

Red Team vs Blue Team

By Vicky Aryan (pwnb0y).

[@pwn_b0y](#)



Why I chose this topic today.

- ❖ To aware you how the cybersec works in real world.
- ❖ All the cybersec works are majorly divided in two teams or groups (ie:- team red and team blue).
- ❖ Importance to working of these two teams mutually
- ❖ To know what is suitable for me which one is my future.





What is Red Team

A red team consists of security professionals who acts as adversaries(cybercriminals), attempting to identify and exploit potential weaknesses within the organization's cyber defenses using sophisticated attack techniques. These offensive teams typically consist of highly experienced security professionals or independent ethical hackers who focus on penetration testing by imitating real-world attack techniques and methods.

They utilize all the available techniques to find weakness in people, process and technology.



Why we need Red teaming and Red teamers.

Just because Hacking is not an incident that happens daily and we don't know where and how hackers try to get into our organization and also we don't know how a hacker thinks.


Then what to do at this point?

That's why we hire some person who has the same experience that a hacker or cybercriminals have and told them to try to hack our organization from all the methods that are possible.

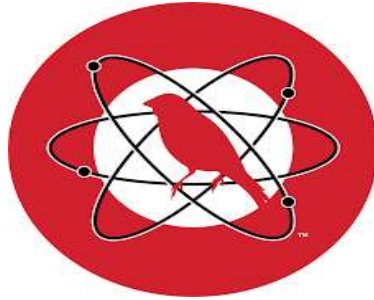
these persons are known as red teamer who works on offensive work in our organization.



Example of Red Team Exercises:

- Performing penetration test(network, webapplication, internal, external)
 - Social Engineering Attacks.
 - Phishing
 - And many more.....
- 

Tools that used in red teaming.



sqlmap®

A few popular red teaming and pentesting certifications to consider include:

- Certified Red Team Operations Professional (CRTOP)
- Certified Cloud Penetration Tester (CCPT)
- Certified Mobile and Web Application Penetration Tester (CMWAPT)
- CompTIA PenTest+
- EC-Council Certified Ethical Hacker (CEH)
- OSCP (My favorite)



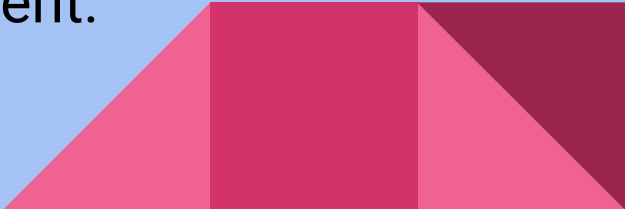


What is Blue Team?

A blue team consists of security professionals who have an inside view of the organization.

They are defenders whose goals are to protect their organization from malicious activity.

The blue team first gather data and document exactly what needs to be protected and carries out a risk assessment.



Roles and Responsibilities

You can work as

- ☐ Cyber Security Engineer
- ☐ Cyber Security Analyst
- ☐ Incident Response Manager

Monitor all the traffic which is going on their network

Analysis of emails that come under the organization

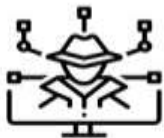
Understanding every phase of an incident and responding appropriately.

Noticing suspicious traffic patterns and identifying indicators of compromise.

Rapidly shutting down any form of compromise.



Tools used in Blue Teaming.



Saga Labs

Tools

Elastic Stack

- Elastic Endpoint Security
 - Detect mode
- Kibana

Velociraptor

TheHive

MISP



elastic



MISP
Threat Sharing



Velociraptor



TheHive



splunk> pf sense



yara



Some Popular Certifications for Blue Teamers

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Incident Handler (GCIH)
- Systems Security Certified Practitioner (SSCP)



Benefits of red team/blue team exercises

Implementing a red team/blue team strategy allows organizations to actively test their existing cyber defenses and capabilities in a low-risk environment. By engaging these two groups, it is possible to continuously evolve the organization's security strategy based on the company's unique weaknesses and vulnerabilities, as well as the latest real-world attack techniques.

Through red team/blue team exercises it is possible for the organization to:

- Identify misconfigurations and coverage gaps in existing security products
- Strengthen network security to detect targeted attacks and improve breakout time
- Raise healthy competition among security personnel and foster cooperation among the IT and security teams
- Elevate awareness among staff as to the risk of human vulnerabilities which may compromise the organization's security
- Build the skills and maturity of the organization's security capabilities within a safe, low-risk training environment

Conclusion

Red teaming provides the most realistic test of your systems' and your organization's defenses against a cyber attack. If your organization is responsible for user data or relies on software systems for day-to-day running, you're vulnerable to ransomware and data exfiltration attacks. If you're developing software, verifying the security of your products and services is essential to protect your users from attacks that exploit your system. To get the most out of red teaming, make it an ongoing practice and ensure all findings are shared and acted upon.



What will next?

Now explore things by yourself and learn from internet.

Don't waste your time

You can do CTF to sharp your skill.

