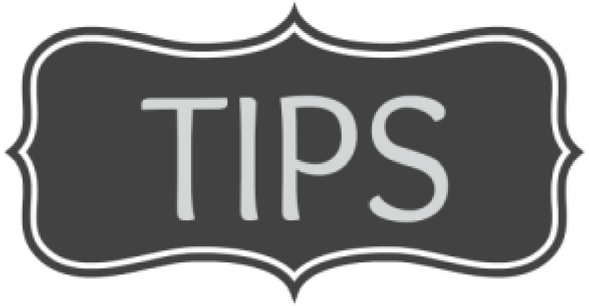
SCHMIDT HAPPENS – NETSEC BLOG

Blog about my experience and journey in netsec / cybersecurity.

HOME HACKING TUTORIALS ACTIVE DIRECTORY HACKING TUTORIALS ABOUT ME LINKEDIN

PWK/OSCP HELPFUL TIPS & RESOURCES

POSTED ON JULY 9, 2019 BY RUMHAM



I've found myself giving people plenty of pointers and links that I think helped me out when I was doing the PWK coursework and the labs for OSCP. So because of that, I figured I'd actually collect everything in one spot and I can just refer anyone interested here. I'll update this as I think of anything else. Skip to the bottom if you are just interested in any helpful links.

Buffer Overflows

This is often the most daunting thing to a student pursuing OSCP. Mostly because it's such a foreign topic. Fortunately for anyone reading this — I can assure you it's not that bad. Here is what I did:

First off, I watched the provided videos from the PWK coursework. I watched them about twice. This helped build a little idea of whats happening and understand some of the terminology.

Second, I read through the PDF. This again reinforced everything I just saw in the videos. The provided screenshots helped take a longer look at the output and allowed me to see a bit more.

Okay, now you've got an okay understanding. Now it's time to go slowly and methodically through the actual work. Follow the videos yet again closely, pausing and rewinding as necessary. Once you've gone through it and popped shell, you're ready to do it all over again. I went through it over and over and over, documenting it EACH time. Yes, each time. It is annoying, boring, and will make you hate the process — however, you will 100% memorize the steps. Now what I did, is perform all the steps from memory a few times over. This ensured that I knew what I was doing yet again.

Lastly, this is probably not necessary, but I gave a friend a class on how to perform a buffer overflow from scratch.

Note: I built my own little lab environment for this step and did NOT share my screen showing any sort of PWK/OSCP coursework, lab machines, etc. This was 100% my own environment that I built, because I did not want to break the rules.

When giving the mini-class, I explained what I was doing in each step, and why I was doing it. I also explained why certain steps were working, and how it will help me pop shell. This took me about 35-45 minutes to walk through buffer overflow with my friend, and I knew the content inside and out. Because of this, I popped shell for buffer overflow in my exam in probably 25-30 minutes. Easy day.

Notes

If you don't hate yourself, take better notes than I did. Document everything you think can be helpful. I initally used Keepnote, but it turned out to sort of suck in my opinion so I switched to CherryTree. If I could do it all over again, I would use a combination of OneNote and CherryTree.

OneNote should be used for all little helpful tidbits of information + coursework. CherryTree should be used to documenting every step of rooting a box from Enumeration to Post exploitation.

My notes were absolutely abysmal and I really regretted it later on during the labs because I wanted to reference back to something, but I had incomplete or missing information. Now my note taking skills are insanely thorough and meticulous. Make sure to document EVERYTHING.

Helpful Links

> https://www.hugohirsh.com/?p=509 (SLMail Buffer Tut)
>
> http://blog.guif.re/2017/11/minishare-141-remote-buffer-overflow.html (Minishare Buffer Tut)
>
> https://nmap.org/nsedoc/scripts/ (Nmap Script Library)

https://411hall.github.io/JAWS-Enumeration/ (JAWS)

https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc (PowerUp.ps1)

https://github.com/rasta-mouse/Sherlock (Sherlock)

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet (Reverse shell cheat sheet)

https://netsec.ws/?p=331 (Metasploit Payloads)

https://netsec.ws/?p=337 (Spawning TTY Shell)

https://www.fuzzysecurity.com/tutorials/16.html (Windows PrivEsc)

https://blog.ropnop.com/transferring-files-from-kali-to-windows/ (File Transfer methods)

https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-

> shells (Escaping SSH Jail)
>
> https://blog.techorganic.com/2012/10/06/introduction-to-pivoting-part-1-ssh/ (Pivoting Pt 1)
>
> https://blog.techorganic.com/2012/10/10/introduction-to-pivoting-part-2-proxychains/ (Pivoting Pt. 2)
>
> ❜❜

POSTED IN **UNCATEGORIZED**

ELEARNSECURITY WAPTV3 TRAINING BEGINS

ABOUT ME

Matt Schmidt
B.S. Information Technology
OSCP, Security+

RECENT POSTS

PWK/OSCP Helpful Tips & Resources

eLearnSecurity WAPTv3 training begins

Getting Sponsored to go to BSidesLV, then tagging along to Defcon 27

AD Hacking: Pass The Hash

AD Hacking: NTLM Relay Tutorial

Search … Search

ARCHIVES

July 2019

June 2019

May 2019

April 2019

March 2019

January 2019

November 2018

CATEGORIES

CTF

Misc.

Uncategorized