

[REVS] Remote Rogue Network Detection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Dec 2005 15:43:09 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Remote Rogue Network Detection

SUMMARY

Unauthorized network links are one of the biggest problems facing large enterprise networks. Users intent on bypassing corporate proxies will often use cable modems, wireless networks, or even full-fledged T1s to access the Internet. These network links can have a drastic affect on organizational security; any perimeter access controls are completely bypassed, making it nearly impossible for the administrators to effectively concentrate their monitoring and intrusion prevention efforts. The linked document attempts to describe different approaches and techniques that can be used to detect these rogue network links.

DETAILS

The Limitations:

The techniques listed in this document will not be able to find all rogue network connections with anything near perfect accuracy. Workstations that block all incoming traffic from the corporate network would not be possible to identify through any active detection methods. Systems that are not used to access corporate web sites or email are immune to the web tracking techniques. VPN traffic that is tunneled through an outbound SSL connection would be very difficult to detect without a man-in-the-middle

[REVS] Remote Rogue Network Detection

interceptor or private key compromise. Network anomaly detection is only valid when you have a known good baseline to compare against.

Three Approaches:

There are three distinct approaches covered in this document. They each have different requirements, levels of accuracy, and user-impact levels. The actual effectiveness of each approach will heavily depend on the configuration of the network and the way that users interact with it.

To read the full document please visit:

<http://metasploit.com/research/misc/rogue_network/>
http://metasploit.com/research/misc/rogue_network/

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fdlist@xxxxxxxxxxxxxxxxxxxx>> H D Moore.

The original article can be found at:

<http://metasploit.com/research/misc/rogue_network/>
http://metasploit.com/research/misc/rogue_network/

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [***\[REVS\] Perl Format String Vulnerabilities***](#)
 - Next by Date: [***\[NEWS\] MultiVOIP Buffer Overflow***](#)
 - Previous by thread: [***\[REVS\] Perl Format String Vulnerabilities***](#)
 - Next by thread: [***\[NEWS\] MultiVOIP Buffer Overflow***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)