Rules of Engagement
NCX LIVE FIRE

NCX LIVE FIRE is an attack and defend, challenge based exercise. Below are the rules of engagement to ensure a fair playing field and that everyone has a fun, learning opportunity with

no unfair advantages. The challenges are critical as completing them provides key information that aids in both attacking and defending, so the students must work as a team to complete the challenges and use those insights to help defend their services and attack other teams' services.

Overview

Each team will be given access to a set of VMs on a subnet specific to their team. 192.168.10.* through 192.168.39.*. The VMs for you to defend will be from 192.168.*.2 – 192.168.*.99. The VMs for you to attack will be on the other subnets in that same range. Any systems on IPs outside of the predefined ranges are not to be attacked to include any services, programs, accounts and/or communication paths they use.

Each team will have a "PLC" (in this case, a highly modified Raspberry Pi with a PLC control board with input/output and LEDs). This system will have an HMI and a few other options which need to be protected (i.e. we'll be putting tokens on this system and checking them for attack/defend points). The IPs of this PLC will be within the ranges above – the ranges able to be attacked and defended.

The PLC will be used and house a flag which users may ascertain by accessing the system and "finding" it. The system is an Echelon PLC, running VxWorks. This flag does score points and is part of the attacking score. A stereo playing music will also be accessible and hackable (to change the music from a list of pre-defined selections), but it does not help teams score points. Both devices will be somewhere in the range of valid attackable devices above (on subnets outside of those any specific team has).

Requirements

Students will bring their own laptops and plug into an ethernet cord available for their computer's user at their team's table. The laptops will be given, via DHCP, an IP within the subnet range of their infrastructure, with the IP's 4th octet above 99 and below 200 (IE 192.168.*.100-192.168.*.200). Wireless will be available for students unable to connect to the ethernet devices, although the IPs they will be allocated via DHCP will not be within their team's subnet range, slightly decreasing their effectiveness (they WILL be able to route to their team's subnet range and still participate).

Students should bring tools on their laptop that allow connections to remote SSH servers as well as remote VNC servers. It is highly recommended that students bring laptops containing both a Linux (Kali Linux is a distribution recommended, as it will come with the necessary tools to achieve success) and a Windows VM (Windows 7 or Windows 10 recommended, with sysinternals tools and Wireshark pre-installed).

Scoring

Given that this is an attack and defend capture the flag scenario-based exercise (with 60 challenges), there are three ways to score (or lose) points, each of which combines equally to determine a team's final score. To ensure each part counts for 1/3rd of the final score, each part is scaled based on the highest team's score in that part. For example, if Team 1 has an attacking score of 3500 and Team 2 has an attacking score of 5000 (the current highest attacking score), Team 1's

effective attacking score is ((3500 / 5000) / 3) * 100 or 23, while Team 2's effective attacking score is ((5000 / 5000) / 3) * 100 or 33. The Parsons CTF Scoreboard calculates the current raw scores and effective scores in real time and displays them during the exercise.

The first 1/3rd of a team's score is derived from challenges. Students solve the 60 provided challenges, with each challenge containing up to five optional hints. Each hint taken decreases the maximum point value for the question, each of which starts at 200 points. Each hint also provides students progressively more detailed tips and explanations on how to solve the challenge. Initial hints provide tool usage suggestions while the final hint (which reduces the point value for that question to zero) proves a detailed solution on how to solve the challenge. This final provided solution still requires the student to follow along and perform the steps in the solution to acquire the answer and move on, facilitating learning and ensuring students never get completely stuck on a question. The second 1/3rd of a team's score is derived from their ability to defend their flags. Each team starts with a defensive score of 9000 and any service unavailability or piece of intel stolen decreases that score. The final 1/3rd of a team's score is derived from their ability to attack other team's infrastructure and retrieve the intel.

Our centralized Intelligence Server delivers the intel to each team's infrastructure using services running on the provided VMs. The Intelligence Server delivers the intel on a random time frame, so students cannot predict when they need to have services running and "game" the system. The Intelligence Server delivers the intel in parallel to all teams at once, so while it is random, delivery is consistent and fair across all teams. This intel is used for three purposes: to validate and score the availability of a team's services, as the defendable flag to protect from other teams, and to be targeted for theft from the other teams. The intel server simulates your fictional teammates in the field that need to deliver critical information to your team in order to survive.
Service availability is scored in this manner: if for any reason a service is down and the service misses incoming intel from their fictional teammates (the intel server), the team loses points for service unavailability (they lose more points due to service disruption [150 points] than if they get that services' intel stolen by another team [max 100 points], so it is to their advantage to keep services up and running). There will be 5 key services that the students must keep running on the VM's they've been provided - a web server on 192.168.*.2, a FTP server on 192.168.*.4, a SSH server on 192.1678.*.6, a mail server, and PLC-related server on 192.168.*.8. Determining how the fictional teammates in the field deliver the intel and how to ensure that the intel can still be delivered with denying the adversary access to it is a key point of the exercise. The intel must also remain at the place it is delivered to not lose defensive points – your fictional teammates get confused if the intel they last placed is there and lose track of what intel to deliver, and this costs you points.

Each time a unique piece of intel is stolen, the team loses 100 points. However, they only lose points the first time a piece of intel is stolen, no matter how many teams steal the same piece of intel, to ensure fairness. For example, if in the first 10 minutes (when only the first set of intel is available), Team 1 steals intel via Team 2's web service, Team 1 gets 100 points and Team 2 loses 100 points. If Team 3 then seals the same intel via Team 2's web service, Team 3 gets 100 points, but Team 2 is not penalized again (since they already lost points for the theft of that intel).

To further ensure the defending part is fair (since students only lose defense points if they get attacked), attackers get a diminishing point value for each subsequent piece of intel stolen from the same team via the same service. This encourages teams to not always target the same defender, as they get more points if they steal a new team's intel. Since each piece of intel is unique, attacking teams also get points for stealing intel from more than one team, encouraging them to target as many teams as possible and to use their coding skills to help script attacks to reduce the manual burden and target as many opponents as possible. This also helps ensure that all teams get attacked a similar amount of times. For example, if in the first 10 minutes (when only the first set of intel is available), Team 1 steals intel via Team 2's web service, Team 1 gets 100 points and Team 2 loses 100 points. If after the next set of intel is delivered, Team 1 again steals intel via Team 2's web service, Team 1 only gets 90 points. If at that same time, Team 1 steals intel via Team 3's web service, Team 1 gets another 100 points. The points decrease by 10 for each piece of intel stolen from a specific team's service, down to a minimum point value of 20. This decrease is specific to a single team's specific service. In the above example, if during the next interval Team 1 steals intel via Team 2's FTP service, Team 1 gets a full 100 points (because it is the first theft by Team 1 of Team 2's FTP service).