Questions and Answers:
"From Exec to Tech - Tales of Red Teaming" Webinar

1. When your Red Teamers are doing physical intrusion at what point does it constitute a compromise if someone challenges them?
   All of IRM operatives carry a letter which basically explains they are carrying out a test and that they have permission to do so, along with contact details of the person that has commissioned the Red Team. In the event of a compromise that individual would be contacted.

   However, what actually constitutes a compromise? A physical Red Teamer, if challenged, will normally try to talk their way out of being reprimanded / held. They'll use a plausible excuse such as they've got the wrong building and then leave the building promptly. We did have such an incident where one of our physical guys was challenged, he made his excuses and then left the building. However, he went and sat in a café opposite the building and he didn't realise that the receptionist, who was suspicious of him, could still see him and she was so concerned she actually called the police. This is definitely an area that needs to be thought through in advance, for example some customers will advise us that we're to take out the consent letter as soon as we're challenged, in the hope that the exercise can continue. Whilst others will instruct us to try and talk our way out of it.

2. Do you use the Kerberoasting technique and how successful is it during your Red Team projects?
   Yes, we do use it pretty much during every red team and active directory review. It's a very effective way to escalate your domain privileges in active directory.

   As an attacker we can request Kerberos service tickets for any of the SPNs (Service Principal Name) of a target service account. A SPN is a unique identifier of a service instance. The vulnerability lies in the fact that when that Kerberos service ticket is requested from the DC by any domain user (the attacker in this case), that ticket is encrypted with the associated service's hash. Since any ticket can be requested by any domain user, this means that we can retrieve that hash and then run a dictionary / brute-force attack against it to retrieve the plaintext password value.

   It's not uncommon to see an SPN belonging to a MS SQL Service account for example, and that account in turn can be part of a privileged domain group, such as domain admins or even enterprise admins. So if you manage to crack that service's hash you will essentially gain DA or EA privileges in the client's active directory.

   In regards to how successful it is, I would say it's about a 30% success rate during every Red Team project or AD review. It depends on the company's password policy, how well their service accounts are protected against brute-force attacks and how big/complex their Active Directory is, but it is indeed a very useful technique.

3. Are there any advantages of a third-party carrying out a Red Team exercise, as opposed to an in-house Red Team?
   There are advantages for both approaches but the particular advantage of an independent third-party Red Team is that they will give a genuine view of an adversary looking at your organisation, without already having a high degree of knowledge about you. In addition, a third-party is likely to have broader cross industry experience which will be of real value to your organisation – they are also likely to have a broader toolkit than an in-house team. The final advantage of using a third-party that we often here is that (whether right or wrong) boards and management often view an independent report as having more credibility that an in-house one – the fact that it's an external organisation means it can carry more weight in getting things done.

4. We carry out a pen test every time a new project is created, how often and when do you recommend Red Team exercises are carried out?
   This is very dependent on a number of factors – size or organisation, risk profile, industry sector etc. We find that clients who engage us for a Red Team exercise tend to have a relatively high level of security maturity – they even sometimes have an internal Red Team carrying out continuous assessments. Typically clients engage us to carry out the exercise annually but spread over a relatively long timeframe – normally 3 – 6 months. An example is a FTSE100 financial services firm engages someone annually but also rotates through three suppliers to get a new angle on the exercise each year.

5. Are employee social media profiles of a target organisation ever scrutinised by Red Teams, to identify, engage with and then manipulate existing disgruntled/disengaged employees?
   Yes, absolutely. The human element of an organisation is quite often the weakest link. We carry out passive and active attacks against the employees of a company during various stages of our Red Team engagements. For example, during the OSINT (Open-source intelligence) phase, we create a number of social media accounts (e.g. Facebook, LinkedIn, etc.) and try to learn more about the company's employees by visiting their online profiles. It is not uncommon for employees to post pictures of their work environment, their desk, etc. on social media sites. Such people don't realise the type of information they reveal online. This can include Post-it notes attached to their workstation / monitor with a plaintext password written on them. The password could be related to a particular portal the company has exposed to the Internet, or it could be related to the company's guest/corporate Wi-Fi network. Furthermore, the actual work environment in the company's office can tell us the type of workstations/laptops they use, the exact version of the Windows operating system (based on how the lock screen looks like), where their network ports are located and so on. All that technical information can help us develop more sophisticated payloads and manage to hide/deploy our hacking devices much better.

If you have any other questions, please email hello@irmsecurity.com
To sign up to our newsletter to hear about future webinars, simply click here.