Hacking 300
Capture the Flag

Welcome to Hacking 300 Capture the Flag. You are a penetration tester hired by Arnaldo Arnaldoson Research Inc. to test the security posture of their corporate network. This document outlines the parameters of this engagement.

About the Client
Arnaldo Arnaldoson Research (AAR) is a research and development consulting firm specializing in continuous celebration event automation. AAR's proprietary technology allows event planners to automatically manage and staff events without the need for a human workforce. AAR's automation prevents the premature termination of celebration events due to factors related to human staff, including illness, overtime wages, scheduling conflicts, and bed time.

AAR operates in a highly competitive industry and is increasingly concerned about industrial espionage. They have decided the cost of regular penetration testing and remediation of vulnerabilities is justifiable when compared to the catastrophic business impact of their trade secrets being exposed or stolen.

Scope and Limitations
The penetration test will target assets related to AAR's corporate network **only**. Employees should not be targeted outside of the corporate environment (**no social media or personal email phishing**). AAR shares an office building with the University of Washington and share a physical network. However, **University of Washington network assets may not be tested in any way**. AAR has reserved the right to hire additional penetration testers and it is possible that multiple pentesters will be working concurrently on the AAR network. **Under no circumstances may penetration testers actively attack one another.**

All testing should be limited to the IP address range provided for AAR Inc's Corporate Network. If penetration testers wish to investigate an IP address outside of this range, they must receive explicit approval from AAR Inc's security team (Hacking 300 Instructors).

A list of these entities and their network address ranges are provided below to easily identify ownership of a network resource or device:

- University of Washington (DO NOT ATTACK)
  - 172.*.*.*
- Hired Penetration Testers (DO NOT ATTACK)
  - 192.168.2.1 through 192.168.2.199
- AAR Inc. Corporate Network (OK TO ATTACK)
  - 192.168.2.200 through 192.168.2.220
  - 169.254.22.100 (NOT DIRECTLY ACCESSIBLE FROM AAR NETWORK)
  - 169.254.22.212 (NOT DIRECTLY ACCESSIBLE FROM AAR NETWORK)

Certain attacks are banned from the penetration test of AAR's network due to their disruptive nature. Denial of Service (DoS) attacks are NOT permitted in any way. ARP spoofing and other “active” types of man-in-the-middle (MITM) attacks are NOT permitted. Passive MITM attacks such as sniffing network traffic ARE permitted. Brute forcing attacks and intensive scans ARE allowed unless they are found to be impacting the overall network availability. If penetration testers are unsure whether any particular type of attack is allowed, they should contact AAR's security team (Hacking 300 Instructors) for approval before executing the attack.

FLAGs and Access to Sensitive Information

To allow penetration testers to prove access to sensitive information without exfiltrating trade secrets, AAR has devised a FLAG system. AAR has placed unique flag numbers next to resources it has determined are of high value to the company. When a penetration tester gains access to a sensitive resource, they should make note of the FLAG number rather than any sensitive information. Any FLAGs captured must be immediately reported to AAR's security team (Hacking 300 instructors) so credit can be given to the penetration tester. When submitting flags to the security team, a penetration tester must submit a short description of WHERE the FLAG was found, the time WHEN the FLAG was found, and HOW access to the FLAG was obtained.

Here is an example of a FLAG (all flags follow this format):

957960-93105375710337871

FLAG Scoring

For scoring purposes, there are different categories of FLAGs with different point values. One flag from each category of vulnerability should be found. The first flag from each Required Flag Category will be awarded 40 points. Additional FLAGs in the same category will be considered extra credit and worth 20 points each. There are 2 additional “Challenge” FLAGs in the environment which will be worth 40 points each - one on the Domain Controller and the second is on the secure Research supercomputer.

Required Flag Categories	**Points (240 total)**
Reverse Engineering	40
SQLi	40
XSS	40
Networking	40
Elevation / Pivoting	40
Hadoop	40

Flags shall be turned in through Module 6-9 Homework Assignments in Canvas. These assignments are pre-created ahead of the CTF and will be open until the Final Report. It is strongly recommended you turn in 2 flags per week for weeks 6-8 to manage your time and allow time for writing the report during week 9.

Problems with the Network
It is possible that unforeseen network/machine outages will occur during the testing period. If you suspect something is not working properly, please contact the AAR security team (Hacking 300 Instructors). It is possible that intentional network features could be perceived as problems – if this is the case we will let you know that what you are reporting is by design.

If you suspect you are battling with another student for control of a machine in the lab (for example you keep getting booted out of a Remote Desktop session), try taking a break for a while or attack a different machine if possible. This is likely to be the most problematic in the first few days of the CTF as everyone is making their first moves in the environment. If you suspect this is happening to the point that it is blocking your progress in the CTF or taking up a lot of your time, please talk to us about it and we will figure something out.

Report
All penetration testers must submit a detailed pentest report of their findings within the AAR Inc. corporate network. **Direct quoting of outside sources is expressly forbidden within the report**. Sources may be used for information about vulnerabilities, mitigations, or other relevant topics but **all writing in the report must be the penetration tester's own words**. **Any time an outside source is referenced in the report, it must be properly indicated with a footnote tied to a reference to the source. Please use UW's excellent resources on how to properly cite sources or ask us if you are unsure. Plagiarism in the final project will NOT be tolerated – if we find evidence of plagiarism we will follow the UW PCE plagiarism policy which can be summarized as "Ahoy matey, welcome to the failboat."**

The report **must** cover the following information about the penetration test:

- Detailed description of the process used to find FLAGs
  - Must explain the full chain of attacks/exploits that led to the FLAG
  - For example: *SQL Injection on the marketing web site allowed compromise of the server hosting the database. From there, a file share within the organization was accessed containing cleartext usernames and passwords. These credentials allowed login to a certain employees workstation. FLAG was found at C:\flag.txt on this workstation.*
- Full description of each vulnerability identified (Where it was found, STRIDE category, severity, what the vulnerability allows an attacker to do)
- Recommendations for fixing the vulnerability
- Business risks to AAR Inc. from the pentest findings
- Appendix containing any supporting evidence, including screenshots, tool output, etc.

It is **recommended** that the Hacking 200 report structure is followed, but **this is not required**. Penetration testers must construct their report in a way that is professional, thorough, and communicates all required information.

The deadline for report submission is due on the due date specified on the Assignment 6-9: CTF FINAL REPORT. Reports will NOT be accepted after this deadline.