DeepSec 2017 Talk: XFLTReaT: A New Dimension In Tunnelling – Balazs Bucsay

Posted on **October 07,2017** by **sanna**

"Our new tool XFLTReaT is an open-source tunnelling framework that handles all the boring stuff and gives users the capability to take care of only the things that matter", says Balazs. "It provides significant improvements over existing tools. From now on there is no need to write a new tunnel for each and every protocol or to deal with interfaces and routing. Any protocol can be converted to a module, which works in a plug-and-play fashion; authentication and encryption can be configured and customised on all traffic, and it is also worth mentioning that the framework was designed to be easy to configure, use and develop."

We askedBalazs Bucsay a couple more questions about his talk:

Please tell us the top 5 facts about your talk.

1. *Tunnelling is not new at all, but this framework is and it unites all the techniques into one.*
2. *The talk includes some low level information as well, it can be easily understood because it will start with the basics and build upon that.*
3. *Live demos will be presented and it will be revealed how easy it is to use the framework and to create working tunnels by selecting the appropriate protocol.*
4. *I will give recommendations for both red and blue teams. Both teams can use the tool to discover and exploit vulnerabilities and misconfigurations on the network. The blue teams can try to detect the hidden data flow, red teams can tunnel connections and exfiltrate data with the framework.*
5. *This framework is awesome.*

How did you come up with it? Was there something like an initial spark that set your mind on creating this talk?

I was in this situation so many times before where I needed unfiltered Internet access on a (filtered) network or just a reliable channel to exfiltrate data as a proof for the client. Unfortunately there were no proper solutions for this, or different tools had to be used. I got bored with this situation and started to play with the thought that there might be a way this could be modelled and coded into a framework. As of now, my original idea seems to be working and the same basic approach works with all the protocols, a module can be created just for tunnelling and all the other stuff is handled by the framework.

Why do you think this is an important topic?

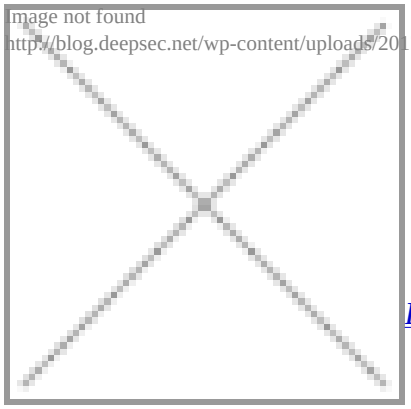
I rather think that this part of IT-Security had to be fixed. If you take a look at the conferences, talks, researches etc., they always try to find new things, new ways to bypass protections or to exploit vulnerabilities but not many people try to improve existing topics. I do not always agree with that approach. I think it is more important to create stable baselines and do research with those rather than creating useless Proof of Concepts. Tunnelling is certainly not a new thing, but have you ever tried to do tunnelling over several protocols? Or use a transport protocol, which is not a typical one? I can tell you, it was a pain and I think I helped on this, now it is a bit easier than it was, and this is what matters to me.

Is there something you want everybody to know - some good advice for our readers maybe?

Do not come to my talk. Just kiddin'. I am Hungarian, I can be bribed with beers, club mate and/or good chats. Come and see me, have your questions and hopefully your answers, join the development, make requests and create issues on Github.

A prediction for the future - what do you think will be the next innovations or future downfalls when it comes to particularly your field of expertise / the topic of your talk?

The world gets more and more digitalised, there will be more breaches all around. We already got used to it and I do not think this will change in a good way. The only thing that we can do is that we try to take care of our own little sweepings to make sure we are not the ones who get breached.



Balazs Bucsay (@xoreipeip) is a Senior Security Consultant at NCC Group in the United Kingdom who does research and penetration testing for various companies. He has presented at many conferences around the world including Honolulu, Atlanta, London, Oslo, Moscow, and Vienna on multiple advanced topics relating to the Linux kernel, NFC and Windows security. Moreover he has multiple certifications (OSCE, OSCP, OSWP, GIAC GPEN) related to penetration testing, exploit writing and other low-level topics; and has degrees in Mathematics and Computer Science. Balazs thinks that sharing knowledge is one of the most important things in life, so he always shares his experience and knowledge with his colleagues and friends. Because of his passion for technology, he starts his second shift in the evenings, right after work, to do further research.

Posted in:Conference,Security | Tagged:DeepSec,Exfiltration,Framework,Hacking,Talk | With 0 comments