



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

General Rules (for all players):

1. The White Cell is responsible for monitoring the network, implementing scenario events, and refereeing.
2. There is to be NO physical contact between the players at any time.
3. All teams are connected to a central router and scoring system at all times.
4. Each team will appoint an official Team Captain who will handle all protests and official inquiries for their team during the competition. The White Cell will only communicate with the team captain.
5. The White Cell will be the final arbitrators for any protests or questions arising before, during, or after the competition.
6. All participants will wear badges identifying team affiliation at all times. Badges will be handed out at check-in.
7. Defending team members will not initiate any contact with members of the Red team during the hours of live competition and vice versa.
8. Defending team members and Red team participants will not enter another team's competition workspace.
9. Scores will be maintained by the White team. No running totals will be provided during the competition.
10. Scoring will be a combination of automated tools and manual checking.
11. There will be no interfering, tampering or attacking the scoring infrastructure.
12. No unauthorized electronic devices or media are allowed in the room during the competition. All cellular calls must be made and received outside the designated competition areas.
13. All players must be registered and badged at all times.
14. No harassment, threats, duels of any kind
15. Rules and infrastructure are subject to change without notice
16. No one is responsible for any real or perceived damage, insult or hurt feelings
17. If we cannot see your badge, you will be asked to leave.
18. No unauthorized hardware or software allowed in the exercise.
19. By registering and playing the exercise you agree to be bound by these and any other rules, signs or White Cell instructions.
20. Failure to follow these and any other signs, rules or White Cell instructions may result in disqualification and removal from the exercise.
21. There will be no returned fees for those disqualified from the exercise.



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

Photo and Traffic Release Form

I hereby grant White Wolf Security permission to use my likeness in a photograph in any and all of its publications, including website entries, without payment or any other consideration.

I understand and agree that these materials will become the property of White Wolf Security and will not be returned.

I hereby irrevocably authorize White Wolf Security to edit, alter, copy, exhibit, publish or distribute this **photo** for purposes of publicizing the White Wolf Security's programs or for any other lawful purpose. In addition, I waive the right to inspect or approve the finished product, including written or electronic copy, wherein my likeness appears. Additionally, I waive any right to royalties or other compensation arising or related to the use of the photograph.

I further understand that White Wolf Security is running tools to capture, store and analyze network traffic generated within the course and scope of the exercise. I hereby irrevocably authorize White Wolf Security to capture, copy and otherwise manipulate any and all traffic generated by myself and the hardware/software used by me in the exercise.

I hereby hold harmless and **release** and forever discharge the White Wolf Security from all claims, demands, and causes of action which I, my heirs, representatives, executors, administrators, or any other persons acting on my behalf or on behalf of my estate have or may have by reason of this authorization.

I am 18 years of age and am competent to contract in my own name. I have read this **release** before signing below and I fully understand the contents, meaning, and impact of this **release**.

(Signature)

(Date)



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

Internet Guest Access

Internet access may be provided at the event. It will be air-gapped and stations will be provided for you to research and download tools/information. Be prepared to sneaker-net things over to the exercise network.

Defending Team Rules

Team Configuration:

1. Each defending team may be up to 8 players (including a Team Captain)
2. Plan on needing skills to cover:
 - a. Windows (server and desktop)
 - b. Linux (server and desktop)
 - c. VoIP
 - d. Cisco firewall

Communication with White Cell:

1. Each team will designate a Team Captain.
2. Only the Team Captain is allowed to address the White Cell.
3. All communications between the Team Captain and the White Cell are to be conducted using the in-exercise VoIP and email network.
4. The White Cell may be reached at:
 - a. Extensions 8001 and 8001
 - b. Email via: whitecell@cyber-exercise.com

Network and System Rules

1. You will be given close to identical hardware and software installations to configure and support.
2. Teams are not permitted to plug anything into the exercise network with prior authorization.
3. No software that is not already installed at the start of the exercise is allowed on the morning of the competition.
4. The Team Captain will be notified when they can use open source and free software (NO trial commercial ware; all software must be 100% free).
5. You should not assume any system is properly secure.
6. Moving services from one IP address or system to another is not permitted.
7. You may not alter the system names or IP addresses of systems.
8. You may not change service providers (e.g., a wu-ftpd server must stay a wu-ftpd server).
9. You may not bring electronic copies of configuration files (e.g., iptables) or scripts (e.g., script to change passwords) to the competition (hard copies are allowed however). These must be created during the competition.



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

10. Each team is required to provide incident reports for each Red Cell incident they detect. Incident reports can be completed as needed throughout the competition and presented to the Gold team representative for collection.
11. There is to be NO counter-hacking or offensive operations conducted by ANY team.
12. Points will be deducted from a team's score if evidence of un-authorized access and/or compromise can be proved.
13. Do NOT plug in your own assets into the exercise network without prior approval from the White Cell.
14. The systems are to remain plugged in to the network at all times.
15. ICMP and IP traffic must flow between all the teams.
16. The systems are to maintain the same IP addresses during the course of the event.
17. A complete list of necessary ports/services will be provided on the day of the competition.

Traffic Rules:

1. You are starting with a basic firewall ruleset:
 - a. IP any any
 - b. ICMP any any
2. Filtering based on source/destination IP address is NOT allowed without consent from the White Cell.
3. A complete list of allowed inbound and outbound traffic will be provided the day of the exercise.

Incident Response:

1. In order to block by source/destination IP address you must complete a Network Incident Response form (handed out the day of the exercise) and run an investigation with on-site law enforcement.
2. The law governing intrusions is 18 U.S.C. 1030. It is recommended that you read this prior to the exercise.

Scoring Rules:

1. Each team starts with 0 points.
2. Your team will be scored in rounds.
3. The team with the lowest score at the end of the event wins.
4. Your firewall will be pinged at the start of each round using ICMP. If your firewall does not respond to ICMP ping, your entire network will be marked as down and the maximum penalty will be assessed.
5. Each round will then check each IP asset via ICMP ping. Failure to respond to ICMP ping will result in the server being down and the maximum outage penalty for that IP asset will be assessed.
6. If the IP asset responds to ICMP ping, it will then be checked for service availability (is the port open - 100 points), functionality (service request - 50 points) and integrity (flag verification - 25 points).
7. If an intrusion has been logged, you will be assessed a 500 point penalty for that round. Each IP asset may receive only one intrusion penalty per round.



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

8. Respond to 'injects' - specific tasks that will be emailed to your Team Captain and require a response/action within a specific amount of time.

General Administration

1. All password changes, except for accounts named 'root' or 'administrator' MUST be emailed to the White Cell (whitecell@cyber-exercise.com). Failure to do so will result in an inability to test for services and therefore result in a scoring penalty. This email is for in-Exercise.
2. Any team action that interrupts the scoring system is exclusively the fault of that team and will result in a higher score.
3. These systems are fully configured and functional and are tested prior to the start of the exercise. Do NOT approach the White Cell with the concern of "it's broken". You have admin rights to all the systems. You must attempt to trouble shoot the issue before requesting help.



www.whitewolfsecurity.com

White Wolf Security
1052 New Holland Ave
Lancaster, PA 17601
717-295-6201 (o)
717-295-6205 (f)

Attacking Team (Red Cell) Rules

1. You are responsible for bringing your own attack hardware and software.
2. You are restricted to the target list (provided separately). Attacking outside this document will not be tolerated.
3. Be prepared to target specific flags. Examples include:
 - a. Password files (acquire and decrypt them)
 - b. Database entries
 - c. Files located on HTTP/FTP servers
 - d. User accounts
4. Be prepared for multi-stage attacks:
 - a. Turn and pivot
 - b. Uploading/downloading tools to compromised systems
 - c. Establishing continued access to systems.
5. No flooding or DDos of any kind
6. You are responsible for attacking the Blue Cell assets. Attackers will be scored on their ability to:
 - a. Corrupt the flags of other teams
 - b. Obtain execute privileges on the other Teams' systems
 - c. Respond to 'injects' - specific tasks that will be emailed to your Team Captain and require a response/action within a specific amount of time.