From: Ofir Arkin [ofir@itcon-ltd.com]
Sent: ÈÂÌ ÁÓÈ˘È 31 ‡Â,ÂÒË 2000 13:40
To: bugtraq@securityfocus.com
Subject: IP TTL Field Value with ICMP (Oops - Identifying Windows 2000 again and more)

The IP TTL field value with ICMP has two separate values, one for ICMP query
messages and one for ICMP query replies.

The TTL field value help us identify certain operating systems and groups of
operating systems. It also provide us with the simplest means to add another
check criteria when we are quering other host(s) or listening to traffic (sniffing).

A. IP TTL Field Value with ICMP Echo Replies
If we would look at the ICMP Query Replies IP TTL field value than we see some
patterns:

- UNIX and UNIX-like operating systems use 255 as their IP TTL field value
  with ICMP query replies.
- Compaq Tru64 5.0 is the exception, using 64 as its IP TTL field value
  with ICMP query replies.
- Microsoft Windows operating system machines are using the value of 128.
- Microsoft Windows 95 is the only Microsoft operating system to use 32 as its
  IP TTL field value with ICMP query messages.

With the ICMP query replies we have two operating systems that are clearly
distinguished from the other - Windows 95 and Compaq Tru64 5.0. Other operating
systems are grouped into the 255 group (UNIX and UNIX-like) and into the 128
group (Microsoft operating systems).

Operating Systems tested:
LINUX Kernel 2.2.x, Kernel 2.4t1-6; FreeBSD 4.1,4.0,3.4; OpenBSD 2.7,2.6; NetBSD
1.4.2; Sun Solaris 2.5.1,2.6,2.7,2.8; HP-UX 10.20, 11.0; AIX 4.1, 3.2; Compaq
Tru64 5.0; Irix 6.5.3,6.5.8; BSDI BSD/OS 4.0,3.1; Ultrix 4.2-4.5; OpenVMS 7.1-2;
Windows 95/98/98SE/ME; Windows NT 4 Workstation SP3, SP4, SP6a; Windows NT 4
Server SP4; Windows 2000 Professional, Server, Advanced Server.

B. IP TTL Field Value with ICMP Echo Requests
One would expect that both IP TTL field values would be the same ...
This is not true in the case of some operating systems.

- LINUX Kernel 2.2.x & 2.4.x use 64 as their IP TTL Field Value with ICMP Echo
  Requests.
- FreeBSD 4.1, 4.0, 3.4; Sun Solaris 2.5.1, 2.6, 2.7, 2.8; OpenBSD 2.6, 2.7,
  NetBSD and HP UX 10.20 are using 255 as their IP TTL field value with ICMP Echo
  requests. With the OSs listed above the same IP TTL Field value with any
  ICMP message is given.
- Windows 95/98/98SE/ME/NT4 WRKS SP3,SP4,SP6a/NT4 Server SP4 - all using 32
  as their IP TTL field value with ICMP Echo requests.
- Microsoft windows 2000 is using 128 as its IP TTL Field Value with ICMP Echo
  requests.

We can distinguish between LINUX, Microsoft Windows 2000, The Other Microsoft
OSs (32 group), and the 255 group.

What if we do not get a match?
Than we know that some one changed the default TTL field value in his machine.

Please note that some networking devices might have values similar to those presented here.

Some might say, that setting the default TTL value with ICMP could be altered.
True. Just do it!

Ofir Arkin [ofir@itcon-ltd.com]
Senior Security Analyst
ITcon, Israel.
http://www.itcon-ltd.com

Personal Web page: http://www.sys-security.com

"Opinions expressed do not necessarily
represent the views of my employer."