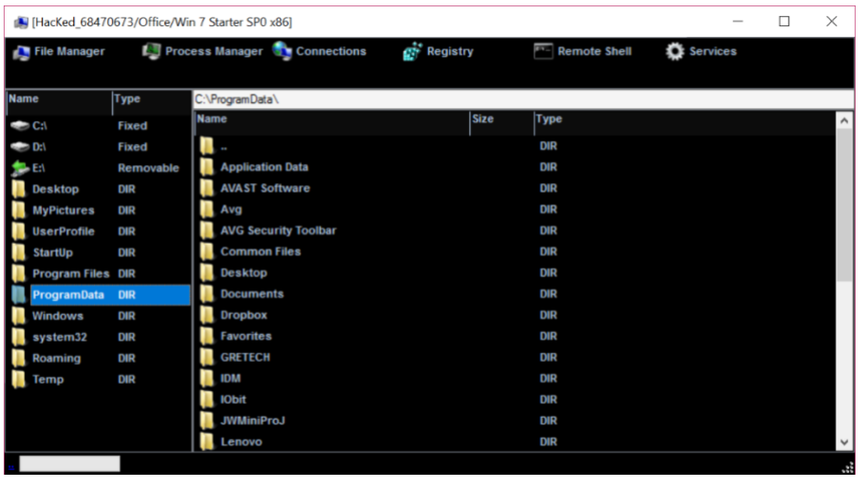
7. Simpan aplikasi hasil build.



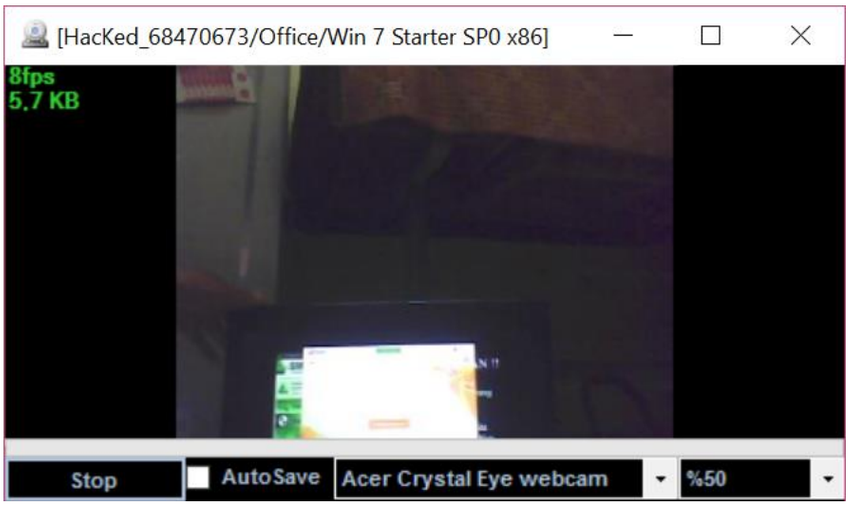
8. Kemudian, copykan aplikasi **keamananjaringan.exe** yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut. Ketika sudah terpasang pada komputr victim, NJRAT pada host akan mendeteksi komputer victim



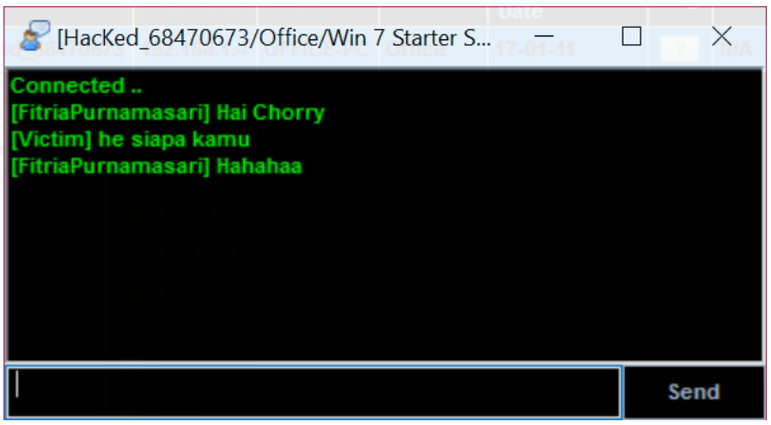
9. Klik kanan pada komputer yang aktif maka akan muncul beberapa pilihan menu, pilih menu **manager** agar dapat melihat seluruh isi file manager yang ada pada komputer victim



10. Pada menu **remote cam** maka akan membuka *webcam* yang ada di komputer victim dan dapat melihat segala aktivitas yang dilakukan oleh victim



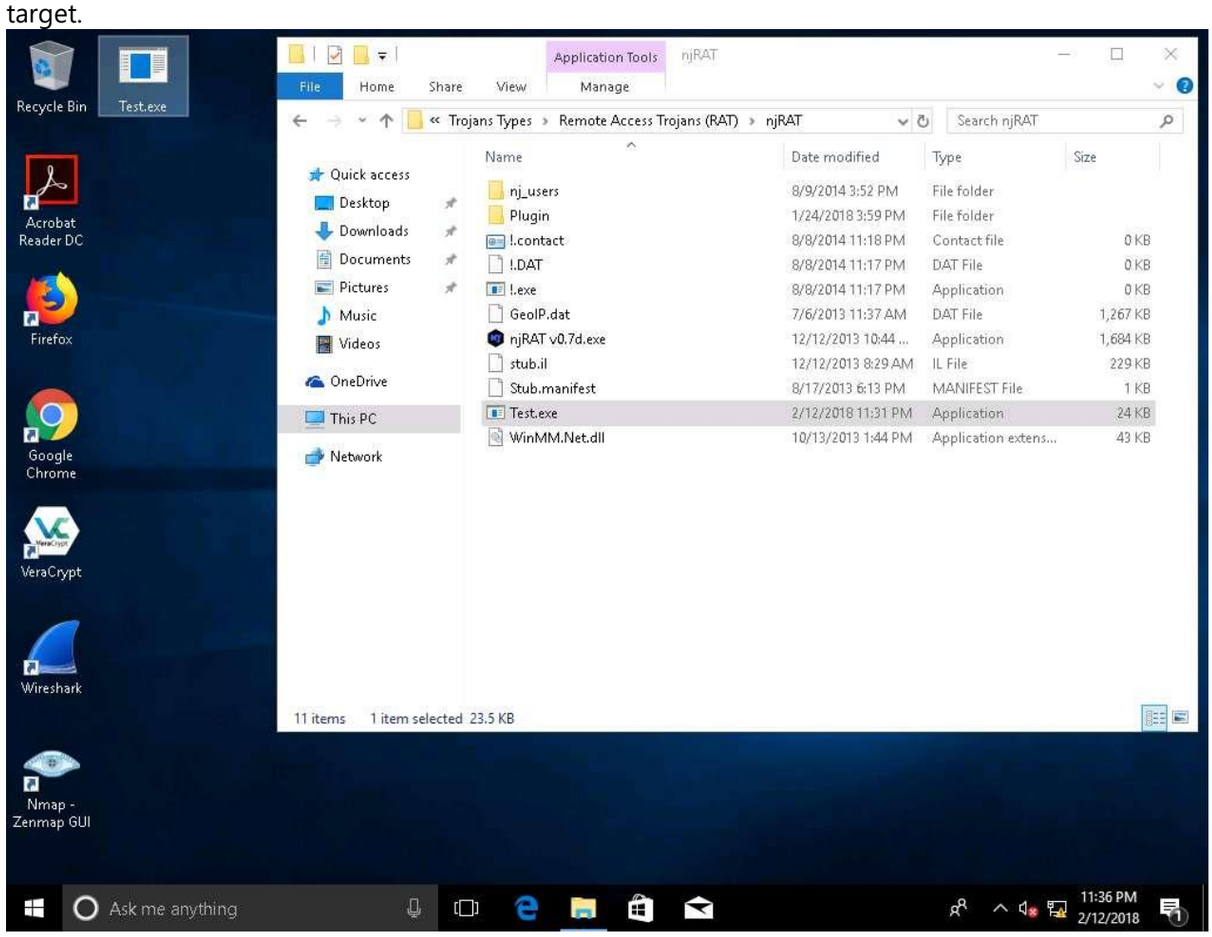
11. Pada pilihan **chat message**, kita dapat mengirimkan pesan ke layar desktop komputer victim, dan user komputer dapat melakukan balasan tanpa bisa menutup chat



NJRAT merupakan salah satu malware sejenis Trojan yang menginfeksi komputer victim melalui installasi program. ketika malware terpasang pada PC, maka segala bentuk kegiatan PC victim dapat dimonitoring / dikendalikan melalui PC host yang berada pada satu jaringan melalui akses IP dan port yang telah ditentukan diawal.

12. Buatlah file trojan dengan nama mahasiswa masing-masingatau nama file **Test.exe** simpan pada **Desktop** di VM

target.

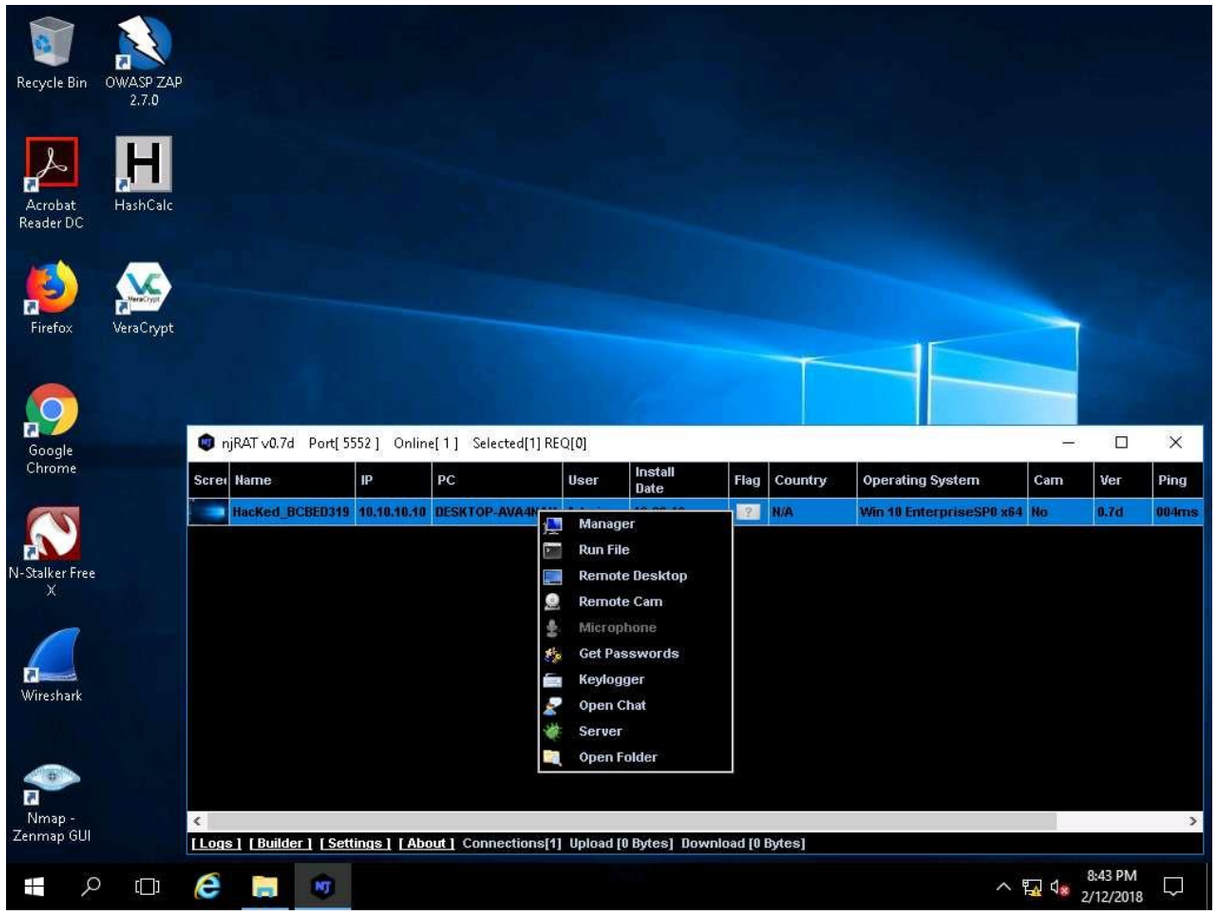


13. Sekarang, klik dua kali **Test.exe** file yang telah Anda tempel di Desktop.

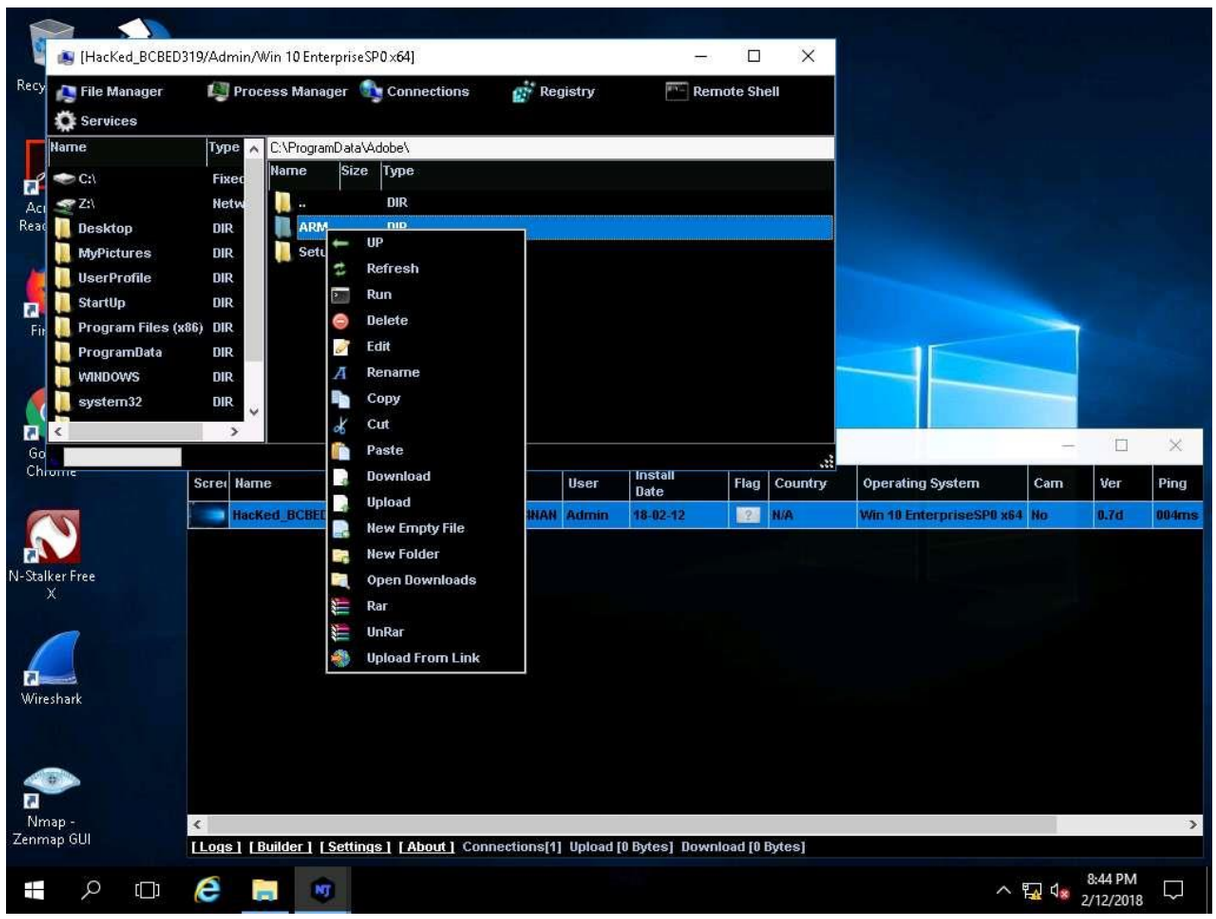
14. mengklik dua kali server, executable mulai berjalan dan klien njRAT (njRAT GUI) yang berjalan di VM Target membuat koneksi persisten dengan mesin korban seperti yang ditunjukkan pada tangkapan layar.

    Kecuali jika penyerang yang bekerja pada mesin VM target memutuskan server sendiri, mesin korban tetap berada di bawah kendalinya.

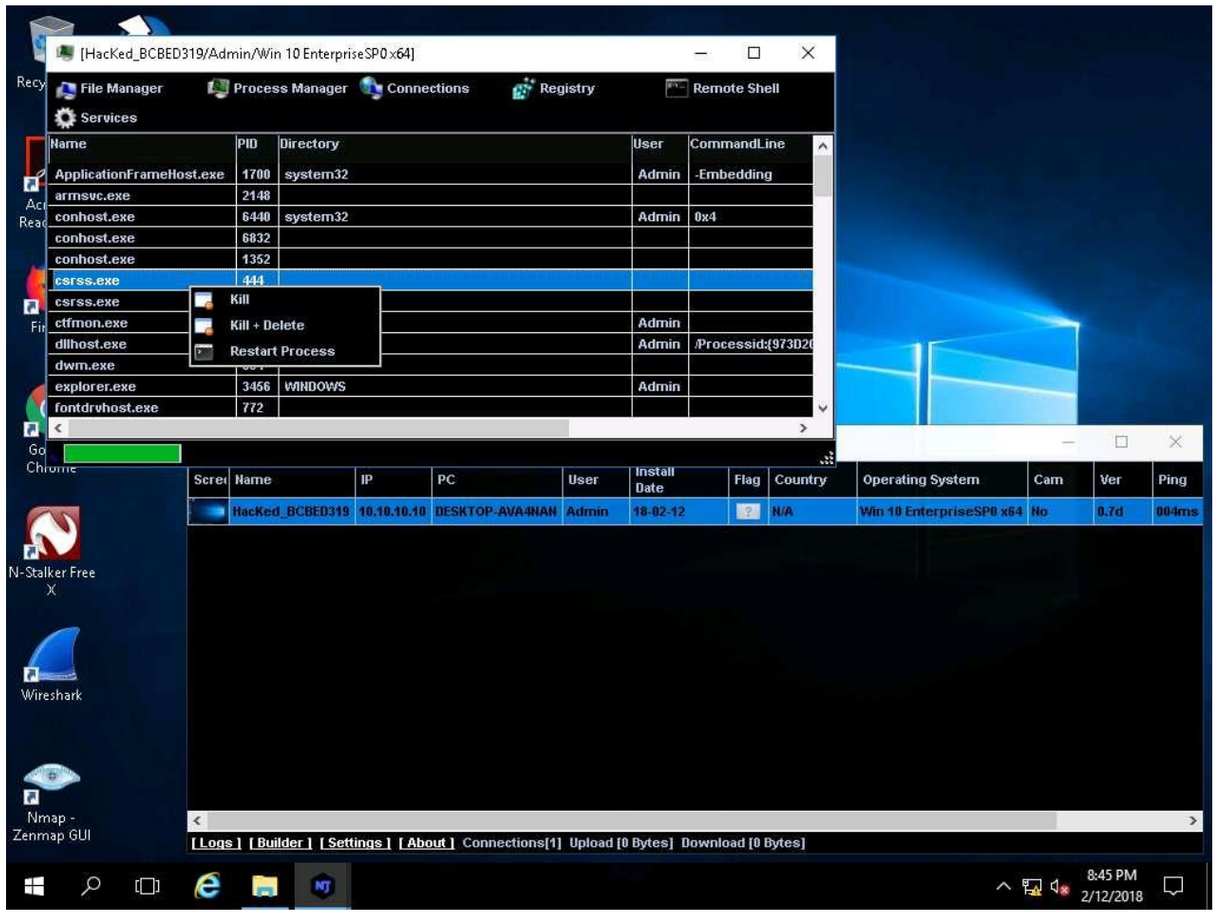
    GUI menampilkan detail dasar mesin seperti **alamat IP**, **Nama pengguna**, **Jenis sistem operasi** dan sebagainya. Klik kanan pada nama korban yang terdeteksi dan klik **Manager**.



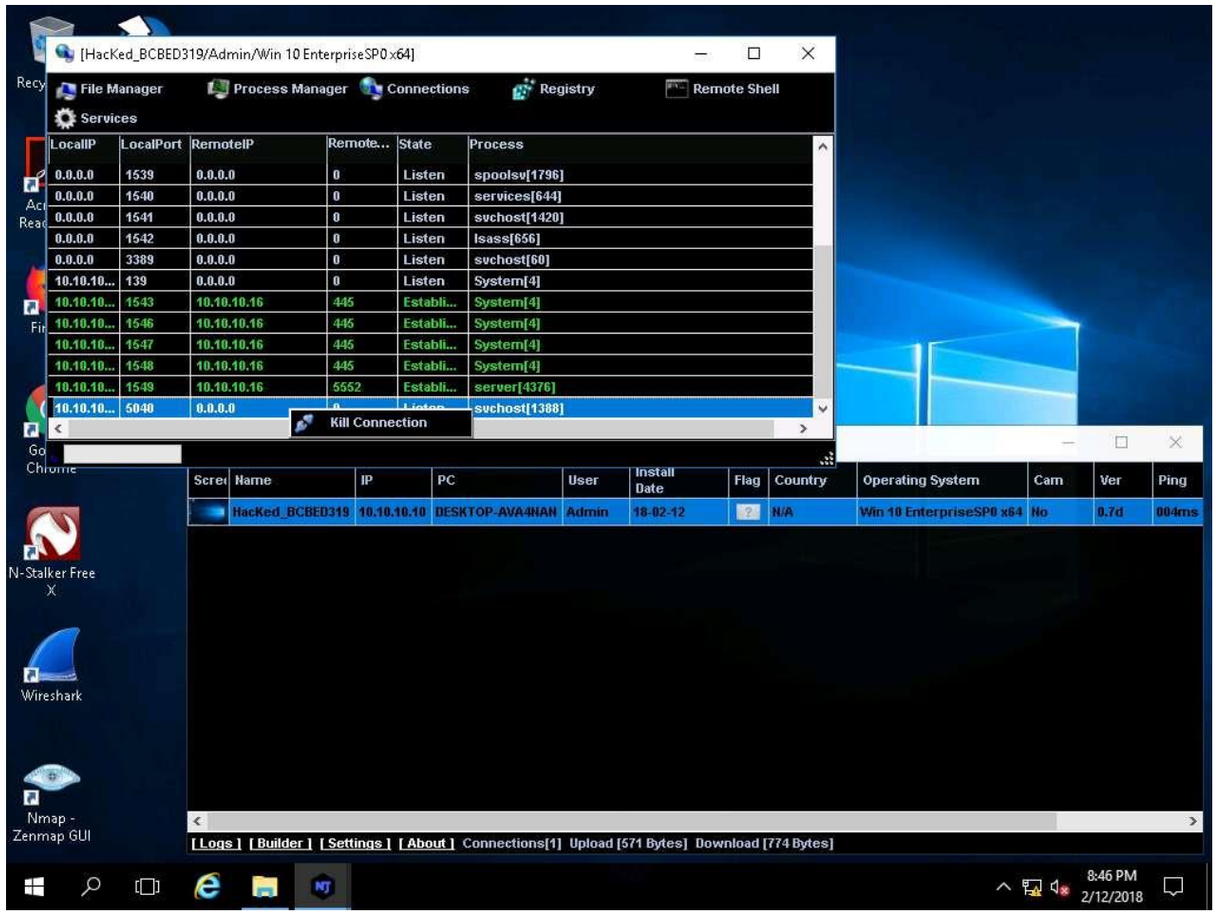
15. Jendela Manajer muncul, di mana **Manajer File** dipilih secara default. Klik dua kali direktori mana pun di panel kiri (**ProgramData**); Semua file/direktori terkait ditampilkan di panel kanan. Anda dapat mengklik kanan direktori yang dipilih dan memanipulasinya menggunakan opsi kontekstual.



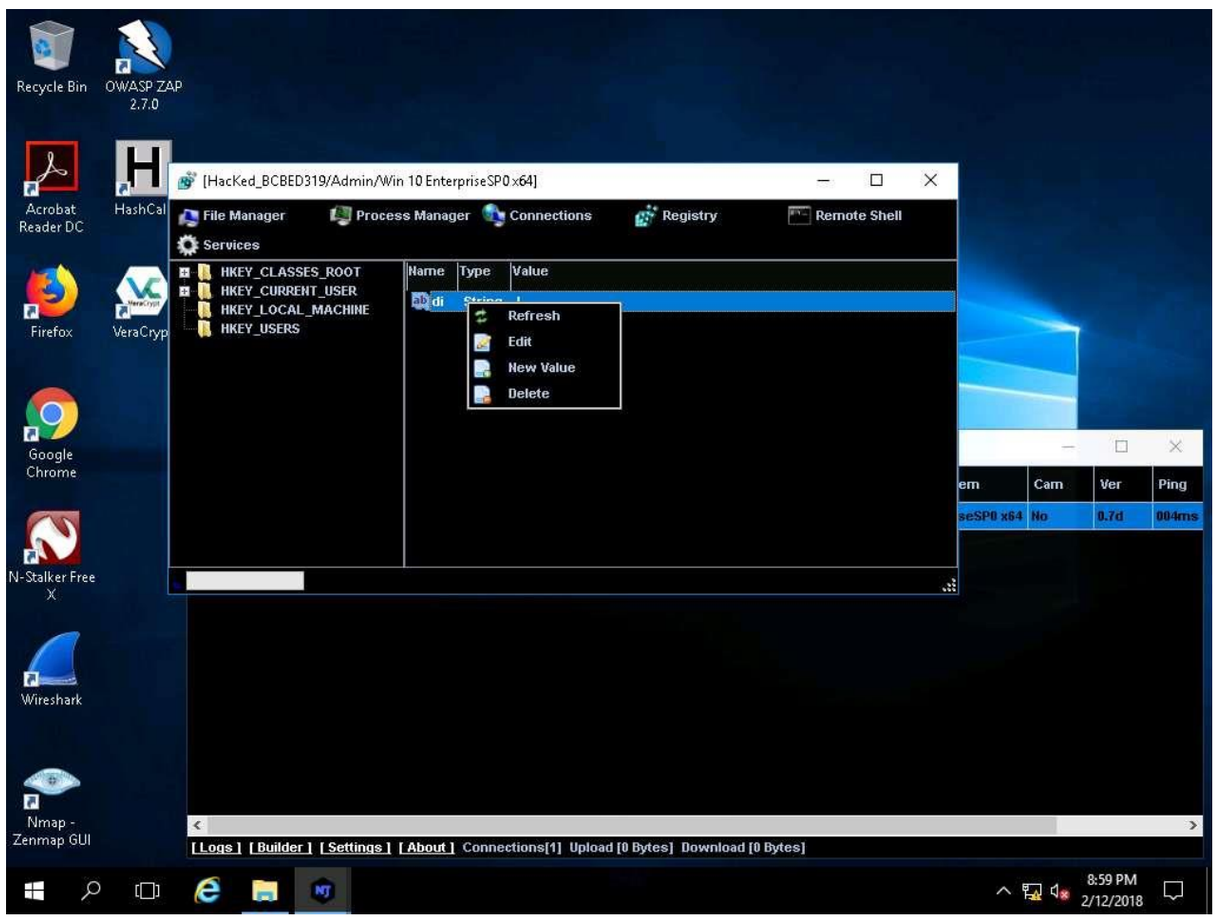
16. Arahkan mouse ke **Process Manager**. Anda akan diarahkan ke Manajer Proses, di mana Anda dapat mengklik kanan pada proses yang dipilih dan melakukan tindakan seperti **Kill**, **Delete**, dan **Restart**.



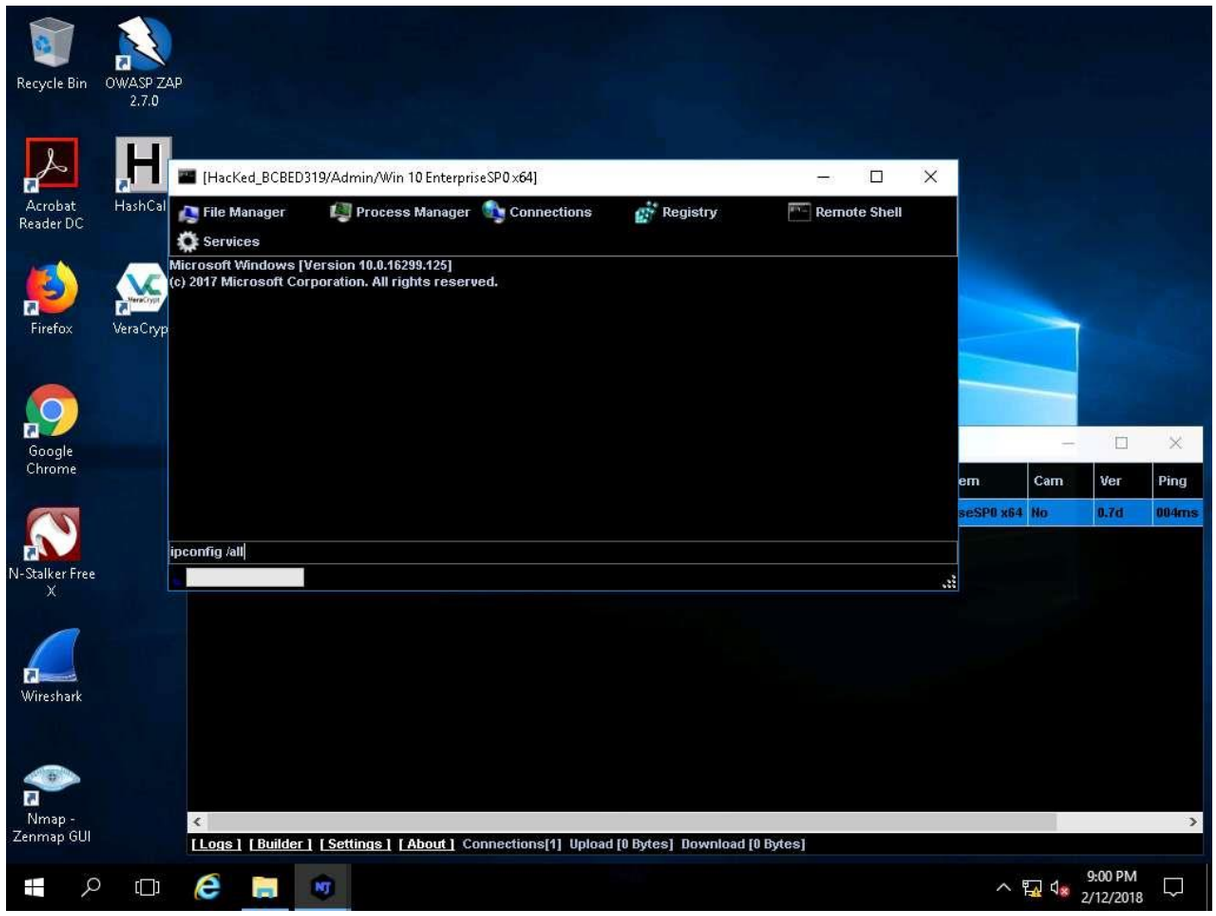
17. Klik Koneksi, pilih koneksi tertentu, klik kanan , dan klik **Kill Koneksi**. Ini akan memutuskan koneksi antara dua mesin yang berkomunikasi melalui port tertentu.



18. Klik **Registri,** pilih direktori registri dari panel kiri, dan klik kanan pada file registri terkait. Beberapa opsi muncul untuk file yang dapat Anda gunakan untuk memanipulasinya.

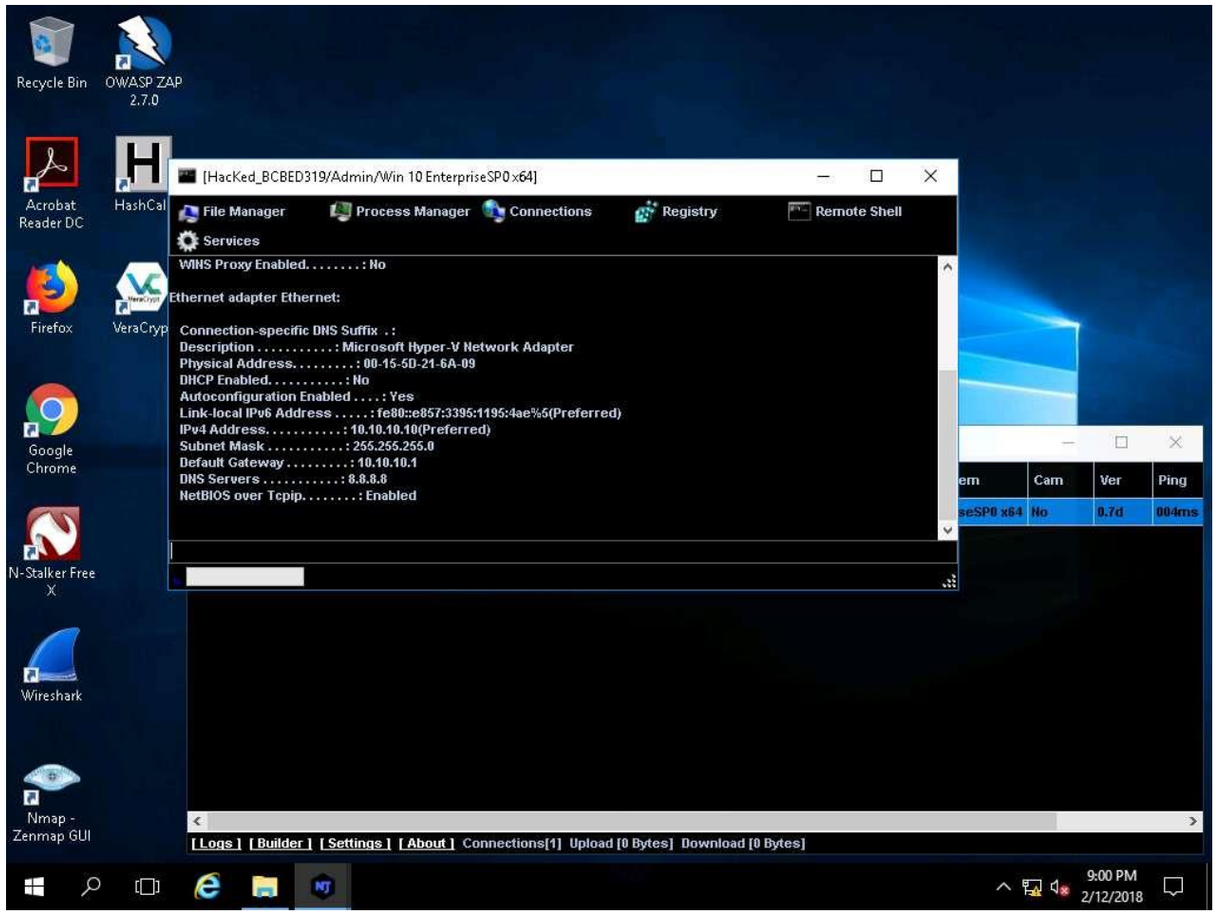


19. Klik **Remote Shell**. Ini meluncurkan prompt perintah jarak jauh dari mesin korban (Windows 10). Ketik perintah **ipconfig /all** dan tekan **Enter**.

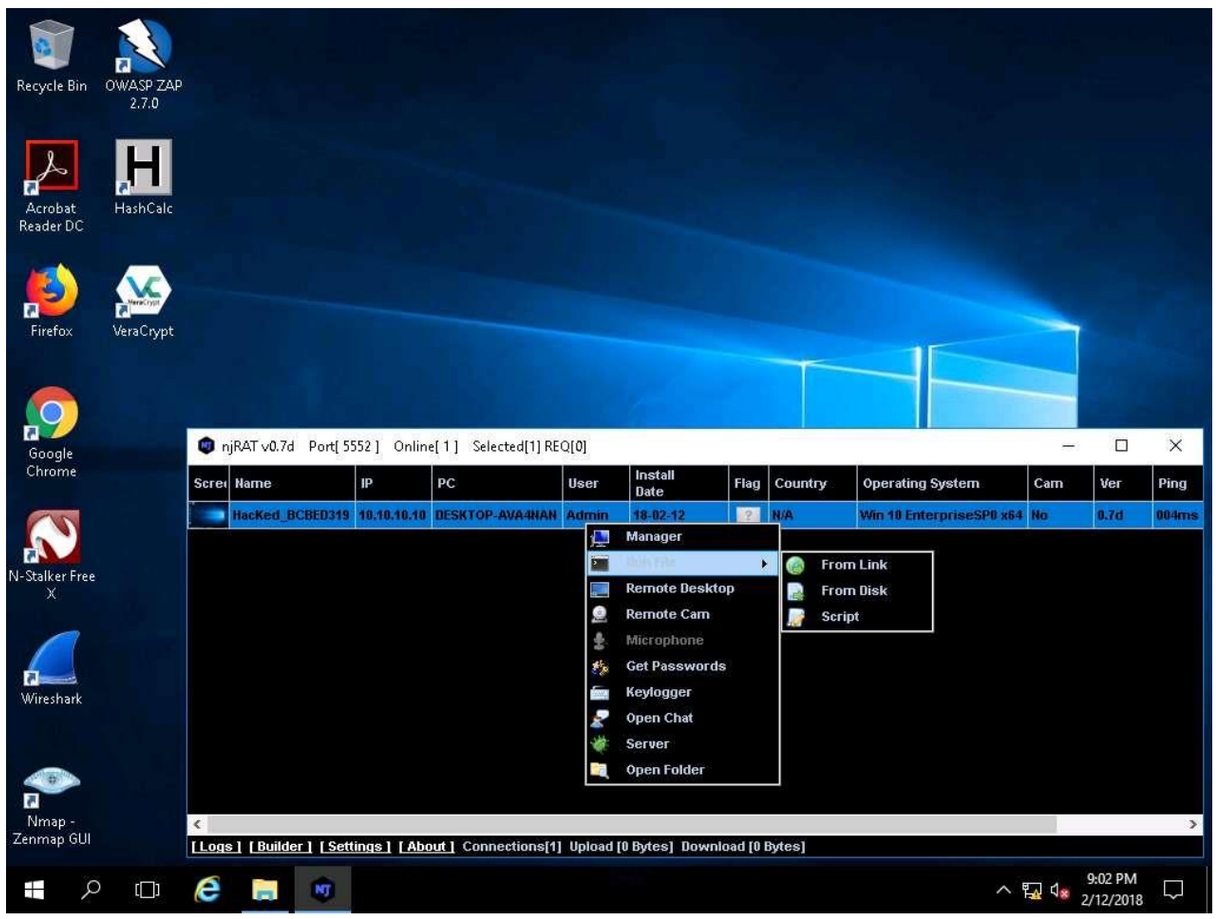


20. Ini menampilkan semua antarmuka yang terkait dengan mesin korban, seperti yang ditunjukkan pada tangkapan layar. Demikian pula, Anda dapat mengeluarkan semua **perintah** lain yang dapat **dijalankan** di command prompt mesin korban.

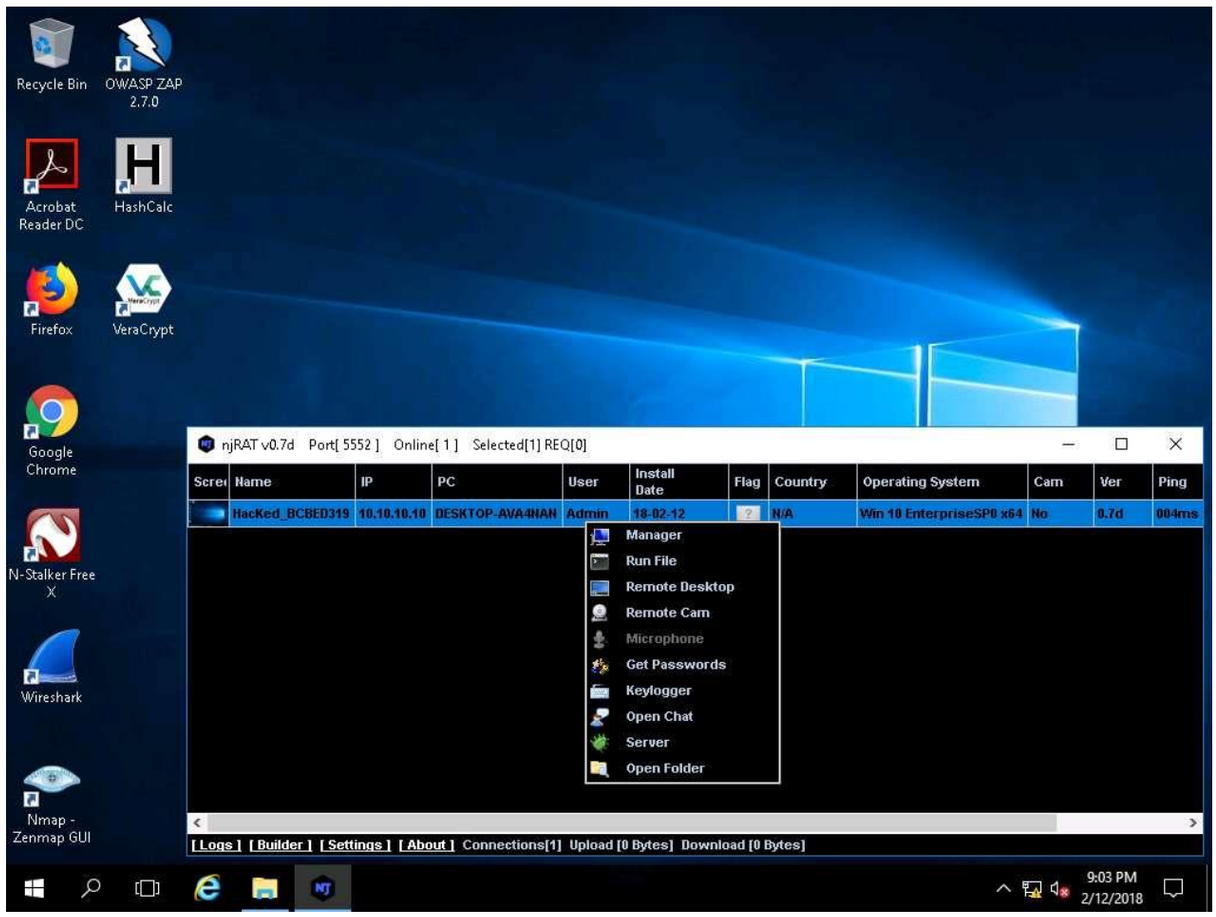
Dengan cara yang sama, klik **Layanan**. Anda akan dapat melihat semua layanan yang berjalan di mesin korban. Di bagian ini, Anda dapat menggunakan opsi untuk memulai, menjeda, atau menghentikan layanan. Tutup jendela **Manajer**.



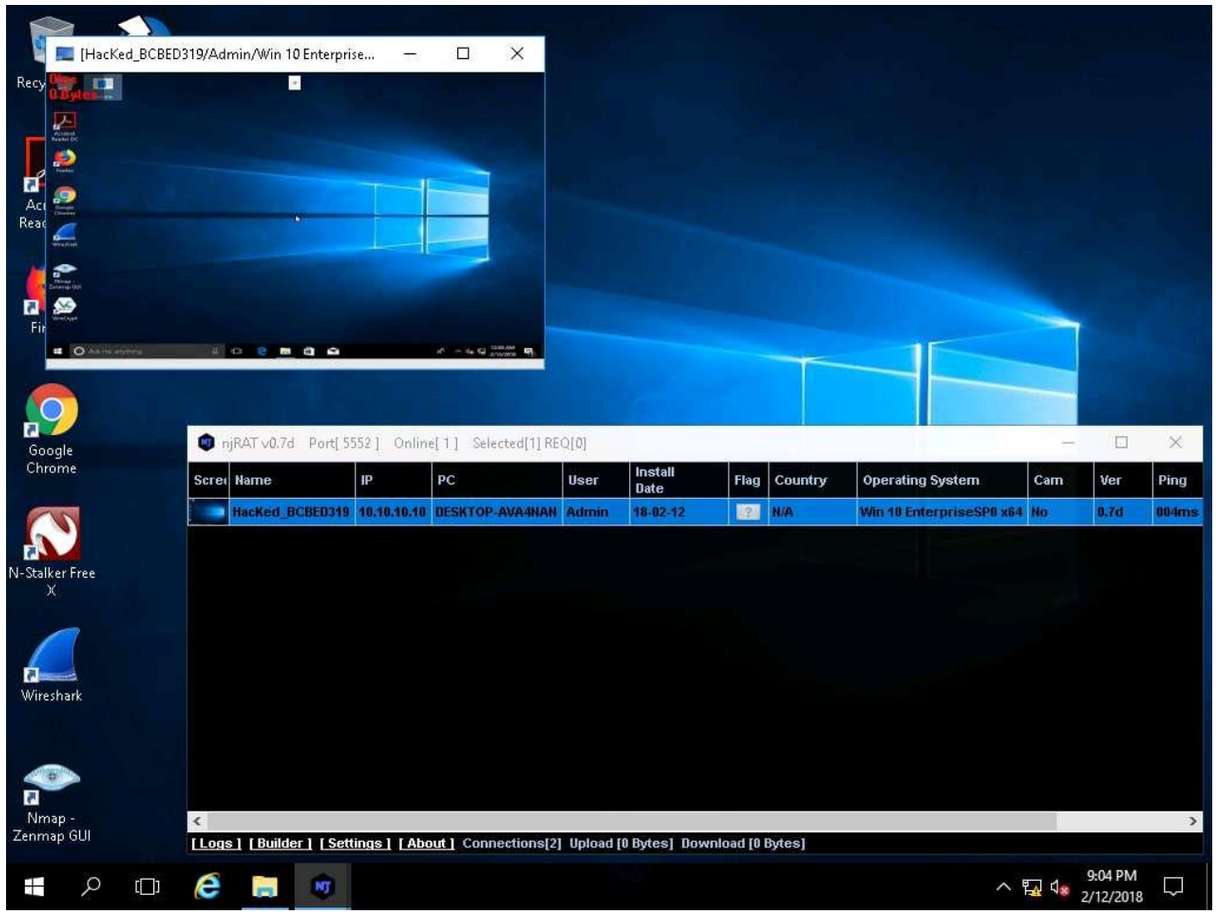
1. Sekarang klik kanan pada nama korban, klik **Run File** dan pilih opsi dari daftar drop-down. Penyerang menggunakan opsi ini untuk mengeksekusi skrip atau file dari jarak jauh dari mesinnya.



1. Klik kanan pada nama korban, dan pilih **Remote Desktop**. Ini meluncurkan koneksi desktop jarak jauh tanpa disadari oleh korban.



1. **Remote Desktop** jendela muncul, arahkan kursor mouse ke bagian tengah atas jendela. Panah bawah muncul, klik panah bawah.

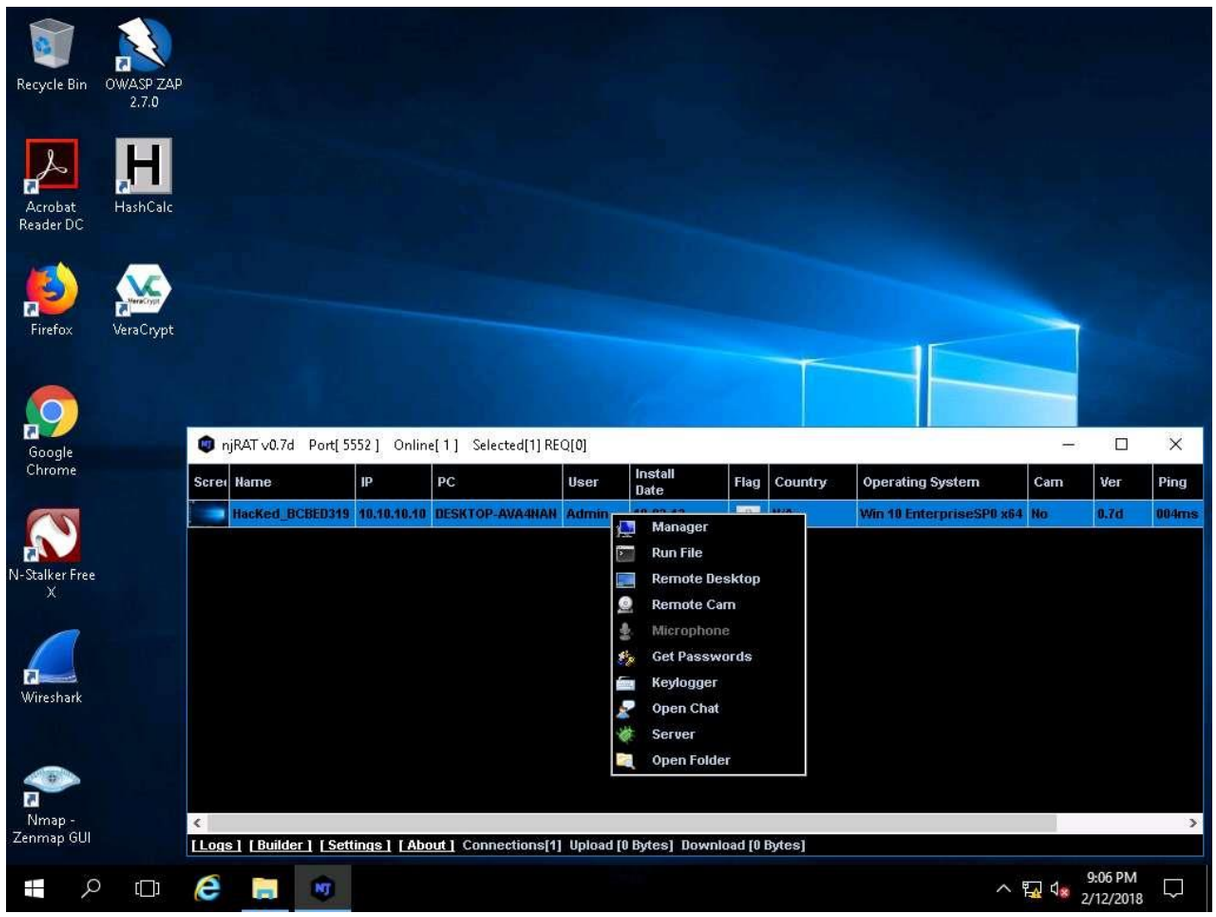


remote desktop panel kontrol muncul; centang opsi **Mouse**. Sekarang, Anda akan dapat berinteraksi dari jarak jauh dengan mesin korban menggunakan mouse.

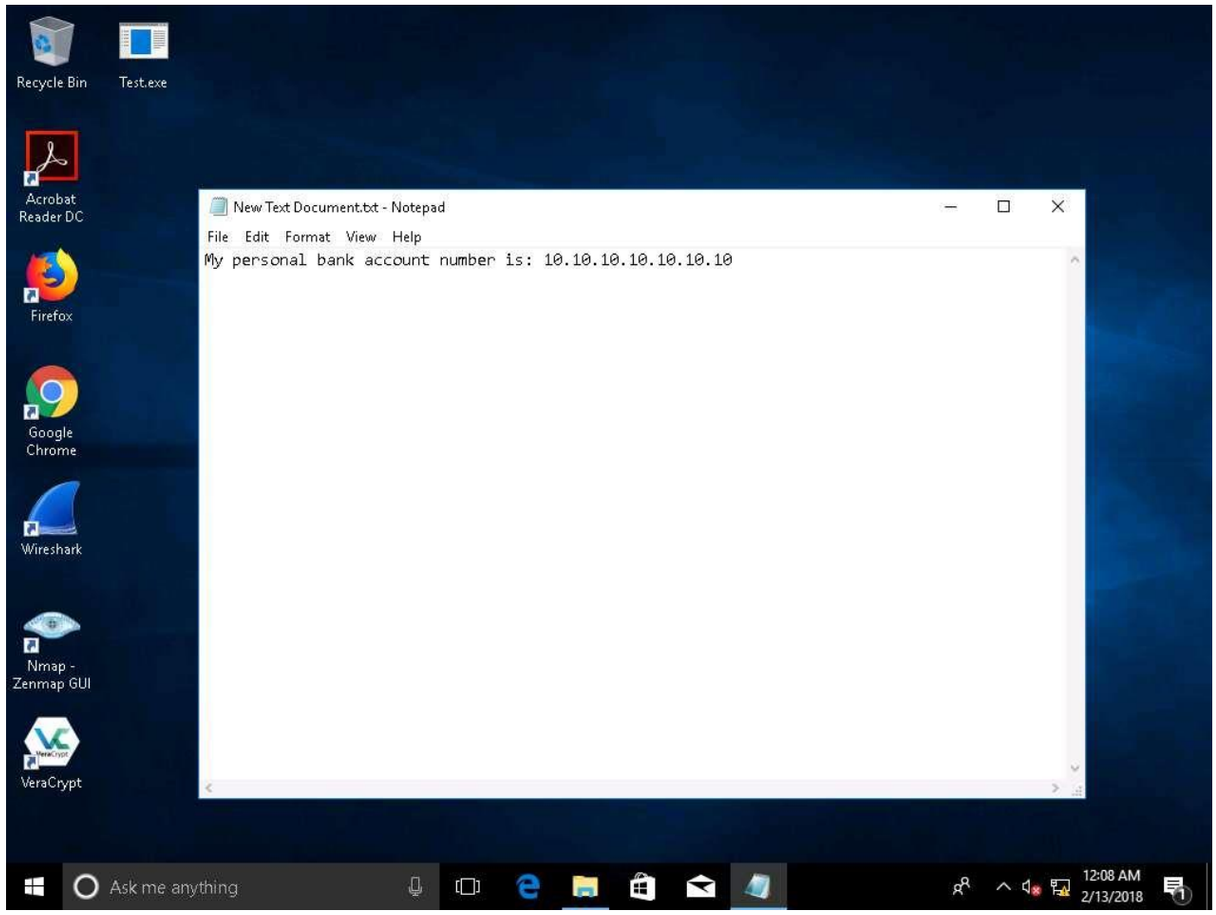
Saat menyelesaikan tugas, **tutup** jendela Desktop Jarak Jauh.

Jika Anda ingin membuat file apa pun atau menulis skrip apa pun di mesin korban, Anda perlu memeriksa opsi **Keyboard**.

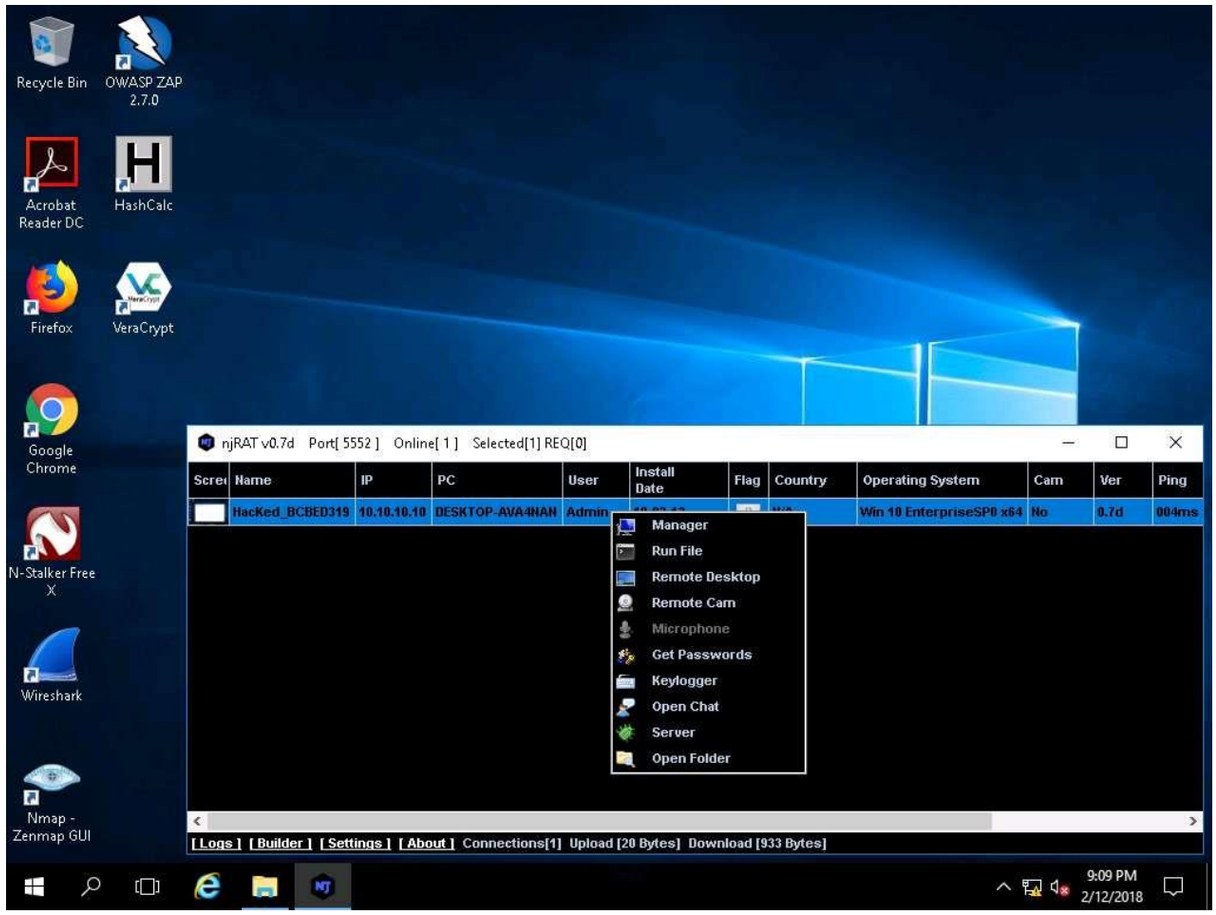
1. Dengan cara yang sama, klik kanan pada nama korban, dan pilih **Remote Cam dan Microphone** untuk memata-matai korban dan melacak percakapan suara.



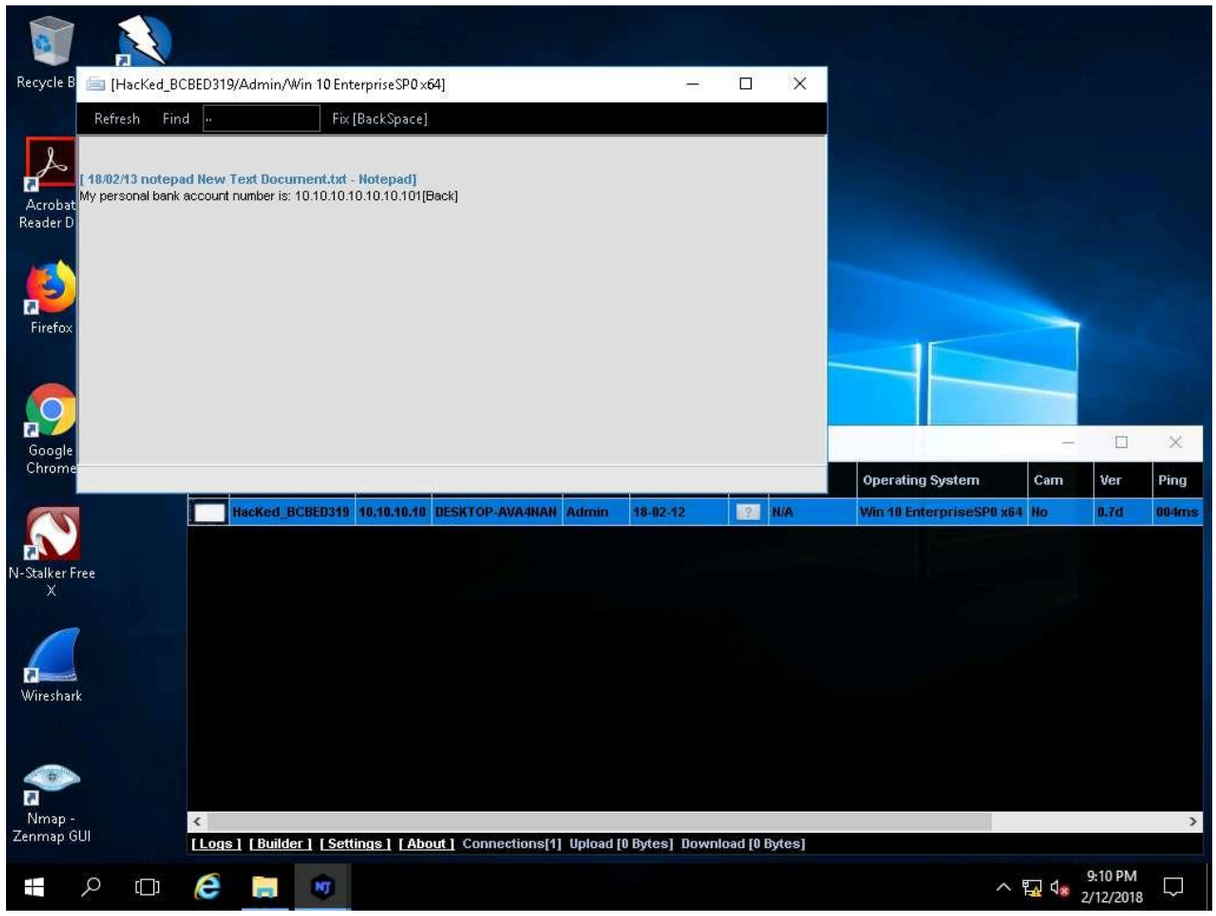
1. Klik Mesin Windows 10 dari panel Sumber Daya, asumsikan bahwa Anda adalah pengguna yang sah dan melakukan beberapa aktivitas seperti masuk ke situs web apa pun atau **mengetik** teks di beberapa dokumen teks.



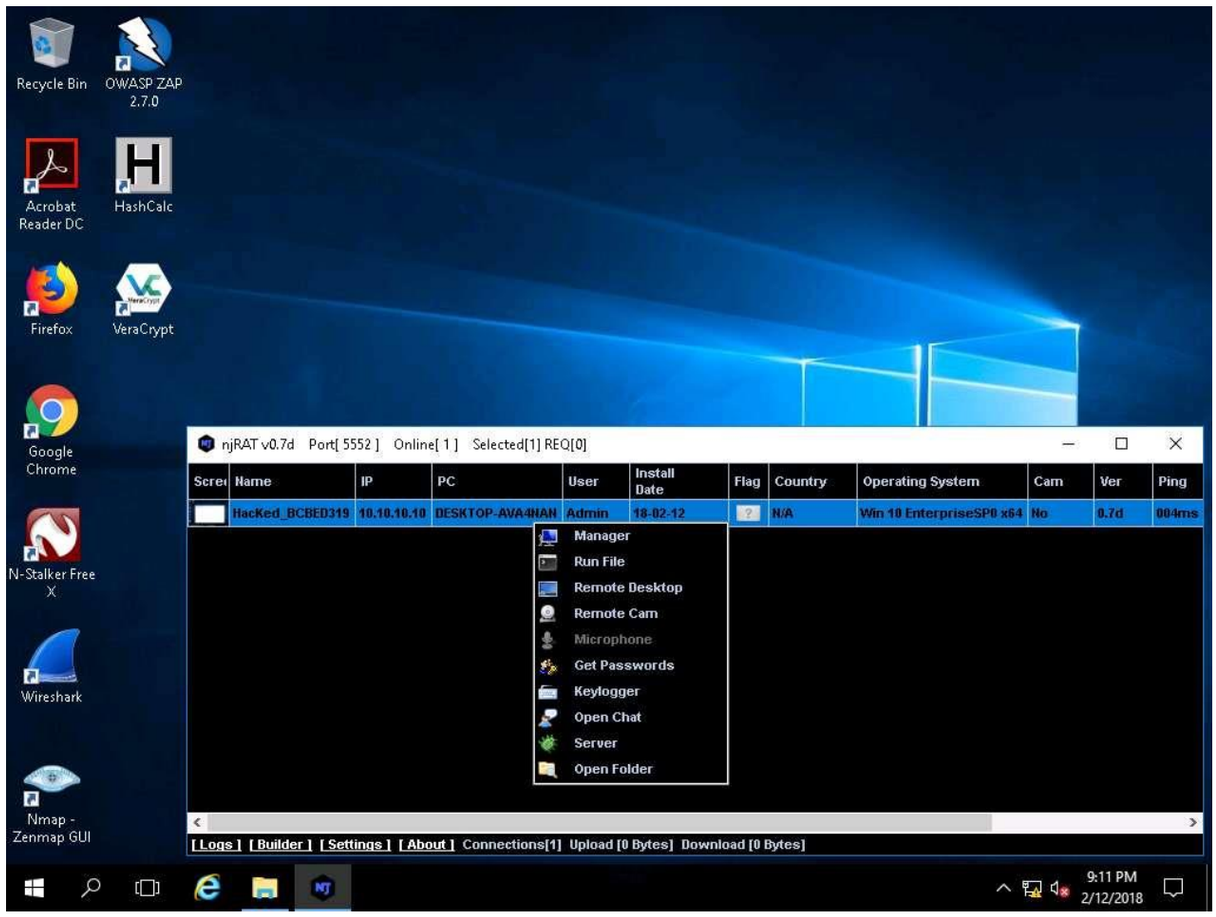
21. Klik Mesin Windows Host dari panel Sumber Daya, klik kanan pada nama korban, dan klik **Keylogger**.



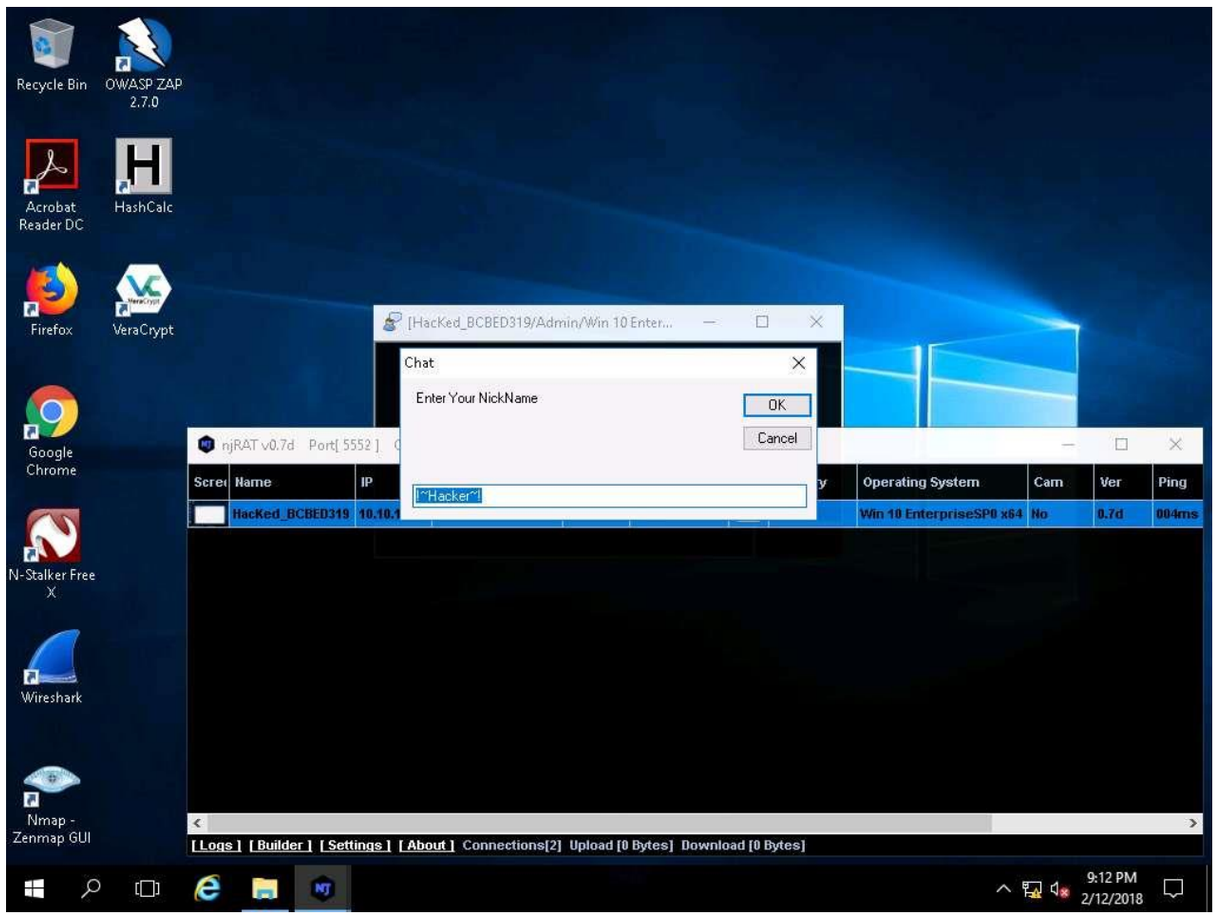
1. **Keylogger** jendela muncul; tunggu hingga jendela dimuat. Jendela menampilkan semua penekanan tombol yang dilakukan oleh korban pada mesin **Windows 10**, seperti yang ditunjukkan pada tangkapan layar. **Tutup** jendela Keylogger.



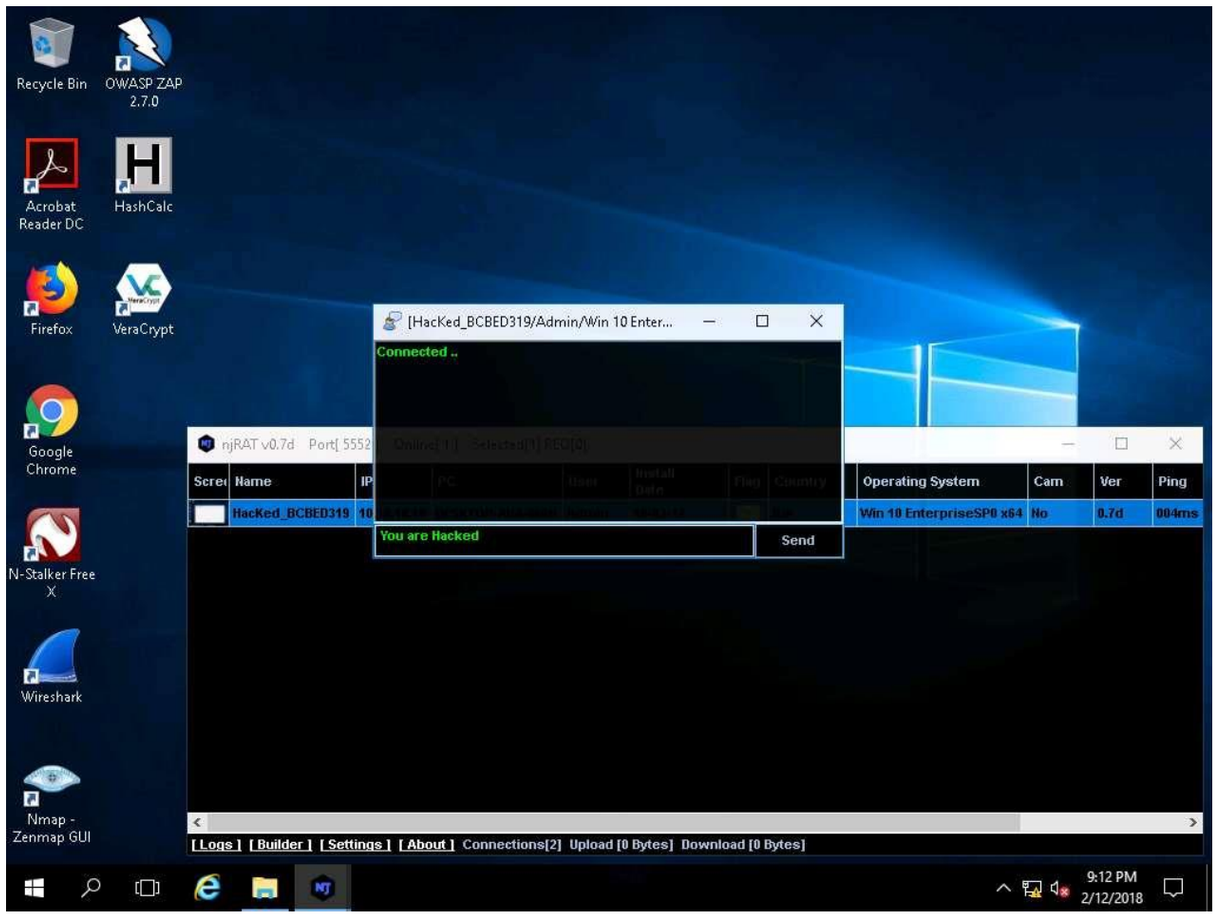
22. Klik kanan pada nama korban, dan klik **Open Chat**.



1. Chat pop-up Muncul; masukkan nama panggilan (di sini, **Hacker**), dan klik **OK**.



23. Kotak obrolan muncul; ketik pesan, dan klik **Send**.

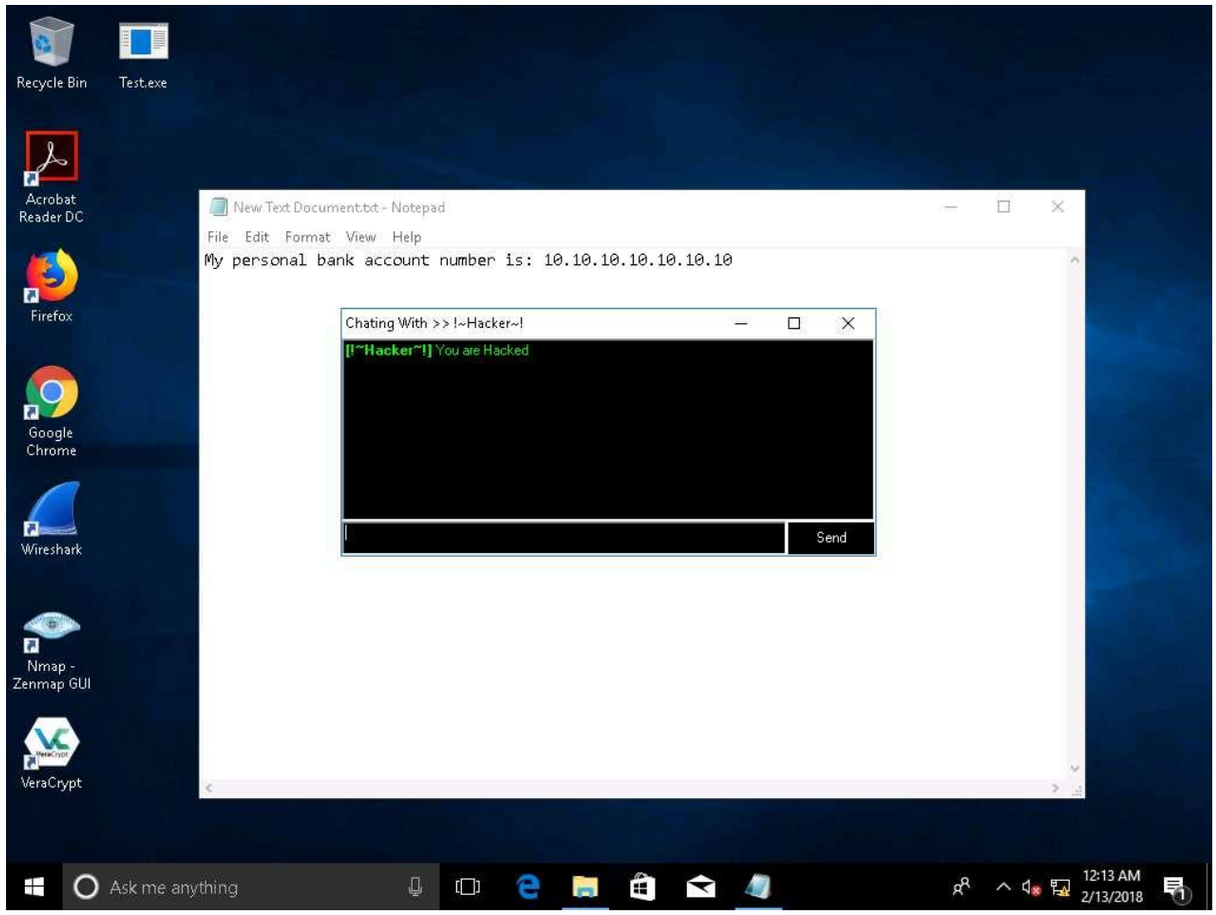


1. Klik Komputer **Windows 10** dari panel **Sumber Daya**. Segera setelah penyerang mengirim pesan, pop-up muncul di layar korban (Windows 10), seperti yang ditunjukkan pada tangkapan layar.

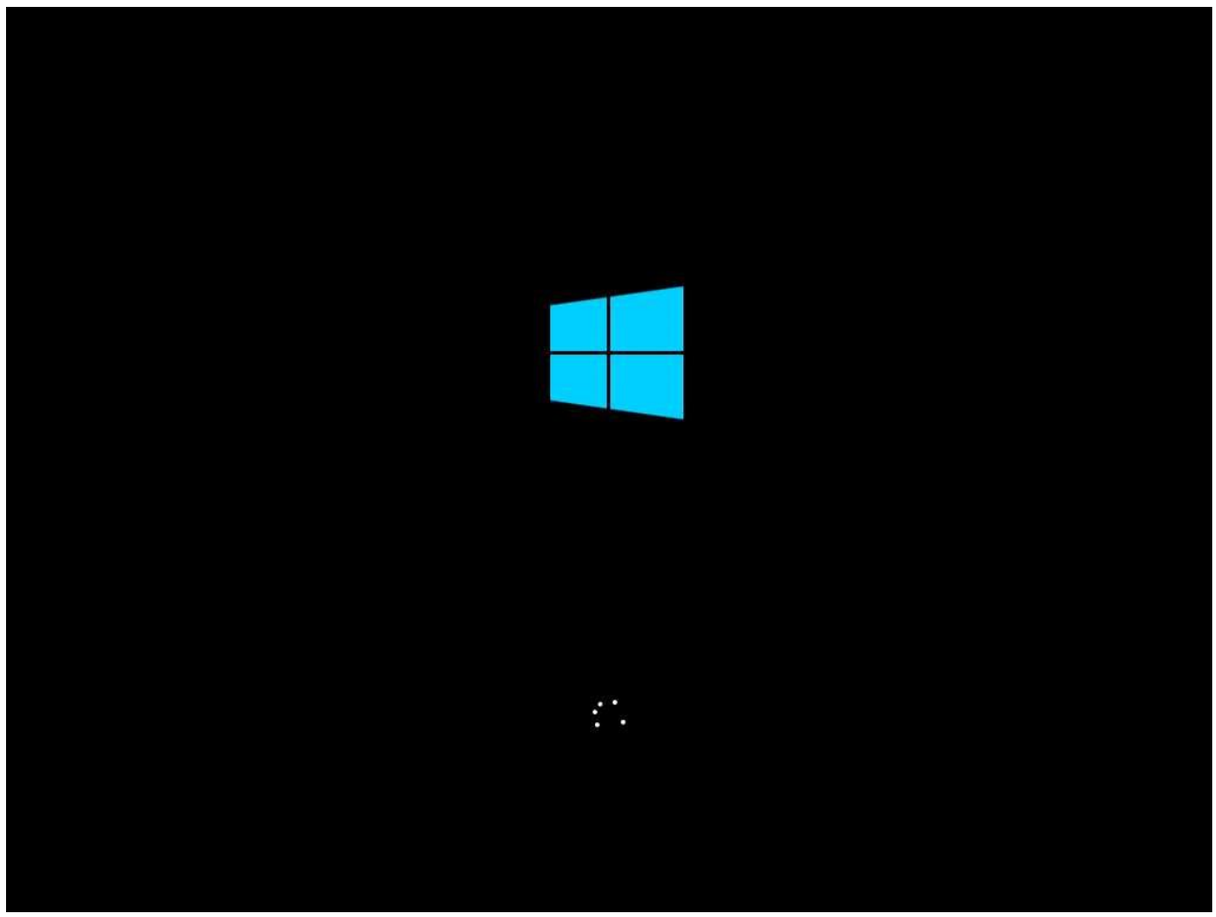
   Skenario serangan dan target :

   Melihat hal tersebut, korban menjadi waspada dan berusaha menutup kotak obrolan. Tidak peduli apa pun yang dilakukan korban, kotak obrolan tetap terbuka selama penyerang menggunakannya.

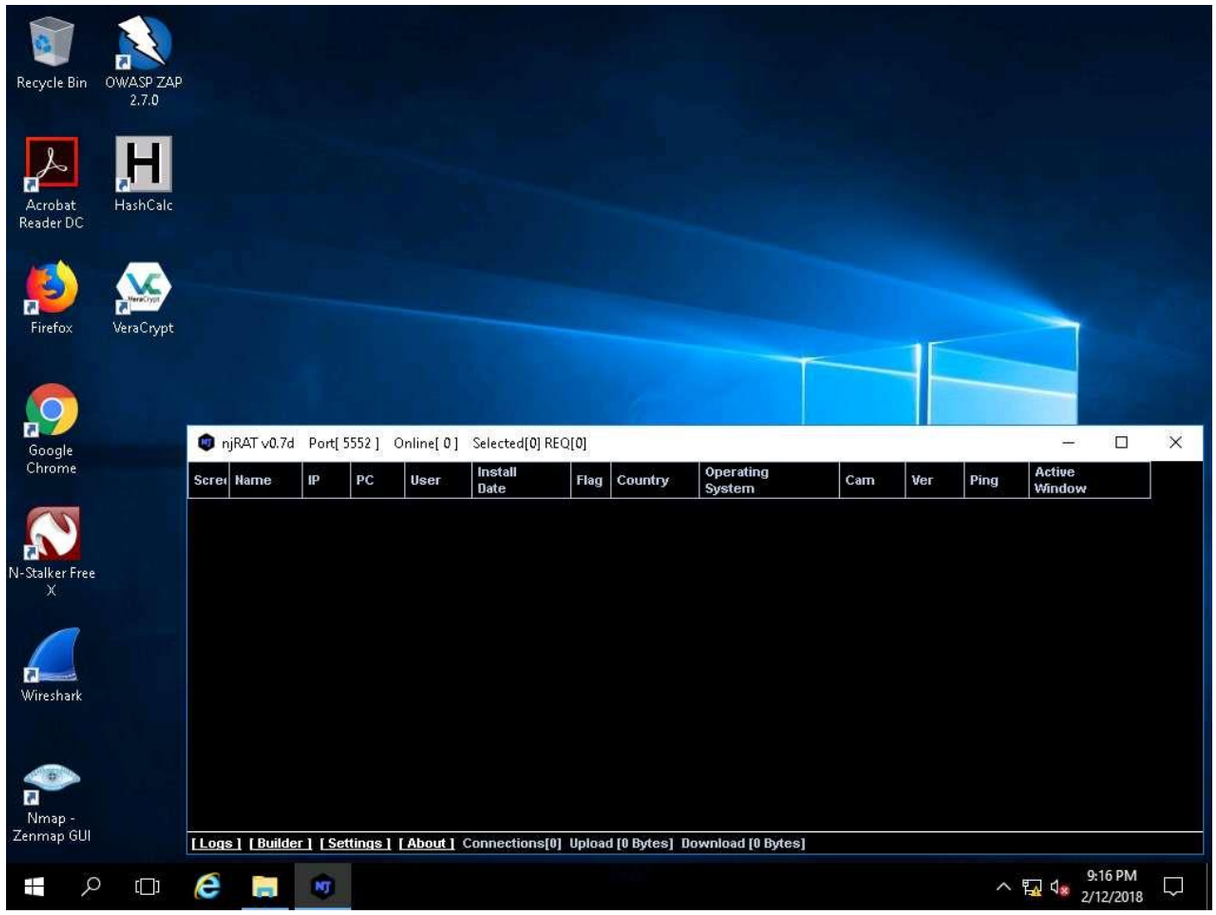
   Terkejut dengan perilaku itu, korban (Anda) mencoba memutuskan koneksi dengan me-restart mesin. Segera setelah dia melakukannya, njRAT kehilangan koneksi dengan Windows 10, karena mesin dimatikan dalam proses restart.



Sekarang restart mesin **Windows 10 pada target**.

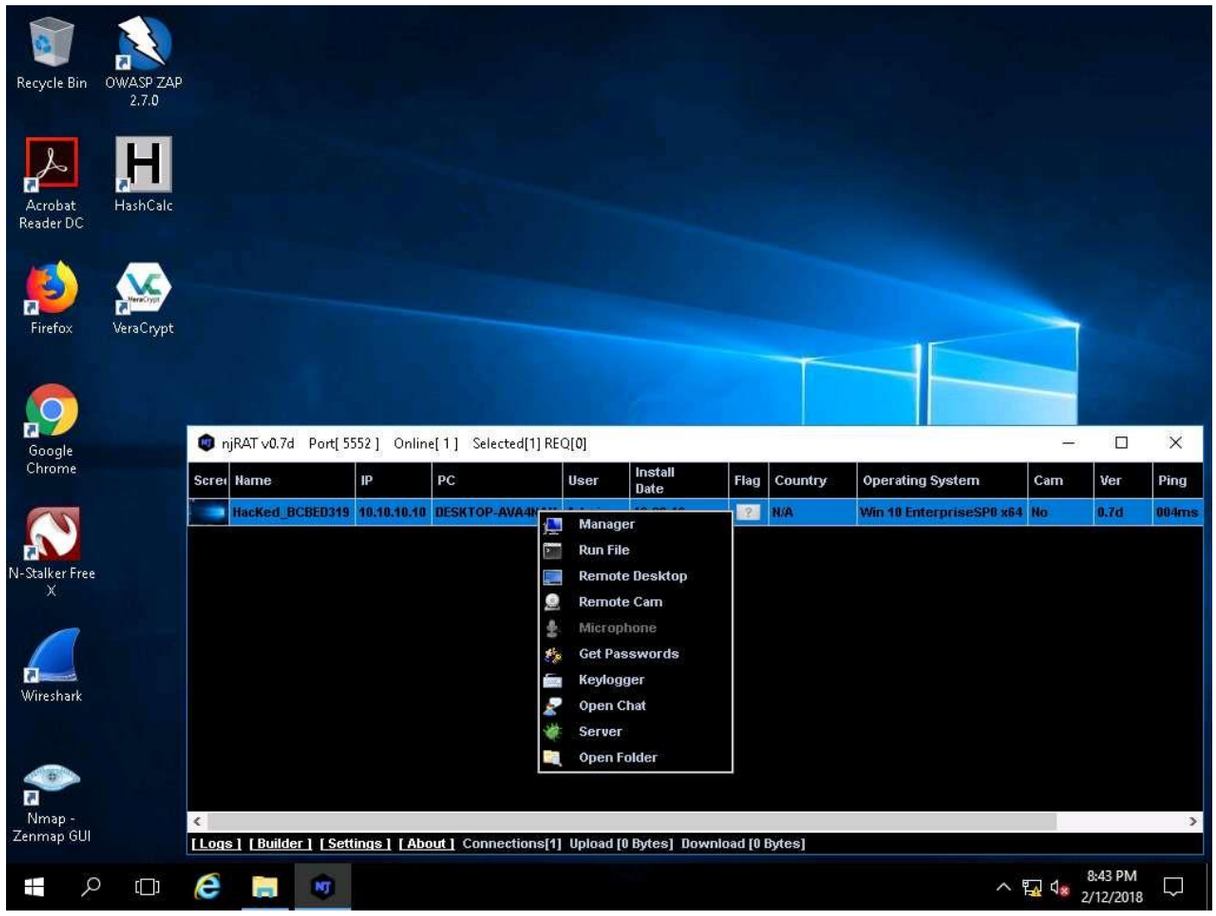


Klik Mesin **Windows** dari panel **Sumber Daya (Host/Penyerang)**, perhatikan bahwa koneksi telah hilang dengan mesin korban.



Klik Mesin Windows 10 dari panel **Sumber Daya**, dan **Masuk** ke komputer. **Biarkan** mesin berjalan.

Klik Mesin Windows Penyerang dari panel **Sumber Daya**, perhatikan bahwa koneksi dibuat setelah mulai ulang. Penyerang, seperti biasa, memanfaatkan koneksi untuk mengakses mesin korban dari jarak jauh dan melakukan aktivitas berbahaya.



Setelah menyelesaikan lab, tutup semua jendela. Di lab ini Anda telah mempelajari cara:

1. Membuat Server menggunakan njRAT
2. Akses mesin korban dari jarak jauh

Port default yang digunakan oleh njRAT adalah_____

Apa alamat IP mesin tempat njRAT dihosting?