**Pros V Joes CTF**

**BSides DC 2019**

**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 one day competition. Due to time constraints, this event will be a one day competition. The event is conducted in a private network, accessible only via a VPN (credentials required).

The following four guiding principles define the game and the Gold Team can and will take any action necessary to maintain them:

1. We are all (Gold, Red, Blue) really on the same team 2. The goal is to learn and have fun 3. The Gold Team has to administer the game 4. The game is a simulation and so some things will have to be imitations of reality

Joes are members of the Blue Teams. Pros are members of either a Blue Team or Red Cell. Competition administrators are members of Gold Team.

Teams of Joes compete against each other. Each team is captained by a Blue Pro. These Teams defend themselves against the Pros on the Red Cell. Part way through the game, 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 Red Cell, whose availability will be at the discretion of the Red Team Captain.

● Blue Teams are responsible for the following

○ Phase One - Classic Red vs. Blue

■ Protecting their flags - files, database entries, accounts, among other things...

■ Maintaining control of their network of computer assets, which includes servers, clients, and firewalls

■ Sustaining the highest uptime for Scored Services

■ Resolving the greatest number of tickets assigned by Gold Team

■ Defending their network of computer assets

○ Phase Two - Purple Combat

■ All of Phase One responsibilities

■ Attacking other Blue Teams’ networks to compromise systems

■ Sending command and control (C2) out from compromised systems to show control

■ Stealing and submitting flags from compromised systems

○ Phase Three - Scorched Earth

■ 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. For a complete list, please see the Prohibited Actions section below.

● Red Cell is responsible for the following

○ Phase One - Classic Red vs. Blue

■ Attacking and compromising all Blue Team networks

■ Stealing and submitting flags from compromised systems

■ Sending flares out from compromised systems to show control

■ Increasing their quantities of Red Cell Joecoin

○ Phase Two - Purple Combat

■ All Phase One responsibilities

■ Supporting any Blue Team that purchases a given Red Cell member’s time for consulting hours on directing offensive activities. Red Team fulfillment of Blue Requests will be at the discretion of the Red Team Captain

○ Phase Three - Scorched Earth

■ Player may now 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. For a complete list, please see the Prohibited Actions section below.

● 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

○ Taking any action, whether documented in the rules or not, necessary to maintain the spirit of the game.

○ Scoring and declaring the winners

**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. The last 30 minutes of pre-game will be for Red Cell early access. During this early access, Red Cell will be fully authorized for all offensive operations allowed by game rules.

**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, establish persistence, plant flares, steal the flags, 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.

**Phase Two**

Within the given amount of time, Blue Teams are expected to to maintain Scored Services, secure systems, protecting 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.

Within the given amount of time, Red Cell is expected to compromise Blue Team assets, establish persistence, plant flares, steal the flags, and increase their joecoin account at the blue teams’ expense. They are also expected to assist the Blue Teams that choose to rent their services as offensive Subject Matter Experts, providing direction for their efforts to attack and compromise other Blue Teams. Due to limited resources, each Blue Team may only rent one Red Team member at a time. Which Red Team Member is available at what time is based solely at the discretion of the Red Team Captain.

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.

**Phase Three**

During Phase Three, some of the limitations on destructive tactics and techniques are removed. Red Teams and Blue Teams that have possession of compromised assets owned by other teams are at liberty to damage those assets according to the guidelines. All scoring aspects from previous rounds will continue through this phase of the game.

**Post Game**

At the end 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 then all players will discuss better ways to defend.

**Scoring**

**Blue Team**

Blue Teams compete against each other for the highest number of points. The following outline explains how Blue Teams earn points:

● The initial servers online at the beginning of the game and lasting through the end are one ‘scoring unit’ (assuming they are all online through the entire game).

○ The rest of the scores will be described in ‘scoring units’.

○ This score is metered out per ‘round’. Each round is 5 minutes long.

● The domain controller is worth twice what the other initial servers are worth per round.

● Flags will exist within the systems the Blue Team protects. If it looks like something that, if stolen, you’d report to the CISO/CIO, it might be a flag.

○ All flags together are worth 1 scoring unit.

○ (If you lose all flags, you lose the same amount you’d game from all initial servers.).

● Flares cost 1⁄2 of a scoring unit.

○ For example, for every flare you lose half the score you get from all initial servers each round.

○ If one flare were online from beginning to end of the game, it would cost you half of a scoring unit.

● Additional servers will come on and offline throughout the game. They are much more per round than the initial servers.

● Teams will be given roughly 30k score at the beginning of the game. This is to motivate investment as well as improve morale.

● The gold team may issue tickets to encourage blue team to respond to Gold needs. Tickets are a significant portion of a scoring unit per round.

● A perfect game will score roughly 8.5 scoring units at the end of the game. No-one is expected to get near this.

A few caveats:

1. We are being purposefully vague. We want you to concentrate on the game, not the

score. 2. Most teams make mistakes in the first two hours. The game will hopefully minimize that

it won't prevent it. 3. We expect teams may go negative during the game. Don't worry, it's ok.

**Red Cell**

Because the competition is among the Blue Teams, Red Cell scores are not displayed to the players.

Red Cell members gain credit for stealing flags and compromising Blue Team assets. Upon submitting stolen flags, Red Cell team members will also get individual credit, with Scorebot displaying their loot on the board for all to see.

Upon compromising assets, Red Cell team members have the option to send flares to Scorebot and prove pwnership. Flares 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.

**Flags**

Throughout the course of the game, each Blue Team is responsible for protecting the Flags in their environment by preventing Red Cell from gaining access to their infrastructure. Flags are globally unique in exact content, but each Blue Team will always have the same quantity and type of flags.

● Blue Teams are forbidden from manipulating flags in any way.

○ Gold Teams are responsible for all aspects of Flags, from creation, to deployment and maintenance in the environment.

● Red Teams are charged with seeking and stealing flags throughout the course of the game. No clues will be given.

**CTF Economics**

As a part of the Pros V Joes game since BsidesLV 2017, we have incorporated 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.

As such, we have introduced an economic system into the game. 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 will be 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 are 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 security infrastructure like Security Onion to be deployed into the environment

● Threat intelligence on the Red Cell

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 collect score through Zencart from Blue Teams. The following are examples of Blue Teams may choose to pay the Red Team for, including, 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 Gold Team of the intent to introduce specialized software. 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 21 October

2019. 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. 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. Gold Team reserves the right to clarify or expand this definition during the course of the game as necessary. 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

● 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, an egress rule must be applied to allow port 22/tcp

● ALL firewalls (host and network) **must** allow the following ingress/egress ports: 25/tcp, 80/tcp, 443/tcp, 53/udp

● 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

**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.

**Ticket System**

To help with the assignment and tracking of tasks, Gold Team hosts a centralized Ticket system in its network. Each Blue Team has an account on this system, and will receive tickets during the game for tasks they must complete. Upon completion of a task, the Blue Team should write a clear description of what was done to accomplish the change, fix the issue, etc, and close the ticket.

**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 may be sent out via one or more of the following means:

● In-game email

● In-game ticketing system

● Shouting

● Sneakernet

● Carrier pigeon

● Dirty looks

● Semaphores

● Smoke signals (pending Fire Marshall approvals)

● ESP Blue Teams may request changes to their environment (new hosts, SPAN ports, 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. For the curious, you can find the code for Scorebot here: https://www.github.com/dichotomy/scorebot.

Please note that the code posted here may or may not be the actual code that is being run in the game.

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 - If Scorebot cany address for any reason

■ 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)

○ Any VPN connected machines (5.5.0.0/16)

○ Scorebot (10.150.0.0/16, 10.200.0.0/16)

● Blue Team may not attack Red Cell, though modest Offensive Countermeasures are acceptable.

● 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

● Players may **not** delete flags or make them completely inaccessible

● Defensive Players may not make flags completely inaccessible

● Defensive Players may **not** source block inbound communications from any address for any reason

● Defensive Players may **not** destination block outbound communications to any address for any reason

● Blue and Red Teams may **not** change anything deployed by Gold Team necessary to maintain the simulation, including in their own environments. If you aren’t sure, ask.

The following list actions are expressly prohibited **until the final combat phase**.

● 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. In addition, here's a few tips.

● 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 the game day. Don't overcommit to hardening a server; instead attempt basic hardening followed by threat hunting.

● The single greatest loss of score for Blue Teams tends to be loss of availability. Don’t shoot yourself in the foot.

● Don’t let the first few hours overwhelm you. Most Blue Team self-inflicted wounds occur early in the game.

● Ensure that the required applications are running

● Change Admin/root 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

● 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.

● Relax - have fun and learn!