

re: Covert Microphone Application

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-07/msg00402.html>

- *From:* gg <geekgirl@xxxxxxx>
 - *Date:* Sun, 30 Jul 2006 10:12:12 -0400 (GMT-04:00)
-

Wake on Lan?

From: Craig Wright [<mailto:cwright@xxxxxxxxxxxxxx>]
Sent: Fri 7/28/2006 6:12 PM
To: m@xxxxxx
Cc: Matt Burnett; shiri_yacov@xxxxxxx; pen-test@xxxxxxxxxxxxxxxxxxxx

No, you should not assume. There is nothing to state the host is on a network. There are ways to do this without network access (eg an application that monitors all the time and records when the sound levels go over a certain threshold).

You could also argue control via wireless networks/bluetooth.

There may be limited access at certain times. Is the host on at all times even? It may be in the room but if it is not turned on for most meetings what use is this. Assumptions are a sign of poor planning and a lack of understanding of the issues. How hard is it to ask a simple question first?

Craig

From: Mike Kuriger [<mailto:m@xxxxxx>]
Sent: Sat 29/07/2006 3:40 AM
To: Craig Wright
Cc: Matt Burnett; shiri_yacov@xxxxxxx; pen-test@xxxxxxxxxxxxxxxxxxxx

The whole point of the challenge is that the employee told his boss that a hacker could get into the laptop and spy on meetings. We should assume that the laptop is on the network, and that the challenge requires making the recording from a remote location. Anyone can plant a bug, but the employee is making a case that there already is a bug in place (the laptop)

~Mike~

re: Covert Microphone Application

Craig Wright wrote:

How about not all making assumptions on how the machine is configured etc.

No body has asked if the machine is networked– you are all making an assumption that may be invalid. What O/S is the host running. Statistically the likelihood is XP not Linux. Thus telnet is likely disabled.

Even if it is XP, is Remote admin/desktop enabled or disabled by policy. Is the host on a domain etc etc etc.

Ask some questions, don't make assumptions.

Craig

-----Original Message-----

From: Matt Burnett [<mailto:marukka@xxxxxxx>]

Sent: Friday, 28 July 2006 1:58 AM

To: shiri_yacov@xxxxxxxxxx

Cc: pen-test@xxxxxxxxxxxxxxxxxx

Wouldnt it just be a lot easier for you or your boss to disconnect the microphone cable than going though some elaborate scheme to prove it could possibly be done? If they can "ruled" any laptop at will then couldnt they also get into your mail servers? Wouldnt anything that would be discussed in your meeting generate followups in a email?

On Jul 26, 2006, at 4:55 AM, shiri_yacov@xxxxxxxxxx wrote:

Hi all,

I have recently entered with my boss to our corp. conference room to discover a new (shining) internet laptop on a side desk in the room.

During our chat I mentioned that the laptop has a builtin microphone and therefore enables covert eavsdropping in case the laptop is "ruled" from remote position, and therefore, a conference room PC should have no builtin mic.

My sceptic boss replied instantly – "I challange you, bring me a recording of any meeting – I'll replace the laptop, and you`ll receive it."

I therefore need a small covert application (no need in process hiding), which will record microphone input to file. command line application is perfect.

re: Covert Microphone Application

Do any of you know any ?

Guys, I gotta have this laptop...

Regards,

Shiri

--

Mike Kuriger
Sr. Systems Engineer
WarnerBros Online
818-977-8198
m@xxxxxx
aim - mikekuriger

Like a seedling in Spring, green and vulnerable.

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution - Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
