Hive Member - Red Team

CovertSwarm exists to outpace cyber threats by constantly compromising our clients. Our Swarm continues to grow, and our Red Team is recruiting.

About CovertSwarm

Our goal is simple: We aim to compromise our clients, constantly. Our Hive teams 'swarm' around our targets, always looking for a new way to compromise them.

As a result, we provide security advice that reflects not only the technological controls and mitigating solutions, but improvements that can be made from a training, process, and physical control perspective.

The role

We are looking for individuals who are driven to find new or different ways to breach organisations, are capable or desire to find new zero-day vulnerabilities, can adapt attacks to bypass controls, and are relentless at finding novel methods to compromise a target.

Unlike the typical production line approach of some cybersecurity businesses, you will not be juggling an overwhelming array of Penetration Test or Red Team projects. Instead, you will be tending to a select number of high-profile clients and challenging their perimeter security, people, processes, and more.

The position is remote based as we strive to compromise our clients in as realistic scenarios as possible. On rare occasions there may be a need to visit clients in person, such as to deliver physical security or social engineering attack vectors.

Responsibilities

- Act as a business contact for CovertSwarm clients, fostering and maintaining relationships with key stakeholders and business partners. Ensuring client communication throughout the engagement and contract.
- Perform cyber security assessment activities against complex networks, applications, operating systems, wired/ wireless networks, and mobile applications/devices.
- Develop and maintain attack plans bespoke to each client to replicate an Advance Persistent Threat (APT).
- Create high quality actionable, threat-based, reports on security assessment results, which the client is debriefed on fully following the completion of any assessments.
- Consult with application developers, systems administrators, and management to demonstrate security assessment results, explain the threat presented by the results, and consult on remediation.

- Communicate security issues to a wide variety of internal and external "customers" to include technical teams, executives, risk groups, vendors, and regulators.

What we are looking for

Whether you have a broad knowledge of all-things cybersecurity, or if you are specialised in certain areas, then we want to hear from you. Some of the key areas to note are:

- Network security, including Linux and Windows infrastructure
- Application security, mobile applications, APIs, thick clients, etc.
- Social engineering with phishing, vishing, and in-person engagement experience
- Coding, scripting, reverse-engineering & debugging
- SCADA, IoT, embedded devices, etc.

While we do not require applicants to have an alphabet of certifications, we are in search of applicants who currently hold CCT INF or CCT APP.

We are keen to meet talented professionals and developers with practical experience and a deep passion for cybersecurity.

You would need to be able to work both collaboratively and be able to plan and deliver attack scenarios independently.

We seek individuals that are skilled, but also willing to learn and share knowledge with others. You also do not need to have dozens of CVEs under your name; we are looking for someone who has the drive and ambition to do so.

Benefits

Aside from working with some of the most talented and passionate people in the industry we can also offer you:

- A fully remote (working from home – 'anywhere in the world') role with only the need to travel to client sites when in-person meetings are required, or we are running our quarterly meetups.
- You will not have to use a word processor for report writing – we deliver the results of our endeavours through our bespoke online portal.
- A culture born of vulnerability research. Reporting missing HTTP headers and SSL/TLS weaknesses, and outdated software patch versions is just 'noise' in our view. We focus on the actual point of compromise and continually look for new ways to breach our clients.
- Work when you want – That does not have to be a 9-5, but we only ask that the job is done well, and core meetings are attended online.
- We all go to DEF CON, every year (well, when it is not cancelled!)

- Software, hardware, and research materials are not bound by strict limits. If you need a resource to deliver to the best of your ability, we will aim to accommodate this.

- Unlimited Training – If it is relevant and will help you, your Hive team, and CovertSwarm to better breach and educate our clients, then you can do whatever training you need to fulfil this.

- Unlimited Holiday – We all need downtime, take it, whenever you need it. There are no prizes for burnout. You work to live, not live to work.

- If you present at a major infosec event/hacker conference, then we will pay your expenses and give you a bonus to reflect this. We want to give back to this great community that continues to help us all.

- No corporate politics – The continued growth of CovertSwarm as a business, the team, and the quality of our services depends upon us being radically candid with one another. Always.

We pay good salaries, have a brilliant culture, and our Board are even hackers too! However, if you are just chasing the biggest pay packet, or are driven by your ego, then we are not for you, and you are not for us.

Join the Swarm

If you love Cybersecurity but are currently held-back, bored, or not inspired to do great work every day in the best and fastest growing industry in the world, then we want to hear from you.

If you truly want to be part of something new, exciting, and different and to get away from the monotony of traditional cybersecurity roles then get in touch by sending us a quick message and your CV/resume: jointheswarm@covertswarm.com