RED TEAM - AN ADVERSARY SIMULATION

Whether you are security manager, CISO or CEO it is important to know what is your security posture against real-world threats. Red teaming is especially useful in organisations with strong culture and fixed ways how to approach problems like corporations, military or government.

We were approached by a CISO of large governmental body with simple question: can you attack us and show us where our security procedures and technologies going to fail? We want to improve our security culture by giving our employees hands-on experience.

OBJECTIVE

Our primary task was to find where existing security and process countermeasures going to fail, suggest improvements and show employees how can attacker abuse processes through social engineering or physical intrusion.

Since red team assessment was not oriented on systems and applications but on whole organisation we expected improvement in security culture because employees will have opportunity to be a part of test as a target.

Our hypothesis was there will be in future decrease of successful phising responses after this test and employees will report suspicious activity whether it is physical intrusion, social engineering or application behaviour.

ABOUT THE CLIENT

Large governmental body with more than 50 branches, 2500 employees and responsibility for more than 155 000 000 EUR in budget/year and managed assets over 2 000 000 000 EUR.

Security department has in place systems like IDS, IPS and SIEM. Regularly performed penetration testing and application security tests.

CHALLENGE

To challenge present status, we had to understand organisation strategy, services and security posture. We had to create real-world plans, challenge these plans to find gaps in our thinking and avoid blunders.

For future decrease in successful phising campaigns we had to coin our phishing mails, physical media and phone calls way they were relatable for organisation, yet bring lesson learned for employees.

RESULT

We successfully identified multiple gaps in application security and IT infrastructure. Successful physical intrusion led to change in procedures for visitors in unobtrusive way for employees and supporting staff.

Since red team assessment and demonstration of social engineering with following training there was 64 % decrease in phishing success.

PROJECT DESCRIPTION

Since we attacked government body we learned lot about our target from public resources – contracts, RFP, budget and other mandatory published documents. This way we were able to speed up our reconnaissance stage about 30% compared to standard corporation or military. This was also first big takeaway for client – transparency required by law almost disables security by obscurity approach. We also looked for metadata in published documents or cooperating government bodies, identified and scanned IP ranges and other standard reconnaissance tasks.

When we finished we decided to separate assessment to three stages:

- security testing of perimeter, systems and applications;
- physical security testing;
- social engineering

SECURITY TESTING OF PERIMETER, SYSTEMS AND APPLICATIONS

After initial reconnaissance and from port scan we identified multiple entry points. We decided not to attack well known systems like VPN concentrator or main website since these are very obvious target. During checking list of applications, we found out there is proprietary system for sharing files with external subjects. We tried to brute force passwords however we were not successful but we were able to identify zero-day bug in application. This way we obtained access to webserver and to demilitarized zone (DMZ later).

To demonstrate other trivial possibilities with list of users we were able to guess passwords on LDAP password change application which was not protected against this kind of attacks.

PHYSICAL SECURITY TESTING

For physical security testing we originally wanted to test simplest approach possible – jump over the fence and act like we belong to organisation. We concluded this is possible however much simpler approach would be just walk through main entrance in central location as a consultant from large consulting corporation. We did not have scheduled appointment thus we were put on hold in waiting area. We clearly knew from news when person we were pretending we have appointment won't be in building. After few minutes of waiting we had opportunity to just blend into group and tail-gate them into main office.

SOCIAL ENGINEERING

For social engineering we used physical media distribution, vishing (voice phishing) and phising email. Each of methods generated successful penetration of perimeter what demonstrated clear need for improvements in egress traffic monitoring and security awareness training of users.

We delivered report and presented results to top management of client and provided guidance for technical team regarding improvements.

HAVE ANY QUESTIONS? INTERESTED? GET IN TOUCH!

CALL US +420 228 224 645, DROP US EMAIL ON HELLO@ROLKEN.CZ