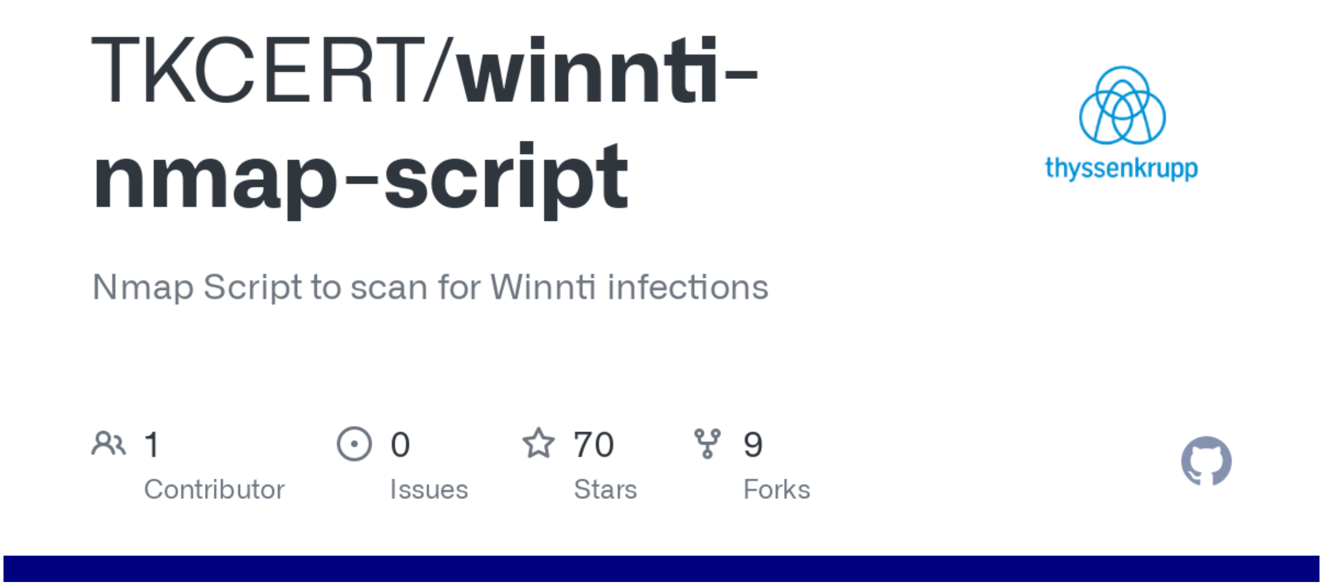
Nmap Script to scan for Winnti infections

github.com/TKCERT/winnti-nmap-script

TKCERT



TKCERT/winnti-nmap-script

Nmap Script to scan for Winnti infections

1 Contributor

0 Issues

70 Stars

9 Forks

This Nmap script can be used to scan hosts for Winnti infections. It uses parts of Winnti's protocol as seen in the wild in 2016/2017 to check for infection and gather additional information.

Winnti

Winnti is a malware that is used by some APT groups.

It has been used since at least 2013 and has evolved over time. You can find some information here

- https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf
- https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
- https://hitcon.org/2016/pacific/0composition/pdf/1201/1201%20R2%201610%20winnti%20polymorphism.pdf

SecOps Warning

WINNTI ONLY SUPPORTS ONE CONNECTION AT A TIME. IF YOU SCAN A HOST FOR WINNTI YOU WILL RESET THE CURRENT CONNECTION IF THERE IS ONE.

Requirements

This script needs **liblua 5.3** to work. You may want to download the latest Nmap version to get support out of the box (confirmed working with Nmap 7.25BETA2 and 7.60).

Installation

```
user@mint ~/src $ wget https://raw.githubusercontent.com/TKCERT/winnti-nmap-script/master/winnti-detect.nse
user@mint ~/src $ wget https://nmap.org/dist/nmap-7.60.tar.bz2
user@mint ~/src $ tar xvf nmap-7.60.tar.bz2
user@mint ~/src $ cd nmap-7.60
user@mint ~/src/nmap-7.60 $ apt install build-essential
user@mint ~/src/nmap-7.60 $ ./configure && make
user@mint ~/src/nmap-7.60 $ ./nmap -sT 127.0.0.1 -p 80,631 --script ../winnti-detect.nse

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-10 12:25 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0018s latency).

PORT    STATE  SERVICE
80/tcp  closed http
631/tcp open   ipp

Host script results:
| winnti-detect:
|   PORTS
|_      631 clean

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Show script help

```
 $ nmap --script-help winnti-detect.nse

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-09-26 17:00 CEST

winnti-detect
Categories: malware safe
https://nmap.org/nsedoc/scripts/winnti-detect.html
  The winnti-detect script checks if the host is backdoored by winnti rootkit.  It
  sends a winnti command to the first three open TCP ports and checks the
  response. When the connection to one of these ports fails, the next port is
  chosen until three successful tries are completed.  When a winnti infection is
  found the script gathers basic host information by sending a query to the
  backdoor and printing the response. Version 1.0, 2016-09-26

  *** SECOPS-WARNING ***

  Winnti only supports one connection at a time. If you scan a host for winnti
  you will reset the current connection if there is one.

  *** IMPORTANT ***
  Winnti installations may use different encryption keys. The default value
  included in this script is 0xABC18CBA (taken from a real sample).
  You can set a custom key with --script-args key=0x........
  The key must be given in big-endian.
```

Run Detection

```
 $ nmap --script winnti-detect.nse 10.10.0.2

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-09-26 16:37 CEST
Nmap scan report for 10.10.0.2
Host is up (0.013s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| winnti-detect:
|   PORTS
|       135 found WINNTI
|       139 skipped
|       445 skipped
|     49152 skipped
|     49153 skipped
|     49154 skipped
|     49155 skipped
|     49156 skipped
|     49157 skipped
|   HOSTINFO
|     Hostname:  SRV1
|     Winnti-ID: NKASJ-OQMDA-NDKQP-AJNCK-MQLAI_
|     Hostname2  XXXXXXXXXX-t
|_    Domain     XXXXXX

Nmap done: 1 IP address (1 host up) scanned in 6.11 seconds
```

Winnti static key

Winnti installations may use different encryption keys. The default value included in this script is 0xABC18CBA (taken from a real sample). You can set a custom key with --script-args key=0x........ The key must be given in big-endian.