

THE SH3LLC0D3R'S BLOG

HOME CONTACT CTF WALKTHROUGHS EXPLOIT DEVELOPMENT MOBILE SECURITY NETWORK

SECURITYTUBE - LINUX ASSEMBLY EXPERT 32-BIT SECURITYTUBE - OFFENSIVE IOT EXPLOITATION SECURITYTUBE EXAMS

CISCO EMBEDDED

Home / VulnServer / Fuzzing VulnServer with Peach

Fuzzing VulnServer with Peach

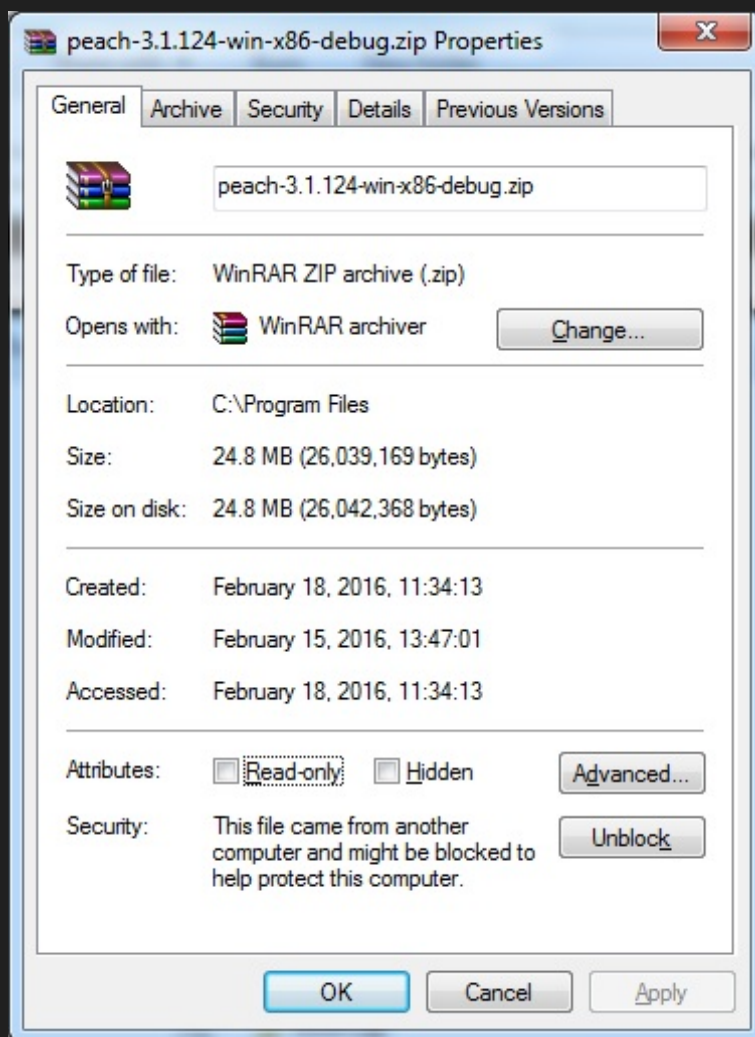
📅 February 19, 2016 👤 elcapitan 🏷️ VulnServer

I followed [this tutorial](#), however I had installation problems. I decided to write down the steps to set up the whole environment.

1, First I created a Window7 32 bit VMWare image. (I could not run it on Windows XP.) I disabled the Firewall. (Firewall is not a big problem, but if we let it run, we have to enable the VulnServer and Peach. It is easier if we simply disable it.)

This blog is dedicated to my research and experimentation on ethical hacking. The methods and techniques published on this site should not be used to do illegal things. I do not take responsibility for acts of other people.

2, Then I downloaded the Peach from [here](#). I right-clicked on the zip file and pressed the Unblock button. Without this step I had problems with running Peach as it came from untrusted source.



RECENT POSTS

Androguard usage

How to debug an iOS application with Appmon and LLDB

OWASP Uncrackable – Android Level3

OWASP Uncrackable – Android Level2

How to install Appmon and Frida on a Mac

CATEGORIES

Android (5)

Fusion (2)

IoT (13)

Main (3)

Mobile (6)

Protostar (24)

SLAE32 (8)

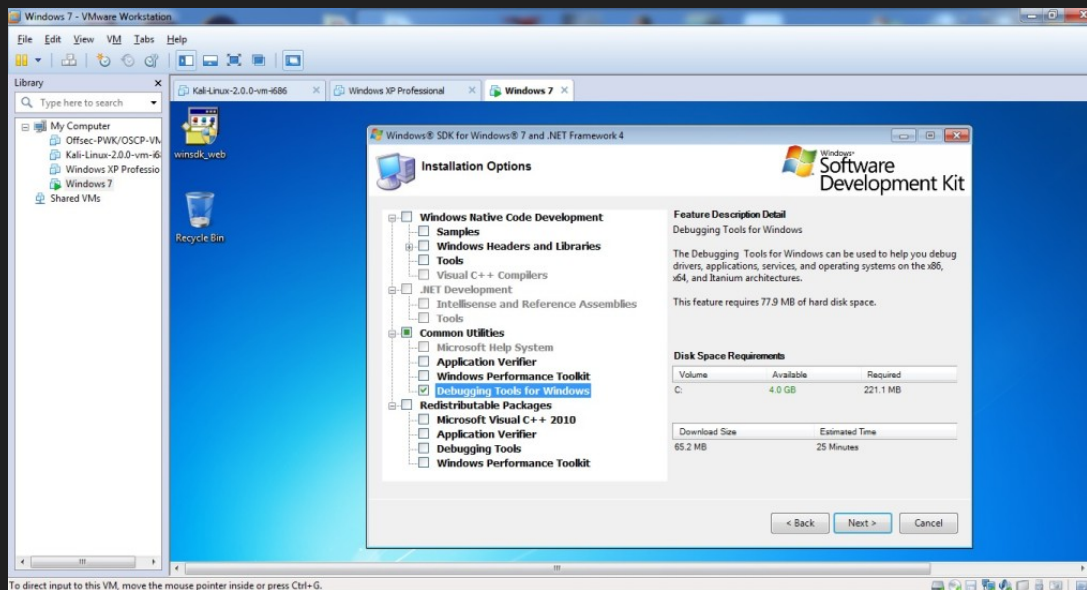
VulnServer (6)

Windows Reverse Shell (2)

Then I extracted the zip file into 'Program Files' folder and renamed it to Peach.

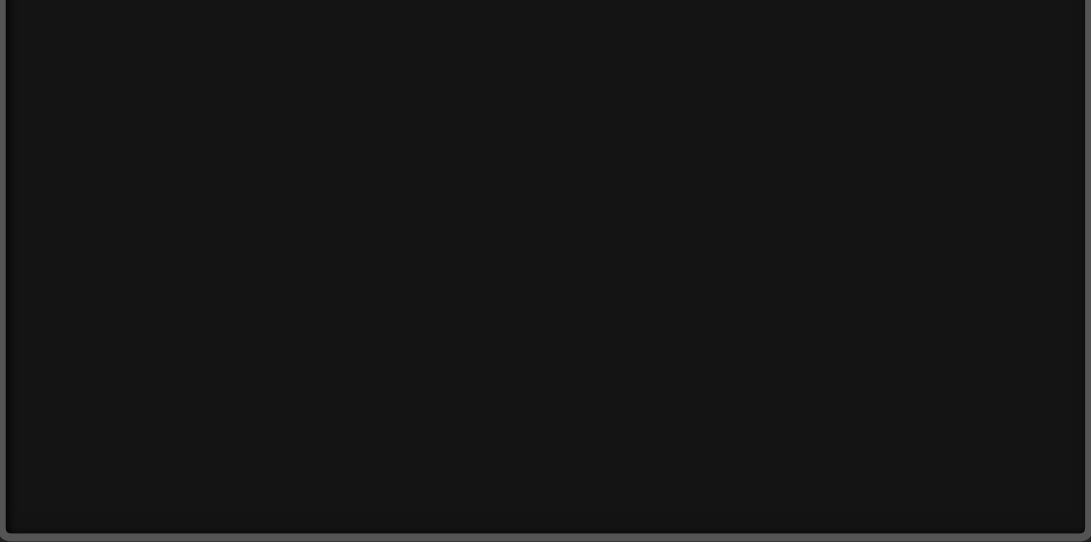
3, I downloaded the .NET Framework from [here](#). I installed it. This is necessary before we try to install the Windows SDK.

4, I downloaded the Windows SDK from [here](#). This contains the WinDbg. I installed it and selected only the 'Debugging Tools for Windows' during installation.



5, I installed the VulnServer into C:\.

6, I created the XML file for Peach. I saved it as 'C:\Program Files\Peach\htr.xml'.



7, I opened a Command Prompt, navigated to 'C:\Program Files\Peach' and executed the following command line:

peach -a tcp

This will start the Peach Agent.

```
Administrator: Command Prompt - peach -a tcp
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation

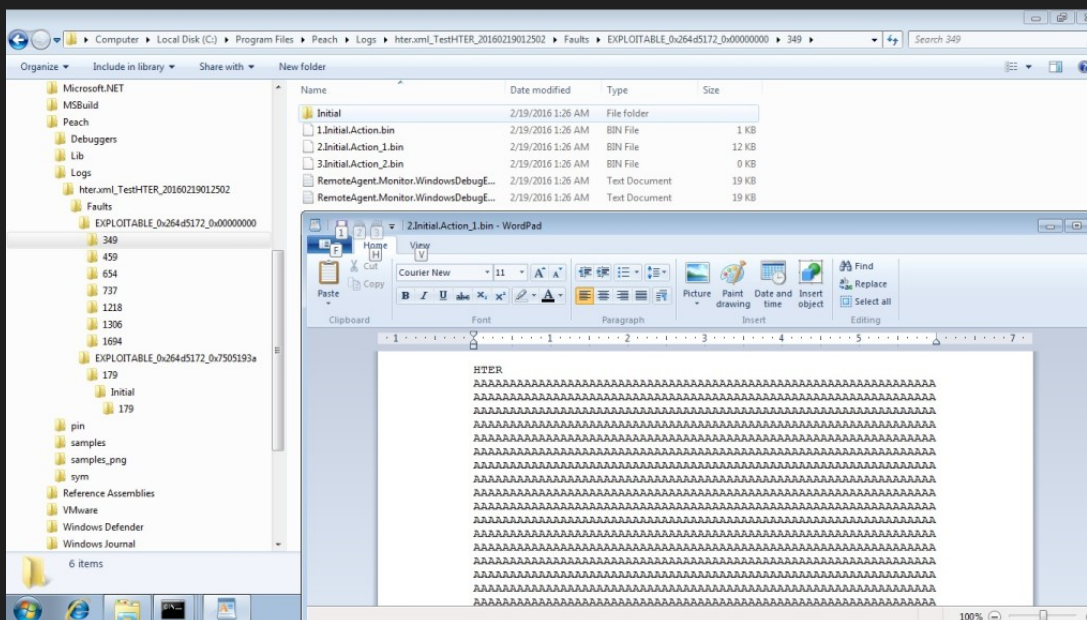
C:\Windows\system32>cd\
C:\>cd "Program Files"
C:\Program Files>cd Peach
C:\Program Files\Peach>peach -a tcp

[[ Peach v3.1.124.0
[[ Copyright (c) Michael Eddington
[*] Starting agent server
-- Press ENTER to quit agent --
```

8, I opened another Command Prompt, navigated to 'C:\Program Files\Peach' and executed the following command line:

peach hter.xml TestHTER

If the Peach Fuzzer finds a vulnerability, it will log it into the 'C:\Program Files\Peach\Logs' folder. The file with .bin extension will contain the data, that is sent by Peach and caused exception.



« PREVIOUS POST

NEXT POST »

Copyright © 2019, The sh3llc0d3r's blog. Proudly powered by
WordPress. Blackoot design by Iceable Themes.

Home Contact CTF walkthroughs Exploit development
Mobile Security Network
SecurityTube – Linux Assembly Expert 32-bit
SecurityTube – Offensive IoT Exploitation SecurityTube exams
CISCO Embedded