Offensive Security and Exploitation

Kick Off

Summary

- About this module
- Plan/Calendar
- Prerequisites
- Project Presentation
- About the assessment
- Report template
- What we're expecting from you
- What we're not expecting from you
- How to turn in?
- Questions?

About this module

Which subjects are we going to learn along this module?

1 - Offensive Security Concepts
2 - Web Exploitation
3 - Network Scanning
4 - Vulnerability Analysis
5 - System Hacking
6 - Penetration Testing Concepts

How will this module take place?

Description of the workshops

You're going to work (alone or as a team) on vulnerable services that we have prepared. We're going to give you tasks to guide you from the first exploitation to a root access on a given machine.

Description of the followups

- 20 minutes of presentation of the student's methodology and approach
- 10 minutes of feedback and questions/answers with the teachers

Format and length of the deliveries :

- 30 minute session in which the group present their report (20 min report presentation + 10min extra/questions)

About this module

- You'll have to audit the security of a **corporate OT network**
- You'll have to present a full penetration testing report with the vulnerabilities you found and remediation advice
- 6 credits

Plan/Calendar

- 03/15 Kick Off *10.30 - 12.00*
- 03/16 Workshop *17.00 - 19.00*
- 03/23 & 03/24 Follow-Up *30 mn*
- 04/06 & 04/07 Delivery *30 mn*

Prerequisites

- WireGuard client
- Network and scripting tools (Kali, Parrot, ArchLabs, BlackArch, Ubuntu, Windows 10, Mac OS, Android [...])
- Curiosity :-)

Project Presentation

- You'll have to audit Powerzio's infrastructure and you will be evaluated like a real professional red team
- You've been granted a remote acces to Powerzio's infrastructure via their VPN
- We are asking you to explore and document machines, services, apps and vulnerabilities you will encounter
- The machines you are going to interact with are used in production, be stealthy and do **not** crash the remote systems
- You are expected to find full-length exploitation paths and discover as many vulnerabilities as possible during the time you are given for this assessment
- Don't neglect your report, the **presentation** of your findings and the quality of your documentation is what you are going to be graded on!

About the assessment

You have been contracted by the worldwide energy contractor **POWERZIO** to assess their internal security.

Most of their teams are working remotely since last month and they figured it would be a good opportunity to finally test their infrastructure's security.

Their mission and the reliability of their system as an energy contractor is **critical**, if something were to go wrong with their IT, it might cause catastrophic issues.

Report Template

- We are expecting you to present your methodology, all of your findings and give remediation advice for every security issue of Powerzio's infrastructure
- Keep continuous track of your work
- Explain what you found
- Your report is the only piece of information we will care about, if it's not in your report, it never happened

What we're expecting from you

- Work as team, communicate with your teammates and don't waste time not parallelizing tasks. You'll have to be efficient if you want to find most of you'll have to
- Work on your documentation as soon as possible
- Assign tasks for everyone, before doing anything else
- If you're stuck, a machine or something technical does not work or if you have an issue within your group, **contact us**
- You'll have to actually **present** your report, you can have a support for your presentation. It's not mandatory but it will make things much easier for you and **much more pleasant and easy** for us to follow
- Absolutely **stay within the scope you have been given**
- Be **nice and clean**, keep your exploits, accesses and files hidden on the remote machines

What we're not expecting from you

- Root every machine. This is a realistic infrastructure, it's not a capture the flag. Every machine isn't here to be bruteforced or pwned
- Bruteforce every service h24, if you're bruteforcing a remote service on this infra, it's more likely you're not going the right direction
- **Get out of scope**. We have absolutely **zero risk appetite**, our machines are monitored and we'll know
- Fix the security flaws on the machine. Keep the machine **as they are** to allow everyone to complete the project
- Attack or give false directions to other students/teams
- DoS or break a machine

How to turn in?

- Create a **private** Github repository for your Team
- Send us an invite (lp1dev + mikkLfr)
- Commit and improve your report as many times as you can

Questions ?

Work environment setup

GNU/Linux instructions

- install the wireguard package available for your distribution (https://www.wireguard.com/install/)
- copy the wireguard config file to /etc/wireguard/wg0.conf
- Work environment setup
- run `sudo systemctl start wg-quick@wg0`
- you should have an IP address on the 10.0.0.0/24 network range

Windows/MacOS instructions

- install the wireguard client (https://www.wireguard.com/install/)
- Click on "Add Tunnel", "Add Empty Tunnel"
- Copy the contents of the file you have been sent by mail inside the "Edit tunnel" window
- Start the tunnel