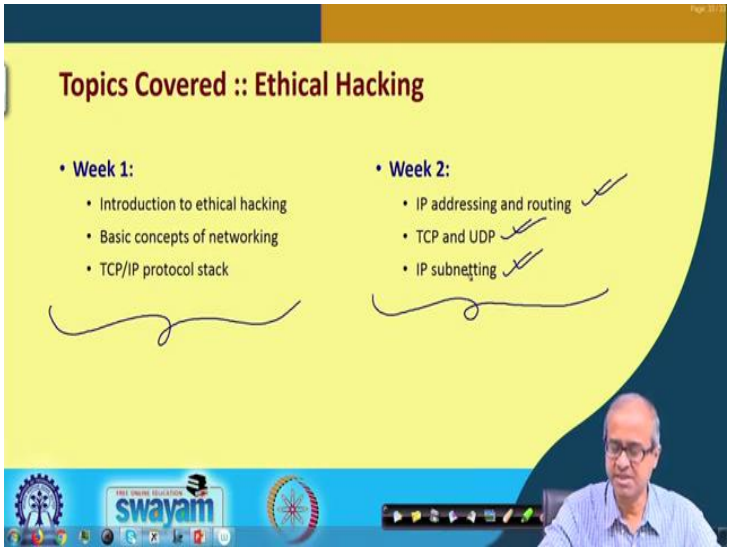
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 60
Summarization of the Course

So, over the last 12 weeks, we have discussed a number of topics and number of issues that are very related to the subject of Ethical Hacking. And some of the subjects which apparently are not very much connected to ethical hacking, but knowledge of those topics are essential to become a good ethical hacker. Now, in this last summarization lecture, I shall be trying to summarize, what are the things we have covered in this course over the last 12 weeks.

(Refer Slide Time: 00:53)



So, let us go week wise. In the first week, if you recall, we talked about some basic concepts of ethical hacking. What is the basic purpose of ethical hacking? What is the role of an ethical hacker, expected role of an ethical hacker and then we moved on to basic concepts of networking. Now, many of you have been asking in the forum that why we are discussing the basics of networking so much?

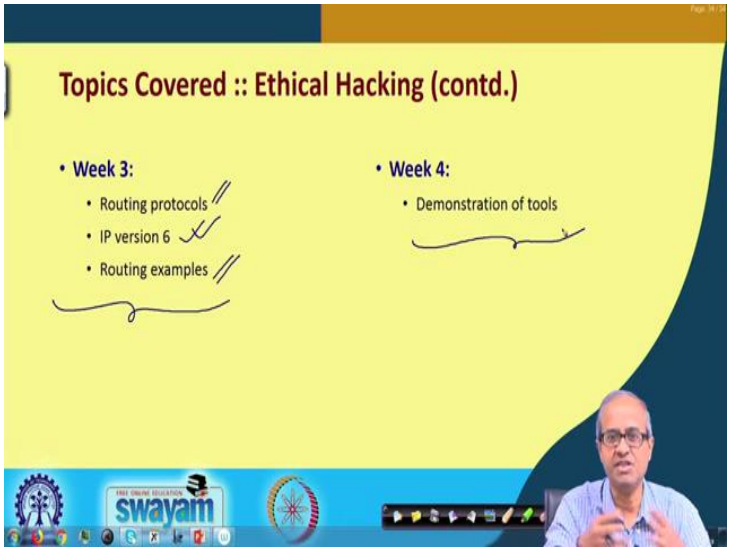
Well, by the end of this course you may have appreciated that unless you have a solid understanding over the basic concepts in networking, what are the types of packets? Why

they flow? How they flow? You will not be able to understand the working of many of the tools that are normally used in ethical hacking.

So, in this first week of the lecture, we talked about some of the basic concepts of networking and we introduced ourselves to the structure of the TCP/IP protocol stack. Then you continued in week 2, there also we continued with some basic networking concepts; specifically, we looked into some details about IP addressing and routing; how IP packets look like? What are the different fields, their purposes and so on.

Then you looked that the TCP and UDP protocol. So, how this TCP and UDP packets look like, connection establishment, the purpose of the different fields in the header and then we talked about IP subnets. What are subnets, the different ways to create subnets, how can we use subnet masks and so on and so forth. These were the topics that you are covered in week 2.

(Refer Slide Time: 02:51)

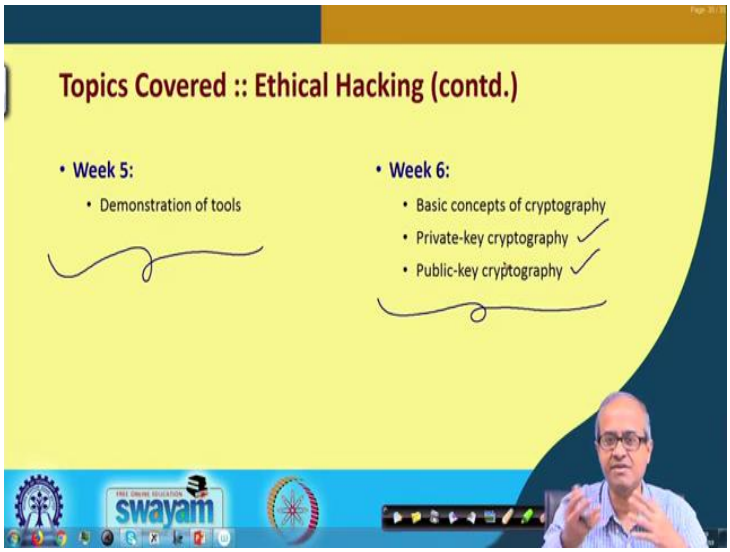


Then, in week 3 we talked about some of the routing protocols. The interior and exterior routing protocols; how packets are actually routed in the internet and we talked about the IP version 6 also which is being deployed in many networks as you already know. But, still most of the networks run IP version 4, the older version because of legacy considerations.

We looked at a number of examples, where we talked about how packets are routed with respect to some routing table examples; we illustrated the process of packet forwarding. We mentioned a very important concepts in this context; that if the destination address of a packet matches with multiple rows in the routing table, then we consider the particular row which is having maximum prefix match and the packet is forwarded to the corresponding interface.

Then in week 4, we had some demonstration of various tools. We talked about virtual box, we talked about Kali Linux, how different tools can be installed, and we also started some experiments with NMAPs. So, how this NMAP tool can be used; the various commands, simple commands can be used and so on, alright.

(Refer Slide Time: 04:29)



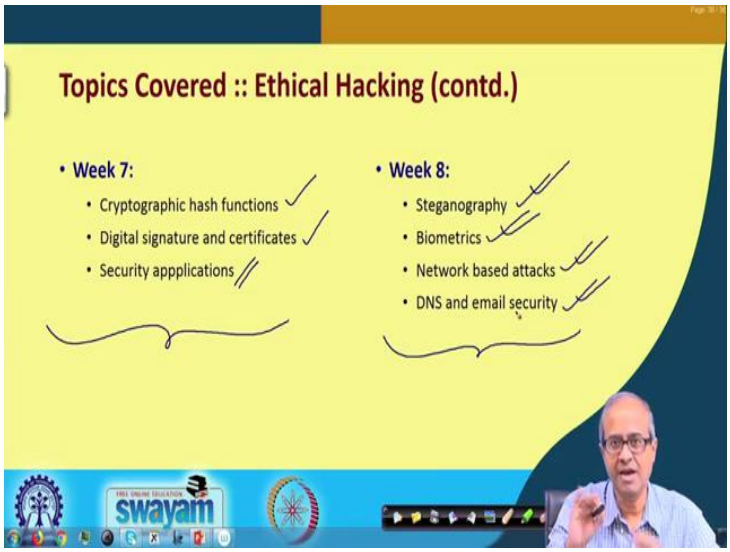
So, continuing to week 5, we continuing means, we continued some more demonstrations particularly with the NMAP tool as you have seen earlier. So, in the last few lectures; we again had a rule; we again had a re look at the NMAP tool to find out the various options available under NMAP and how they actually work. We try to give you also some explanation about the working of the different commands, how they work, ok.

Now, many of the network protocols that have meant for enhancing security are based on encryption of some data or some kind of authentication mechanism. So, you need some cryptographic tools and techniques. So, it is during week 6, we started some basic

tutorial on cryptography. We talked about some concepts of the cryptographic techniques. Specifically, we looked at the private and public key cryptographic algorithms. We mentioned that in the internet scenario, we need a combination of both public key and private key cryptography to efficiently share information over a secure channel.

Private key cryptography is fast; public key cryptography is slow; but public key has some very interesting advantages in the internet scenario. These are the things we had discussed.

(Refer Slide Time: 06:08)



And then coming to week 7, we continued with our discussion. We talked about cryptographic hash functions which are so very useful for carrying out or ensuring data authentication or entity authentication which also form the foundation to create digital signatures and certificates which are so useful in the present day context. And lastly, we look at some of the security applications, where all these things, this public key encryption, private key encryption, cryptographic hash function, they are used in combination in some particular way, ok.

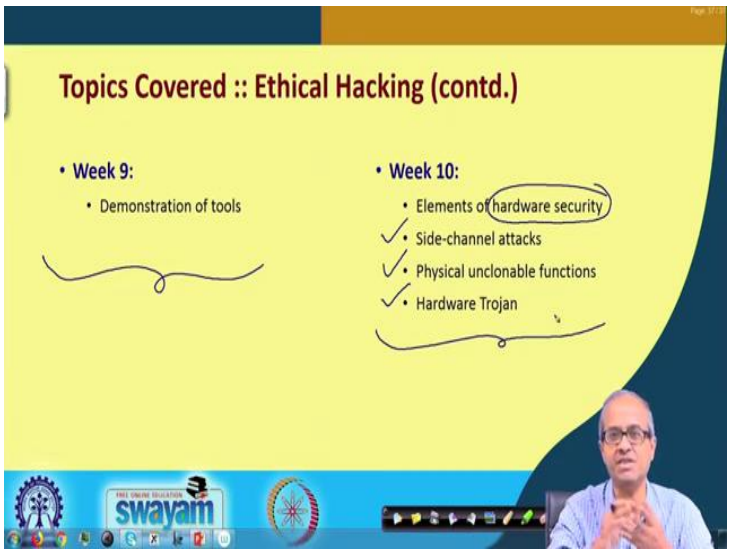
Then, week 8; we first talked about some of the slightly unconventional ways to ensure security, likes steganography or information hiding. We hide something inside something else so that casual looker will not feel the presence of the hidden information; that is steganography.

Biometrics is becoming so much useful nowadays, starting from iris, fingerprint, gait, then means various kind of hand gestures. So, different kinds of biometric trades are used to uniquely identify human beings. These are becoming important. So, some basic ideas and concepts we had discussed.

Then we talked about some of the network based attacks; that typically carried out to well, both for offensive and defensive purposes. If an ethical hacker, you will be doing that to identify vulnerabilities in the system. But if you are a malicious attacker, you are possibly trying to break into a system with some malicious intent.

Then lastly we took, we talked about two specific protocols which are important, DNS, name server and email and some security issues with respect to that.

(Refer Slide Time: 08:30)



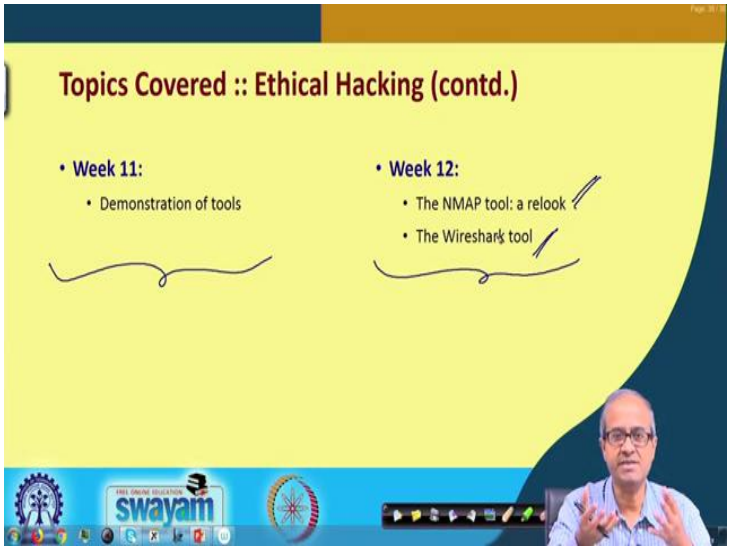
Then, week 9; again, we looked at some of the demonstrations of the tools with respect to various security and ethical hacking applications. And in week 10, we looked at a slightly different thing; we looked at some technologies related to hardware security.

Nowadays just ensuring software security is not enough; there are so many handle gadgets that we use, starting from mobile phones to so many other devices. And ensuring security at the hardware level for those devices is becoming that much more important. We talked about side channel attacks which can make a device vulnerable; because the

implementation is not safe enough; may be the algorithm is strong, but the implementation is weak.

We talked about physical unclonable function, which can make implementing hardware security easier and we have also mentioned something called hardware Trojan; we can, which can both make our systems safer. And can also make some systems you are getting from other places vulnerable, if you are not sure about what is there inside the system. So, these are some of the things that you had discussed.

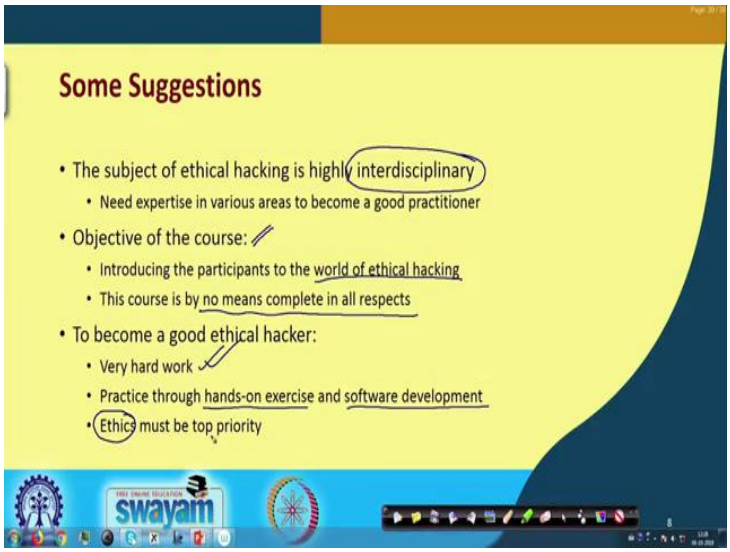
(Refer Slide Time: 10:03)



Then in week 11, again we looked at some tool demonstration. But, here mostly we looked at something like SQL injection attack; then accesses cross site scripting and so on, where application level security or website vulnerabilities were considered, ok. So, you had looked at number of tools.

And in this last week, we had a relook at the NMAP and the Wireshark tool which have already seen earlier in the demonstration sessions. But, we thought that if we more formally go through these tools, their functionalities and how they work, then it will be easier as an ethical hacker for you, to assimilate and do things in a proper way in the proper contexts, ok.

(Refer Slide Time: 11:06)



So, to summarize there are a few suggestions I would like to make; the first thing is the subject of ethical hacking is highly interdisciplinary. You need expertise in a lot of different subjects in order to become a good ethical hacker, a good practitioner in the field. So, if you feel that I will be doing one or two such courses and you will become an expert in ethical hacking you are absolutely wrong.

It requires years and years of hard work, decades of hard work to become a good ethical hacker. So, make it a point, remember that there is no alternative to hard work; you have to put in lot of hard work, lot of knowledge you have to gather to understand how it work. You see, just downloading some tools NMAP, Wireshark, running and doing something is not ethical hacking. You have to learn how think works; you have to build your own tools. Because, some customer some organization may ask you do something which is not readily available. You may have to develop your own tools for those purposes; but for that you have to understand how things work.

Now, as I mentioned repeatedly, the objective of this particular course is primarily to introduce you to the world of ethical hacking, introducing you to some of the basic concepts. We are a no way to trying to compete with the other courses that are available on the same subjects. We are not trying to make you experts in usage of the tools, not at all. But, our philosophy will be to introduce to the subject. And if some of you are motivated, get motivated by what we are trying to say, you will learn the subject

yourself, ok. You will be learning it in a way which is much better that what the other courses, the existing courses teach you to do. You will become an expert in your own write.

So, just to repeat, this course is by no means complete. We are just trying to put you on a proper platform from where you can start your learning process; your start, your learning process starts now. So, to become a good ethical hacker as I had said, you need to put in a lot and lot of hard work, hands on exercises and experiments; there is no alternative to that. You may need to develop a lot of tools on your own, because everything may not be readily available.

And lastly I am repeating, ethics must be your top priority. Do not do anything which may harm others physically, mentally or emotionally. That is not part of ethics. So, what we are trying to say, you learn the tools, do the experiments, but not at the expense our harming others, ok. So, if we are able to convey this message to you. We will feel that, we have been at least partially successful in achieving the objectives of this course. So, with these few words, we have come to the end of this course and you take this opportunity to thank you all for attending.

Thank you once again.