Information security - IV

Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 56
Re-cap of all topics

So, as we are nearing the end of this Information Security Level 4 course; we will actually spend a few minutes in this module as a Re-cap of all the topics that we had discussed till now in the IS course level 4. So, we actually had started looking at initially the; recap of the IS level three course where we actually went and defined; what is network security, what kind of cryptographic a mechanisms are there like a symmetric key, asymmetric key and so, on. Then we basically started talking about different types of tools that we are actually looked at like a firewall, like the kind of packet filtering that one could actually do and so, on.

So, all this initial thing was more recap of what we are actually discussed as a summary of the IS level three course just to ensure that we are having the basics refresh before, we actually go in into these specific topics of this particular level four course. So, in the level four we actually started looking at the initial penetration testing introduction of how kali Linux with different kinds of tools is actually helping us do a penetration testing effort.

So, we started off with a trying to understand, how we can actually have kali Linux installed on a server and made use of for this particular purpose. So, after we looked at the initial methodologies that one could actually adapt for doing the penetration testing; we looked at the different types of steps right from doing a reconnaissance stage in trying to understand the particular target and trying to get more details about the particular target. We started then subsequently looking at the different type of tools that we actually have right.

So, we basically classified the tools that is actually available in kali Linux under different heads, where in we started talking about tools that are typically available on the client side, tools that are actually available in the server side. So, for example, if one wanted to basically wanted to do password attack kind of a tool what kind of tools that he could potentially make use of and we also saw how to make use of those tools.

So, after looking at the different type of tools that we had in client side and on the server side we went into very expensive detail on how one could do different types of authentication attacks, where in we really looked at the tools that are typically adapted right from a trying to identify and sort of crack the passwords to doing different types of attacks after determining what kind of software is actually running on that particular target machine which the attacker is trying to bring down currently.

Different types of authentication attack tools was actually covered and then, we went into looking at the different types of tools that are actually available for basically trying to do a web based attack. So, where in we talked in detail about; how one could actually do a man in the middle attack with tools and how one could actually do a distributed denial of servers or a normal denial of servers attack which is very distractive on that particular target.

So, we actually had looked at the tools that could one could actually make use of for doing any of these kind of attacks over the web. So, after we had actually looked at it we also spend some time very briefly. In trying to understand from a network or a security administrator point of view, what kind of defensive counter measures that he or she could have actually adapt to sort of protect their network from the attacker meeting the objective of successfully bringing down a particular system.

So, we actually ah saw a few set of guidelines; like the stick guidelines or different kinds of password policy statements that one as an administrator could actually enforce on their systems. To minimize the possibilities of any of these attacks happening successfully right; so there by either it the attack is the possibility of the attack is completely eliminated or there is a less chance of the attack going unnoticed by the administrator before the objective of the attacker is actually met.

So, after looking at the different types of counter measures; that we as a administrator could typically adopt; we actually started looking at the different type of network forensic subjectives that one could actually have and what kind of tools that are actually available in kali Linux towards meeting the goals of network forensics. What possible best out comes could actually be had even though some of them could be impossible in terms of the final results and again what kind of evidences that has part of network forensics one will end to collect.

So as part of this we actually had looked at the different type of tools that are there which are used typically for collecting the network evidences like, protocol analysis tools, like Wireshark, then we also looked at different packet analysis technique that I could do. So, once I capture the packets in the network using a tool like wireshark one needs to do analysis of what kind of traffic is actually coming which has possibly resulted in the attack being successful.

So, this is where we looked at different type of packet analysis techniques that were there. And then based on the packet analysis we discussed in detail about a few flow analysis algorithms and tools after defining what is exactly a typical flow. Then we went into looking at challenges that are there in terms of a wireless network and what kind of very much easily possible attacks could be typically done on a wireless network.

So, based on that we actually went in and also define what we exactly mean by intrusion detection system and inclusion prevention system and how it is different as compared to a host based intrusion detection system and a network based intrusion detection system. So, we actually had seen a certain modules like; the start application which could actually be made use of for doing this intrusion detection and intrusion prevention related activities.

Then we also had a quick look at the firewalls and, what are the different possible configurations that I could have and how could I actually use the firewall lock measures details that is getting generated out of the firewall lock files to do an analysis of what exactly has happened? Then as an one of the very popular open source implementations, we had looked at the IP tables as the firewall implementation which is typically available on any open source Linux distribution. It actually has got complete and very sophisticated functionality from a firewall perspective.

So, we are actually seen some demonstration of that as well and finally as part of the end section; we actually had looked at a few of the log formats like syslog and rsyslog including; the triplet logs which actually stood for authentication, authorization and accounting right. So, these are the some of the typical logs that could come in handy for doing any kind of a postmortem analysis to sort of understand, how the attack has actually happened after it has happened with the intension that in future the same attacks or related type of attacks has to be actually prevented from happening on our system and on our network.

So, with that we actually come to an end of what exactly we had seen till now as part of this course. As part of the next four sessions remaining four sessions in this course we are going to be actually talking about very recent attack that was actually got exposed and also got good publicity the media called as the meltdown attack right.

So, we are going to see how this attack actually has happened and how the different topics that we are actually tried to be covering in a sequence right from our IS 1 till IS 4 is actually helping to prevent us from actually having any kind of an impact out of the this something some attack out of an attack like this like the meltdown that is, actually happened. So, if you have seen a media reports it s actually very serious attack that is actually possible inside the processor, because of the fact that it is tries to prefetch lot of things by passing the security mechanisms.

So, the next four sessions we going to actually have a coverage of what is this attack all about? How did that actually happened? And what kind of preventive mechanism that we have been all along discussing from our IS 1 course till the IS 4 which if it that been followed would have actually been sort of help us to minimize if not completely eliminate the possibility of getting impacted from an attack like this.

So, with that we come to an end of this quick recap modules session. So, we hope that you have enjoyed all the topics that we have actually covered as part of this module and we also hope that you enjoy the remaining four sessions in which the meltdown topic is going to be extensibly discussed and deliberated.

Thank you very much and wishing you all the best.