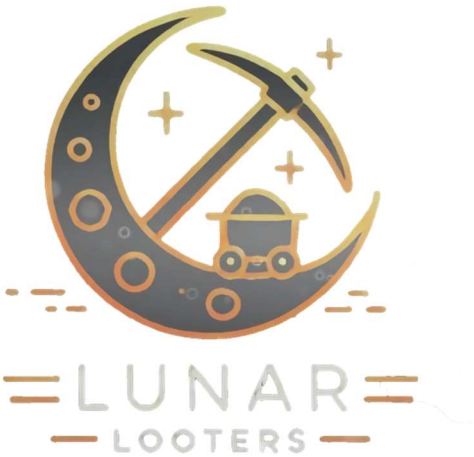


Lunar Looters

Thank you for agreeing to take the reins of the IT/Cyber Division at Lunar Looters LLC. Our mission is clear: to expand humanity's presence on the Moon, while engaging in cutting-edge research and resource extraction (and, yes, maybe a little looting on the side). We've had a bit of a transition recently, with a mass exodus of cyber and IT staff due to some inconsistencies in work locations, but now, we have you! We're thrilled to have you on board, and even though we're still working virtually for now, we're eager to get you up and running alongside us.

Our goal is to lead the charge in lunar resource extraction and research—trust us, the discoveries we've made so far will blow your mind! But that's not all—we're also at the forefront of space solutions, offering everything from launch and recovery services to spacewalking, decompression management, high-speed altitude loops, and, perhaps most impressively, we've surpassed even SpaceX in the rapid disassembly of space-faring objects. Yes, you read that right.

Whether you're navigating the vastness of space, geeking out over space tech, or managing the disassembly of satellites with a dash of decompression, Lunar Looters is your go-to for out-of-this-world experiences.

We offer a complete suite of space mining services, lunar research facilities, and Low Earth Orbit assets—perfect for any aspiring entrepreneur looking to make their mark in the next great frontier.

At Lunar Looters, we're on track to be a leader in the emerging wave of sub-orbital, orbital, lunar, and extra-lunar projects. We're glad to have you with us as we reach for the stars—and beyond!

Welcome!

We're excited to have you with us. We think you'll be a great addition to our team. Remember, here at Lunar Looters "YOU" are the grease that keeps the cogs in the space machine turning. You will always feel appreciated, special, loved, grounded! I will be your interface with the company as you take over our IT infrastructure and security operations. We know that you will fit right in with the rest of us here and are excited to see you bring more passion and vision to the network! Our systems should be very friendly and easy for anyone to use.

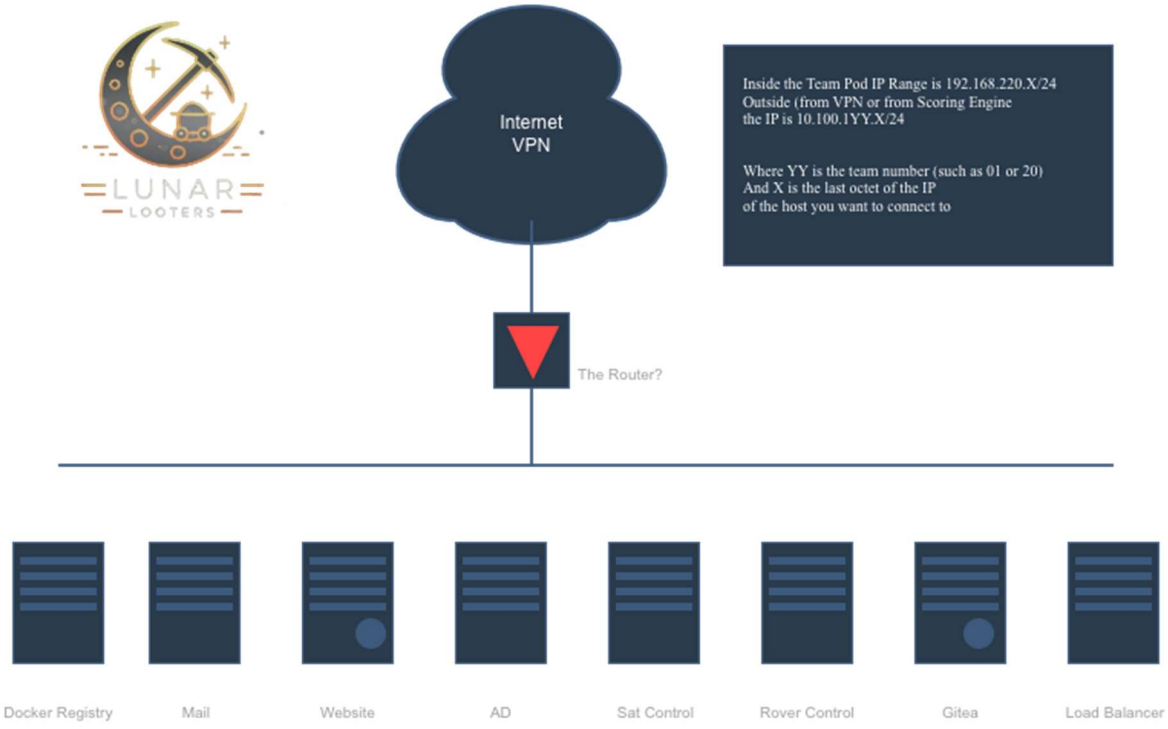
Remember, it isn't just about launching rockets that go BOOM! It is about getting the rockets to the Moon and making them go BOOM!!! Then collecting stuff and organizing rescue missions that don't go BOOM! This is our vision for the future!

Job Perks

We offer a really competitive workplace including:

- Weekly off hour orbital office hours
- Anti-Gravity Ping Pong Tables
- Medical (You may need this!)
- Ergonomic Space Suits.
- A great can-do, you-do, so we all do BOOM! attitude
- Long Term Disability and Dismemberment (You probably will need the latter!)
- Maintaining an environment free of unionizing
- Refrigerators stocked full of NRG drinks
- Service Branches in Exotic, Off-Planet, Seemingly Untouchable Locations! (Really, you may not want to touch some of this stuff!)
- Orange Space Suit Day!
- Team Building and Blow Up exercises.

Services and Scoring



IP	Name	OS	Purpose / Service(s)
.2	balrog	Alpine	Router/Firewall
.111	Cthulu	Windows 10	Satellite Communications
.254	kerberos	Windows Server 2016	Domain Controller
.231	Brassknuckles	Debian 12	Mail Server
.221	Tartarus	Talos Principal Linux	Kubernetes Containers?
.44	nix	NixOS	Company Web Server
.42	pandemonium	NixOS	Development Server (git)
.234	donut	Ubuntu 24.04	High Performance Load Balancer
.245	Viking	Windows 10	Satellite Tracking Applications
.13	Charon	Alpine	Docker Repository / Samba Share / Reports

Services

We do have customers, and we want to make sure they can access our services to support their financial transactions and online exchange needs in the crypto banking world. We have some traditional banking services as well as IT services that you would find in any modern-day business.

*NOTE: There may be other servers and services. I would do an inventory once you login…

Common Protocols

RDP	SSH
SNMP	SMTP
IMAP	POP3
VNC	OpenVPN
HTTP/HTTPS	Telnet
DNS	NFS
SMB	FTP

Scoring Instructions

Services will be scored with SLAs occurring after 5 failed checks. Roughly Ten (10) services will be scored across most servers (Plus or Minus 2 services) every 2-4 minutes.

Routers

You will have a fully custom build Alpine Linux based router based on nftables/iptables and netmap. This means you have complete autonomy over your firewall. I HIGHLY suggest that you tread carefully with this device as if you lock yourself out or block off your access or worse block access to the scoring engine you will be having a very challenging day.

Your services will be subject to going down if this device is misconfigured. Box Resets for this PFsense router / firewall will be an automatic -100 point deduction per reset.

Please keep in mind that you will have the 1:1 NAT in place, so when you connect to a system on 10.100.1XX.Y you will actually be connecting to 192.168.220.Y. For example, 10.100.102.10 translates to 192.168.220.10 from outside the router and ONLY the outside of the device. Put simply, you better know how NAT / PAT works!

If you run into trouble with the router, after filing out a ticket, please keep in mind the following:

- Cutover Windows are every 30 minutes (e.g. 10:00 or 10:30 etc) This includes resets!
- A credential will be provided in the ticket to you that will let you administer the router completely
- You are allowed to change or delete or disable the “admin” user. Be careful with this! If you forget the password and delete the admin, you are looking at a box reset.
- It is recommended that you do not disable syslog or WAN firewall configuration access so that you can get data / administrate from the outside of the firewall, but that is up to each individual team to decide as the RED TEAM will also have access…

Resets and tickets will be provided on team-managed routers, and costs will be defined below. **However if we lose access, a reset will take place.**

Connection Guidance

Teams will receive PAN Global Protect credentials for VPN access. Each team member will access the VPN with only one end device. Your device count is capped at 9 devices. This connection will serve as your starting point for ALL of your players. You basically will share the network (Via separate desktops / terminals.) Don’t worry, it is beefy enough to support your activities for the day of the competition. You no longer need to supply your IPv4 addresses. We will monitor the number of address and connections into the environment.

To help try to clarify, each competitor will have an account. ONLY one account can be used at a time. Each Team gets 9 accounts (8 Team Members and 1 Coach). Once in this network, they can reach their IP addresses relating to their pod via the connection. This will happen promptly at 9AM and you will have access onto the 192.168.220.0./ 24 network. This IP address range accepts credentials via SSH, VNC, Telnet, and Remote Desktop depending on device (See Table Above).

Service Locations (Critical Services):

For this invitational, you are going in “BLIND” and scored services will be provided to you via the scoring engine the day of the competition. You will receive an email from the “GOLD” team of WRCCDC with your single sign-on credentials. These creds will allow you to login to the WRCCDC environment and your jump box (when it becomes available). You will only receive the master credentials for the competition systems at 9AM the day of the competition when the competition starts.

The table above with the system hostnames and last octet number, will give you a clue as to the services that will be scored. Beyond this, it is up to you to learn your environment quickly to master it.

As the former IT team did not leave any information or documentation other than what is provided in this document, I HIGLY recommend that you inventory all assets including virtual machines, IPs, hostnames, applications and any other valuable information as soon as possible.

Support, Scoring and Help

Integrated Scoring Engine

We have a new scoring engine!!!

The integrated scoring engine is located at: https://scoring.wrccdc.org/login

Here you can find information on scored services, retrieve and turn in your injects, and submit your password change requests. The portal is very intuitive but if you have questions or issues please submit your questions through your TEAM DISCORD.

Your username: TeamXX (where team XX is 01…04..10, 25, etc)
Your password: (See Password Document) – (To be sent out Friday afternoon /evening)

The service scoring engine is out of scope of red team. They will not attack it and will leave it alone.

Injects will be distributed, returned, and scored in the service scoring engine. WRCCDC staff will distribute credentials via email/discord either the evening before or the morning of the competition. The first inject will be available at the start time of the competition.

Injects are scored based on complexity of the tasks required. They are given a time period for completion and have a rubric for scoring. One judge will be assigned per inject for scoring so as to level any inconsistency with scoring a single inject. There will be several judges assigned to injects over the course of a competition.

Once logged in, you will find injects there. Additionally, we will push any announcements through this application.

Injects will be scored based on criteria given in the inject. As mentioned before, rubrics will be leveraged to level scoring. Not all injects will be weighted the same. Examples are below:

As you can see, there will be a very wide range of scoring across all injects based on complexity. Please note, the “or” indicates a range of values, for example 0 through 25.

All injects are timed. They will show their completion time in ISE. There will also be a “Reject” Time. The “Reject” time will be the time at which submissions will no longer be accepted. We try to make the reject and completion time the same. Late injects will not be accepted.

All Judging is final. It will take us about a day or two to calculate scores and provide them to the competition organizers at which time finalists will be published. It is our intent to share the scoring rubrics to their teams. Teams will not receive other teams rubrics.

This will be the only notice for inject scoring guidelines. Points will be deducted for not following these rules.

File Names:

File names must be in the following format:

- Inject number must be first
- Team Numbers Only - **DO NOT** mention your School
- Underscores as spacing
- If the inject is a single digit, pad with a leading zero
- All lowercase letters

File types must be PDF only. No other file formats will be accepted.

Example of file naming convention:

- inject04_team13.pdf

Citing Sources:

When revising an existing work, such as editing a template found online, you **must** cite the source. The format of the source is not important and does not need to be standardized (MLA, APA, EIEIO, etc.). A reference URL is good enough.

Example reference, or “reference”, if you will:

> Our team was able to find a sample policy from the following site:
> https://templates.office.com/

If you follow these submission guidelines, you will do just fine. Good luck team!

Use of Artificial Intelligence sites such as ChatGPT or Google Bard will cause you to lose ALL points for that inject. We will be checking injects against several online portals setup by OpenAI, Alphabet, and other Universities against your submissions. IF they post a result of 20% or greater being fake, the inject will be thrown out.

Discord

Discord may be used during the competition as a means of communicating to Black Team, Orange Team, and White Team. It is a means of communicating between your team securely

and an easy way to share files to your team and competition organizers. You will not be required to leave after the competition, and you may use this Discord server to freely chat between schools and teams and participate in other events we have. Your team will be unassigned from you after the competition.

As part of this packet (or sent separately at the same time) you will have been given twelve tokens (Up to 12 Team Members, including alternates) These may be used to register you into your team role in the competition discord. Your coach may use one of these as well.

Steps to Join and Setup Discord:

1. Join Discord using a personal account or one generated for the competition provided by the organizers.
2. Read the instructions in #welcome.
3. Set your role using !usekey in #role-selector
4. Begin using your team channel
5. You are joined!

If you have any issues during the competition, or want to request consultation services, you can do it via DISCORD. However, we also ask you to open a Ticket (See Below). You will see the appropriate channels and can get our attention via an @ Call. For example @blackteam will get the attention of the Black Team, @whiteteam will get the attention of the Competition Judges. @redteam will, well, that actually WON'T work so please don't try it…

Service from these teams for the invitation is on a 1st come 1st served, BEST EFFORT basis. So please do not bombard the BlackTeam or WhiteTeam with erroneous requests, you will get ignored when you do need them…

TICKETS

For scoring adjustment and cases that you want tracked please use the ticketing system. Do this for everything (Except Password Changes – Please do this via the Scoring Engine!) Go to: https://tickets.wrccdc.org and use your provided credentials to login.

Here, you will be able to log an issue. (Upper Right Corner). Please be as detailed as possible. Please do not put in tickets that are vague. (I.E. "Chowder is Broken") Well, what does that mean. However, if you give detail, we will do some digging first before we get back to you. In brief, help us help you!!!

This will also help us track similar issues across all teams. The form is very intuitive. Provide what information you can and again, BE DETAILED!!!
We will get to these as quickly as we can. We operate with about 4-6 staff on competition days and our invitationals and qualifiers can have many, many teams.

Common Service Requests

- Service Scoring Validation
    - 0 points, but we'll cut you off if you abuse it
    - If you believe your service is working 100% correctly and you want us to verify the check, file this ticket. If it's used frequently without additional consultations, we will require a Service Scoring Check ticket at minimum.
- Service Reset / Scrub
    - 60 points
    - We will reset your box to start of competition state and notify you when it is ready
- Scoring Service Check
    - 10 points
    - Have black team provide additional context surrounding the service check (details on the failure)
- Black Team Phone Consultation
    - 100 points
    - Have black team diagnose your issue over the phone with you
- Black Team Hands on Consultation
    - 200 points
    - Have black team gain access to your box to investigate and describe the issue to you, attempting to to fix things along the way
- Orange Team Verification/Questions
    - 10 points
    - Have orange team respond to you about how a score or service was performed

Manual Scoring (Orange Team)

There will be services that are scored manually. These can be blogs, file services, calculators, spreadsheets, Outlook Web Access (OWA) portals, Games, etc. Orange Team members will be checking these. What is a legitimate to check? Typically, we try to stick to the main applications that you would see in a real business. For example, if you notice a FTPsite that requires authentication, that could be scored whereas one that allows anonymous access would not. Same with remote access. A SSH connection could be scorable where as a Telnet Access Session would not. We try to make this as "common sense" as possible. Typically, the Orange team will contact you via Tickets, or Discord Chat (if available) to let you know that something is down. Orange Team points are scored based on number of checks attempted and do not account for more than 10% of overall scored points.

Orange Team Services

TBD, We will reach out to you if an Orange Team Service goes down. At this time we are limited on Orange Team Members so this will be a very LOW scored area and only account for about 5% of the Final Score FOR THIS COMPETITION.

Point Deductions (Red Team)

If in case your environment or one of your applications / systems is compromised, points will be deducted.as outlined below. This is direct from National Scoring Guidelines.

Successful Red Team actions will result in penalties that reduce the affected team's score. Red Team actions include the following (penalties may be different than listed below):

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access or equivalent): -25 points
  - If standard users can be escalated to Root/Administrator Privilege, this is an additional -100 point deduction.
- Recovery of user IDs and passwords from a team system (encrypted or unencrypted): -50 points
  - For example, a user list, Active Directory with Hashes, SAM file, Shadow File
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points
- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points
- Recovery of encrypted customer data or an encrypted database: -25 points
  - -25 points additional if database can be unencrypted

Red Team actions are cumulative. For example, a successful attack that yields a system breach that causes a dump of active directory hashes followed by the decryption of said hashes leading to a user login finalized by a privilege escalation to Administrator that provides access to an encrypted database with customer data that in turn allows for the compromise of privilege information of customers' addresses and telephone numbers would be a net deduction of:

-100 for System Breach
-50 for AD hash dump
-25 for Database Recovery
-25 for Database Decryption
-25 for Customer Data Breach
-200 Points for PII loss

Total Deduction from one Incident would be: -425 Points.

Red Team actions are scored on a per system and per method basis – a buffer overflow attack that allows the Red Team to penetrate a team's system will only be scored once for that system; however, a different attack (Vulnerability) that allows the Red Team to penetrate the same system will also be scored. Only the highest level of account access will be scored per attack – for example, if the Red Team compromises a single user account and obtains root access in the same attack the penalty will be -100 points for root level access and not -125 points for root and user level access. Please note the point values described above are examples – actual penalty points may be adjusted to match the competition environment.

Red Teams can also execute additional malicious action based on their access. Attacks such as defacing websites, disabling or stopping services, adding/removing users, and removing or modifying files are permitted and may occur. This can affect service scoring and is legal Red Team Activity. Red Team can modify and reboot any server except for the router(s) which they may only change ACL rules.

Red Team needs to provide proof of breach or data compromise along with a date / time stamp for point deduction.

Remote Site Judges

There are NO Remote Site Judge Requirements for this Invitational Competition.