Pros V Joes CTF Rules

Game Overview

The Pros V Joes CTF gives players a venue to practice their offensive and defensive Information Security skills in a hands-on, live-fire combat environment. Pros work with the Joes to teach them defensive skills and the art of offense in a multi-day competition. The event is conducted in a private network, accessible only via a VPN (credentials required).

The spirit of this game can best be expressed in the 3 priorities of Pros V Joes. These are, in order:

1. Learn
2. Have fun
3. Win if you can

Joes are members of the Blue Teams. Pros are members of either a Blue Team or Red Cell. Some games may also include a Gray Team, which consists of volunteer “Users”. Competition administrators are members of Gold Team.

Teams of Joes compete against each other, each captained by a Pro. These Teams defend themselves against the Pros on the Red Cell.

During the course of the game, Gold Team will eventually announce that Blue Teams are authorized to conduct offensive activities against other Blue Teams. Red Cell continues with their prior responsibilities, but Blue Teams can rent out consulting hours from one Red Cell member.

Blue Teams are responsible for the following

- Day 1
    - Maintaining control of their network of computer assets, which includes servers, clients, and firewalls
    - Sustaining the highest uptime for Scored Services
    - Defending their network of computer assets
- Day 2
    - All Day 1 defensive responsibilities
    - Attacking other Blue Teams’ networks to compromise systems
- Prohibitions
    - Player may not render a host unreachable or unusable. This includes, but is not limited to
        - Deleting files on a hard-drive such as to break the operating system or remote-access services (SSH, telnet, RDP, VNC, etc)
        - Deactivating needed remote-access services (see above)
    - Blocking remote access with firewalls or other ACL type mechanisms

    - NOTE - Some destructive behaviors are PROHIBITED even during Scorched Earth (the final combat phase of the game). For a complete list, please see the Prohibited Actions

Red Cell is responsible for the following

- Day 1
    - Attacking and compromising all Blue Team networks
    - Beaconing out from compromised systems to show control
    - Increasing quantities of Red Cell Joecoin
- Day 2
    - Attacking and compromising all Blue Team networks (equally)
    - Stealing and submitting flags from compromised systems
    - Beaconing out from compromised systems to show control
    - Increasing quantities of Red Cell Joecoin
    - Supporting any Blue Team that purchases a given Red Cell member's time for consulting hours on directing offensive activities

Gold Team is responsible for the following

- Running the CTF environment and Scorebot
- Helping players with issues they may encounter
- Fixing technical issues that arise during the course of the game
- Scoring and declaring the winners
- Taking any actions deemed necessary and appropriate to manage the game, including making rule updates and enforcement decisions that aren't documented within the rules

Game Play

All about the flow of the game, what happens when, and what the responsibilities of each team are.

Pre-Game

Before the start of the game, all players connect with their VPN clients.
Blue Team players log into their assets and ensure they have control of all systems listed in their handouts. Blue Team is forbidden from making any changes in its environment.

Red Cell players confirm they have connectivity and can ping Blue Team networks Red Cell conducts no other activity until Gold Team gives explicit signoff that the game has commenced.
Gold Team readies Scorebot for game play, assists players having difficulty, and fixes technical issues encountered during checkout.

Game Time

When Gold Team announces the start of the game, all teams authorized to attack are free to do so, and all make any desired changes to their environments.

Phase One

Within the given amount of time, Blue Teams are expected to maintain Scored Services, secure systems, and protect the network and their own flags. Blue Teams are prohibited from any offensive actions.

Within the given amount of time, Red Cell is expected to compromise Blue Team assets, plant beacons, and increase their joecoin account at the blue teams' expense.
Gold Team will monitor and maintain the gaming infrastructure to ensure continued play. Gold Team will monitor all teams and players to ensure things are going smoothly, providing assistance as necessary.

After at least 8 hours of game play, an intermediary, hot-wash light will be held between Blue & Red. The amount of information given will be minimal, but this will serve as a checkpoint, as well as giving the Joes the opportunity to ask the Red Team questions (which they may or may not answer).

Phase Two

Phase two will be announced by the Gold Team during the second half of the game. An hour's advanced warning will be given.

Within the given amount of time, Blue Teams are expected to maintain Scored Services for the benefit of Gray Team (if applicable), secure systems, and protect the network and their own flags. Services are expected to remain fully functional throughout the game. Blue Teams are also expected to attack the other Blue Teams networks, compromise their systems, and steal their flags.

Gold Team will monitor and maintain the gaming infrastructure to ensure continued play. Gold Team will monitor all teams and players to ensure things are going smoothly, providing assistance as necessary.

Post Game

At the end of each day of the game, the Pro's and the Joe's will review what happened. Red Cell members will reveal how they breached the Blue Team environments, and all players will discuss better ways to defend.

During any hotwash meetings held throughout the game, Red Cell will disclose (at their discretion) information to Blue Teams regarding their persistence mechanisms. Post-game hotwash consists of full disclosure.

Scoring

Blue Team

Blue Teams compete against each other for the highest number of points. Points are obtained by maintaining scored services up and running. See the Blue Team SOW for details.

Red Cell

Red Cell members gain credit for compromising Blue Team assets.

Upon compromising assets, Red Cell team members have the option to send beacons to Scorebot and prove pwnership. Beacons can either be advertised on the scoreboard, or hidden from view. Different point values will be given for each, the values of this will be disclosed to Red Cell. The Blue Team whose asset is being beaconed from will lose points.

CTF Economics

The Pros V Joes CTF includes an economic overlay to the game. What the fuck is that, you might be asking yourself? Well, let us explain.

In the real world, defenders and adversaries are both commonly limited by resources. It is not possible to deploy infinite amounts of defensive hardware and software, nor is it possible to devote infinite amounts of time to developing exploits and compromising a given host.
Points earned by Red and Blue can be exchanged for Joe or Red Coins, which can be used to buy resources for the game.

This exchange and purchase system is achieved through a Gold Team managed ZenCart that interfaces with Scorebot. Each team will have their own account in ZenCart to make purchases. The current exchange rate of points to coins will be advertised on the scoreboard. All transactions will be considered final and non-refundable.

The following examples of what **might** be in the store for purchase by **Blue Teams** include, but are not not limited to:

- Additional servers with scored services to earn more points during the rest of the game
- Additional flags to earn more points during the rest of the game
- Additional security infrastructure like Security Onion to be deployed into the environment
- Threat intelligence on the Red Cell
- Insurance against future (but not current or past) breaches

The following are examples of what **might** be in the store for purchase by **Red Cell** include, but are not limited to:

- Credentials to Blue Team assets
- Knowledge of vulnerabilities in the Blue Team environments
- Access to Blue Team assets

Red Team will be authorized to add items to Zencart for sale to the Blue Teams. The following are examples of what this **might** include, but are not limited to:

- Surrender of a compromised asset back to the original Blue Team that owned it
- Flags that were stolen but not yet submitted to Scorebot for penalty against the Blue Team in question

Using Additional Software During the Game

We encourage players to utilize methods and tools that they're comfortable with. This game is about learning and having fun as you try to keep services up better than the other Blue Teams. Gold Team will not limit the usage of any single-user software that players choose to bring, and utilize, on their personal devices. Teams *may not* bring or host servers or server applications via personal devices.

Any team who wishes to introduce additional software into the game environment must abide by the following process. Attempting or using additional software without following this process will result in a significant points penalty as determined by Gold team.

1. Notify the Gold Team of the intent to introduce specialized software by 29 July 2021. Gold Team will not announce or disclose the details of any request to other Blue Teams
2. Acquire four licenses of said software, and provide all four to Gold Team by 29 July 2021. All licenses will be made available for purchase via Storefront during the game. Each team will pay a points-fee if they wish to leverage the specialized software. Also, each team must install and configure said software on their own. Gold Team offers no guarantees regarding the successful functionality of this additional software.

This process is intended to prevent a situation where any team may purchase their way to victory.

Game environment

The CTF gaming environment consists of a network for each Blue Team, with multiple servers and desktops running varying OS and services. Each Blue team has a dedicated firewall they can use to defend their network. Each Blue Team possesses and is in control of an authoritative DNS server that services their network to the rest of the Gaming Grid.

Firewalls

Use of Firewalls comes with certain restrictions in this game, due to the nature of trying to simulate real-world hacking adventures in a compressed time frame and without actual business users and benign traffic in the game environment. These rules cover both network and host firewalls, all protocols, and any alternative means attempted to achieve the same effect through alternative means such as routing, DNS, or other means.

Note the following definitions:

- Ingress - communications coming from the outside network into the defended network

- Egress - communications coming from the defended network into the outside network

The following rules must be followed **at all times**:

- Defensive Players may **not** restrict a host by any identifier, including IP address, netblock, hostname, or other means. This includes, but is not limited to the following list:
    - Source blocking ingress communications from any address for any reason - all ingress rules must have an ANY field for source address
    - Source allowing ingress communications from any address while blocking all other traffic
    - Destination block egress communications to any address for any reason - all egress rules must have an ANY field for destination IP address
    - Destination allowing egress communications to any address while blocking all other traffic

  Gold Team reserves the right to clarify or expand this definition during the course of the game as necessary.
- For any port that traffic can be initiated into the defended network, another firewall rule must allow that same port for traffic initiated from the defended network.
    - e.g. – if a rule allows a connection to be initiated from the external networks into the defended network with port 80 / TCP, then another rule must be created to allow a connection to port 80 to be initiated from the defended network.
- Firewalls **must** allow the following egress ports: 25/tcp, 80/tcp, 443/tcp, 53/udp
- All ingress rules **must** have egress counterparts that allow the opposite traffic flow.
    - For example, if an ingress rule is applied to allow port 22/tcp initiated from the outside network connecting into the inside network, an egress rule must be applied to allow port 22/tcp initiated from the inside network connecting to the outside network
- Rules with ANY for BOTH the source and destination IP address are allowed, but not required

PROTIPS

- DNS is required for Scorebot to score your hosts
- ICMP is required for Scorebot to score your hosts
- Focus on locating Red persistence mechanisms on your defended hosts. Don’t spend cycles attempting to find creative ways to adhere to the letter of the firewall rules while violating its spirit by stopping all red traffic through network mitigations not explicitly spelled out here

In-game Communications

Email

To facilitate Gold Team communications with the Blue Teams, an in-game email system exists. This in-game email system is only to be accessed via in-game computers. Each Blue Team has their own dedicated email server, and at least one email client already configured at the start of the game.

Changes

During the course of the game, Gold Team reserves the right to deploy new assets for the Blue teams to defend. The Blue Teams may or may not be notified of these changes during the course of play. Any such notifications will be sent out via one of the following means:

- in-game email
- Shouting
- Slack
- Morse code
- Carrier pigeon
- Dirty looks
- Semaphores
- Smoke signals (pending Fire Marshall approvals)
- ESP
- Spam texts to your cell phone

Blue Teams may request changes to their environment (new hosts, etc) via the Ticketing System. Gold Team will accomplish these tasks as time permits and will update Blue Team through the ticketing system and/or email. Blue Teams may make use of email in addition to the ticketing system, but any request without a corresponding ticket will be ignored.

Scorebot

Central to the game is the Scorebot scoring engine. This is a homegrown application that will track all aspects of the game and score players and teams accordingly.
During the game, Scorebot performs the following actions:

- Provides a total score for all Blue Teams
- Service scoring - Scorebot regularly monitors scored assets of each team throughout the game, following this process:
    - DNS lookup - Scorebot will do a DNS lookup for each host against the Blue Team's own DNS server. If this check fails, the asset is marked unavailable, full points are docked, and Scorebot moves on
    - Ping - After an IP address is acquired, Scorebot will ping the host. If most of these pings fail, Scorebot will mark the asset as unavailable, full points are docked, and Scorebot moves on.
    - Services - for each service, Scorebot does the following
        - Connect to scored devices
        - Defensive Players may **NOT** destination block outbound communications to any address for any reason

Prohibited Actions

The following lists actions that are expressly prohibited at all times. Players violating these rules may cause players to be expelled from the game.

- **ALL PHYSICAL LAYER ATTACKS ARE OUT OF SCOPE**

- Players may NOT launch attacks targeting any assets outside of the Gaming Grid. This prohibition includes, but is not limited to
    - Any Internet routable address - addresses not within RFC1918 are EXPRESSLY PROHIBITED
    - Any infrastructure addresses (10.20.30.0/24, 10.20.31.0/24, 172.25.20.0/24, 172.19.21.0/24, 172.16.16.0/24)
    - Any VPN connected machines (5.5.0.0/16)
    - Scorebot (10.150.0.0/16)
- Blue Team may not attack Red Cell, though modest Offensive Countermeasures are acceptable. Gold team retains the right to deny any Blue countermeasure deemed in violation of the spirit of the rules.
- Players may **not** deploy self-propagating malware
- Players may **not** intentionally conduct denial of service attacks
- Players may **not** use a Blue Team's firewall to completely lock them out of their environment
- Defensive Players may **not** source block inbound communications from any address for any reason (See the Firewalls section for a more comprehensive list of limits for traffic blocking)
- Defensive Players may **not** destination block outbound communications to any address for any reason (See the Firewalls section for a more comprehensive list of limits for traffic blocking)

The following list actions are expressly prohibited **until Scorched Earth, the final combat phase of the game**:

- No player may render a host unreachable or unusable. This includes, but is not limited to
    - Deleting files on a hard-drive such as to break the operating system or remote-access services (SSH, telnet, RDP, VNC, etc)
    - Deactivating needed remote-access services (see above)
- Blocking remote access with firewalls or other ACL type mechanisms

Tips to the Joes

Look to the Pro's, your team captains on both days, and the Red Cell members that join you on Day Two. In addition, here's a few tips.

- Work as a team, collaborate constructively with your peer Joes and the Pros, who are there to help. Previous years' winners always made teamwork and preparation a top priority.
- If DNS doesn't work, scoring doesn't work. Plan accordingly.
- Ensure that the required services are running and fully functional as they were when your team took possession of the asset.
- Many servers will come online and go offline throughout both game days. Don't overcommit to hardening a server and instead attempt basic hardening followed by threat hunting.
- The single greatest loss of score for blue teams tends to be loss of service availability.
- Ensure that the required applications are running
- Change Admin passwords on all devices (discover unknown accounts)

- Check for accuracy of the documentation provided (hidden servers, services, and accounts?)
- Learn how to spot unusual and malicious behavior on the systems you'll be defending. The MITRE ATT&CK Framework is an excellent resource.
- Use what you know - bring your own system with familiar software (e.g. Event Log Explorer, Wireshark)
- Focus on the basics: Look for unsigned keys and software, auto-start processes, etc.
- Collect > Analyze > Escalate > Respond
- Time management! Be aware of the clock as you do what needs doing
- Try something new!
- Don't lock yourself out - the firewall (network or host) can be your best friend or worst enemy!
- Check permissions (Guest acct with admin rights?!?)
- Check Shared files ("C:\" is shared to the world?!?)
- Get familiar with your systems (user accounts? suspicious software?)
- Communicate with your team on findings - get help if you need it!
- Know your people's strengths!
- Google is your friend
- Know your vulnerabilities - scan your own network
- Making a Major system change - get your captain's approval.
- Document everything you do and everything you find
- Protect what you write down (passwords / vulnerabilities)
- Research - Balance your time on researching and assigned tasks
- Remember - Red Team always wins. (The networks you defend are very, Very, VERY vulnerable...)
- There is not enough time to fix everything, this is an exercise in triage.
- Bring Stuff - Notepad/Laptop/Snack/Caffeine Drinks/Open Mind
- Take breaks. Rotate out for bio needs and mental down time. ***This is ESPECIALLY true with a marathon game format.***

Above all: Relax - have fun and learn!