BINARY EXPLOITATION TUTORIALS

by dropzone

This article was first posted on GREYSEC.NET. This document contains the thread's initial message. To follow the full discussion, please visit https://greysec.net/showthread.php?tid=560.

Inspired by Insider's *Exploit Tutorial* thread (http://greysec.net/showthread.php?tid=559), I figured since we don't have much on this topic I'd put together a list of some of the solid resources out there for binary exploitation. One requirement for this list is that I'm focusing on free, online resources. If you want to add something don't add paid courses, or books, or anything else that isn't freely accessed online and, naturally this is for binary exploitation only.

Introduction to Software Exploitation - http://opensecuritytraining.info/Exploits1.html

In my opinion this is the best resource out there for learning the basics. It covers the basics, you won't learn about modern mitigation but you'll learn the core concepts that haven't changed.

***Corelan* Exploit Writing Tutorials - https://www.corelan.be/index.php/2009/07...overflows/**

There are 11 parts to the tutorials starting with the linked one. It is Windows focused and it starts on familiar ground if you did the *OpenSecurityTraining* course but quickly gets into material not covered by that course such as dealing with stack canaries, and writing egg hunters. If you're thinking you just want to hack servers running Linux, don't worry just because there is a windows focus and some of the content is more applicable to exploiting windows machines its good to learn and the knowledge does transfer.

Exploits 2: Exploitation in the Windows Environment - http://opensecuritytraining.info/Exploits2.html

Another *OpenSecurityTraining* course, this time focused on windows techniques. It covers much of the same material the *Corelan* tutorials cover so you might find yourself skipping stuff(be sure to do the labs though).

Modern Windows Exploit Development - http://expdev-kiuhnm.rhcloud.com/2015/05/11/contents/

Yet another windows focuses resource, you'll find a lot of stuff is happening in the windows world now because of the malware industry using exploits to infect. This is a nice resource that covers multiple browser exploits right through to exploitation in IE10 and IE11. You'll also get exposure to dealing with *EMET* which is the Windows exploit mitigation system.

Project Zero - http://googleprojectzero.blogspot.com/

Okay, this one is a blog but they often post good write-ups of modern exploits. Its worth following, always good quality.

Heap Exploitation

Heap Exploitation, seriously there is so much awesomeness in heap exploits but its damn hard because you need to understand the system to full carry one out. Not only do you have to overwrite some data, but you need to overwrite it in such a way so that when its operated upon it it leads to doing what you want. And what you want it to do is modify other areas so that when those areas are acted upon you'll start to get some control... There is a lot of indirection in heap exploits. Its covered a bit in the above resources but these are the classic resources.

Vudo Malloc Tricks - http://phrack.org/issues/57/8.html
Once Upon a Free() - http://phrack.org/issues/57/9.html
Advanced Doug Lea's malloc exploits - http://phrack.org/issues/61/6.html
Exploiting the Wilderness - http://seclists.org/vuln-dev/2004/Feb/0025.html

Four classic papers on heap exploitation. They are indeed classics but are for vulnerabilities that no longer exist. Yet they are not a waste, like I said they are classics and understanding the old methodology helps with the newer techniques.

Malloc Maleficarum - http://seclists.org/bugtraq/2005/Oct/0118.html

Back in 2005 after the above exploits had been patched this paper was released. Its purely theoretical, no walk through or demo code. This paper was merely to open the minds of hackers to the possibility that heap exploitation was still a possibility and detailed several attacks that were still viable after the initial patches. Some of these attacks are still viable today in the current Linux *allocator* ptmalloc2.

.aware eZine Alpha - House of Mind - http://www.awarenetwork.org/etc/aware.ezine.1.alpha.txt

In 2006, a practical paper was released detailing exploitation of one of the attacks from *Malloc Maleficarum*: House of Mind. This is a practical walk through of some exploitable code.

Malloc Des-Maleficarum - http://phrack.org/issues/66/10.html

More of the attacks from *Malloc Maleficarum* are proven in this paper, *walk through* and just good, eye-opening exploitation.

The House Of Lore: Reloaded - http://phrack.org/issues/67/8.html

It took all the way until 2010 for House of Lore from the *Maleficarum* paper to fall from he same guy who wrote *Des-Maleficarum* he finished the job.

If you're looking for more...especially more modern or exotic stuff consider reading CTF write-ups. CTF organizers often keep on top of new exploit development 'trends' and will base challenges on them. So in the write-ups you get all the cool stuff without the extras hassles that come from big, modern systems.