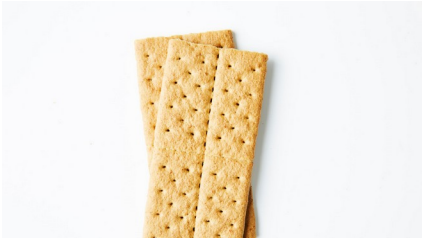
Real Security ™ course by Khawar Nehal

Real Security is different from other security courses in many ways.

We noticed that most of the courses tech topics which are related to cracking.

Before we confuse people we shall define cracking and hacking according to the RFC.

cracker



A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system. See also: hacker, Computer Emergency Response Team, Trojan Horse, virus, worm.

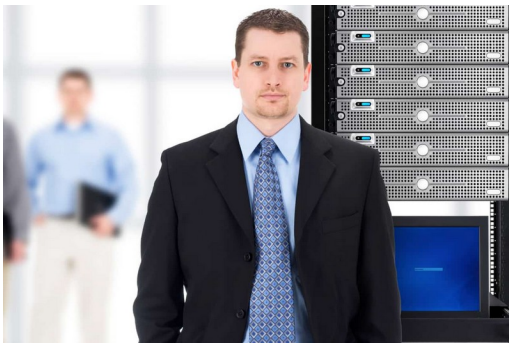
hacker

A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term. See also: cracker.

Most of the mass media and the mass public uses the word hacker to mean cracker.

When we say hacker we shall mean the “real” hacker who makes stuff vs break stuff.

Breaking stuff is what crackers do.



Since a lot of the people in the field of IT security define an ethical cracker as ethical hacker. So we shall clarify that too. By ethical it just means they have permission to test the network they are cracking. And unethical or what is termed black hat hacking is actually still “technically” cracking.

https://datatracker.ietf.org/doc/html/rfc1392

Now that we have cleared the meanings. Lets get back to the details of the topic. Security.

Over 10 years ago we learned that the security of the ISPs and Telecoms was different. They did not hire security people and did not need to worry about it. So we thought why is that. We came to the conclusion that it was due to their softwares. They used Unix and Linux and the others use less capable and buggy software. Due to the large number of holes and lax default configurations, it was the reason why the difference existed.

A few years ago we noticed something else. Reliability.

Before I explain how reliability is connected to security, I shall explain my 4 levels of security.

We have boiled security down into just 4 levels.

1. Physical security.
2. Software.
3. Configurations.
4. Social engineering on users who have some access, admin or super user access.

Each layer needs to be completed to allow the next layer to work.

Let me explain.

If you allow physical access, then the other 3 layers cannot do anything for security.

If your software has bugs in it, then configurations cannot help solve it and you do not need to worry about social engineering also.

If you complete physical security, make sure there are no known bugs in the software then you need to make sure there are no mistakes in the configuration.

If all three are completed then you can work on the last layer. The user. There are multiple ways to prevent social engineering attacks from the user layer.

One of the best is to eliminate the layer completely.
If you can make sure there is no way to access the machine then it shall work as a server and continue to do so. You can instruct the machine to update all software for any security related updates which become available.

Since servers need some modifications, make sure you can only access them through the LAN from a few restricted machines. This shall prevent access from everywhere.

Also setup a program inside the server to allow access only when you send a special instruction via a method only known to the program and you. This way access shall not be allowed at all times when the administrator is not requiring access.

Set the inside program to shut access after a few hours of granting it. The admin can reopen the access via the secret messaging method as needed.

For most admin related tasks like monitoring, make programs to send the information to the admin without requiring any access. Send all reports regularly and the admin can delete all the emails as needed.

Topics which shall be covered in the security course.

These topics are selected from the overall security related topics and we feel these are important to provide and maintain security. Most of the topics related to cracking have NOT been selected because they become useless if security is well maintained by the reliability maintenance methods described above.

We shall also be discussing which admin and user tasks can have gateways made or a single server manager deal with all of these tasks. This shall reduce the chances of configuration related mistakes even more. This method is a proprietary KN/ATRC method which shall be developed and refined further along with the participants of the courses, users and clients of ATRC.

Topics currently selected for the Real Security course.

VPN Concepts

OpenVPN Practical

Tor network concepts

Tor Browser Bundle Practical

Networking concepts.

Network packet filtering concepts.

IPTables practical

Email digital signing and encryption

Thunderbird with signing and encryption practical

How the Internet works concepts.

BIND DNS practical.

IP routing practical.

Suggestions with reasons for other topics are welcome.

Prerequisites : There are some prerequisites for this course so please send your background experience related to computers.

If you are interested in taking this course, then contact :

Mr. Khawar Nehal
+92 343 270 2932
khawar@atrc.net.pk
http://atrc.net.pk