Committed To Defence And Security Worldwide

DEFENCE & SECURITY ALERT

DECEMBER 2019 | VOLUME 11 | ISSUE 03 | ₹150

The First and Only ISO 9001:2015 Certified Defence and Security Magazine in India
The Only Magazine Available On The Intranet Of Indian Air Force

www.dsalert.org
info@dsalert.org

NAVY SPECIAL

Manpower and Technology for Futuristic Oceanic Navy: India's Expanding Role in the Seas

Admiral Karambir Singh
PVSM, AVSM, ADC
Chief of the Naval Staff

ISSN 0976-204X

10 YEARS OF EXCELLENCE

DSA™

An ISO 9001:2015 Certified Magazine

INTRUSION PREVENTION

Red team assessment is the only and fool proof method to check physical and human vulnerabilities beyond the technical vulnerability assessment. Red team engagement gives you an opportunity to identify weak entry points and patches the vulnerable node against the upcoming cyber-attacks.

Red teaming is a professionally simulated multi-layer attack practice to test how well a company or organisation is protected in terms of technical, human, and physical security against potential cyber-attacks in the real world. As per "dark reading" report in the first 9 months of the year 2019, 5,183 big data breaches reported worldwide with total 9.9 million records. That is an increase of almost 35 per cent in data breaches.

Realistic Attack

In red teaming, government and non-government agencies employ a team of security experts and are given full permission to break into their computer networks without any limitations. A good red teaming is not only about finding loopholes and weak entry points in your organisation, but also provides an opportunity to improve that defence in the future. This process is very similar, but not the same as vulnerability assessment and penetration testing, and is the pursuit of a goal to compromise an individual or organisation and extract valuable Intelligence. In this, every security officer should be prepared on how a cyber-attack or intrusion occurs in a real world situation and how should they react and handle the situation. Red teaming typically uses email or SMS in attack delivery mechanisms. Sometimes attackers send hacking payloads behind files from real software such as power point, document, music file, image or PDF. The email looks very similar to the official email address; when the victim opens the email without cross-verification, the hidden exploit will run in background and the hacker will be able to get access through the payload.

According to EY Global Information Security Survey 2018-19, 6.4 billion fake email sent worldwide, 1,946,181,599 records containing personal and other sensitive data compromised between January 2017 and March 2018, and 550 million phishing emails sent out by a single campaign during the first quarter of 2018.

Cyber Audit

In a red teaming assessment, highly trained security professionals perform various attacks on vectors to reveal technical, physical and human vulnerabilities. An auditor scans web applications, servers, network devices and other appliances of an organisation for technical audit. In regards to human mistakes, auditor performs a test for Phishing, Spear Phishing, Vishing, Smishing or other advanced social engineering attacks. For physical attacks, auditor runs a test to breach physical security at data centers, offices, warehouses and buildings. Physical security breach is considered as the biggest attack in the security department. Sometimes attacker can connect devices to the network such as "Raspberry Pi" via honey trapping attacks to steal the confidential information, through which cyber intruders can have complete access even from a remote location. "Killer USB" and "Rubber Ducky" can also be used to completely destroy a data center or a

Red teaming typically **uses email or SMS** in **attack delivery** mechanisms security agency. By simply inserting a pen drive, you can copy, destroy and alter its entire data or even hardware crash.

Penetration Methodology

In the context of information security, social engineering is a Psychological manipulation practice to shape a user to make security mistakes, provide access to critical infrastructure and share the sensitive information. Security consultants always gather information about the target prior to design a threat model, such as background, hobbies, profession and weak entry points. A picture uploaded by a soldier with a weapon can also pose a threat to the entire security department. If the profile of the same soldier is public, then the cyber Intelligence team of the country will easily find him on social media platforms. By pretending to be a senior officer or the government official of his country, the Intelligence team can trap him on social media. By taking advantage of this soldier as a launch pad, the internal security of the department can also be breached.

As per the perspective of the defence organisation, Red teaming is proving to be helpful for both offensive and defensive purposes.

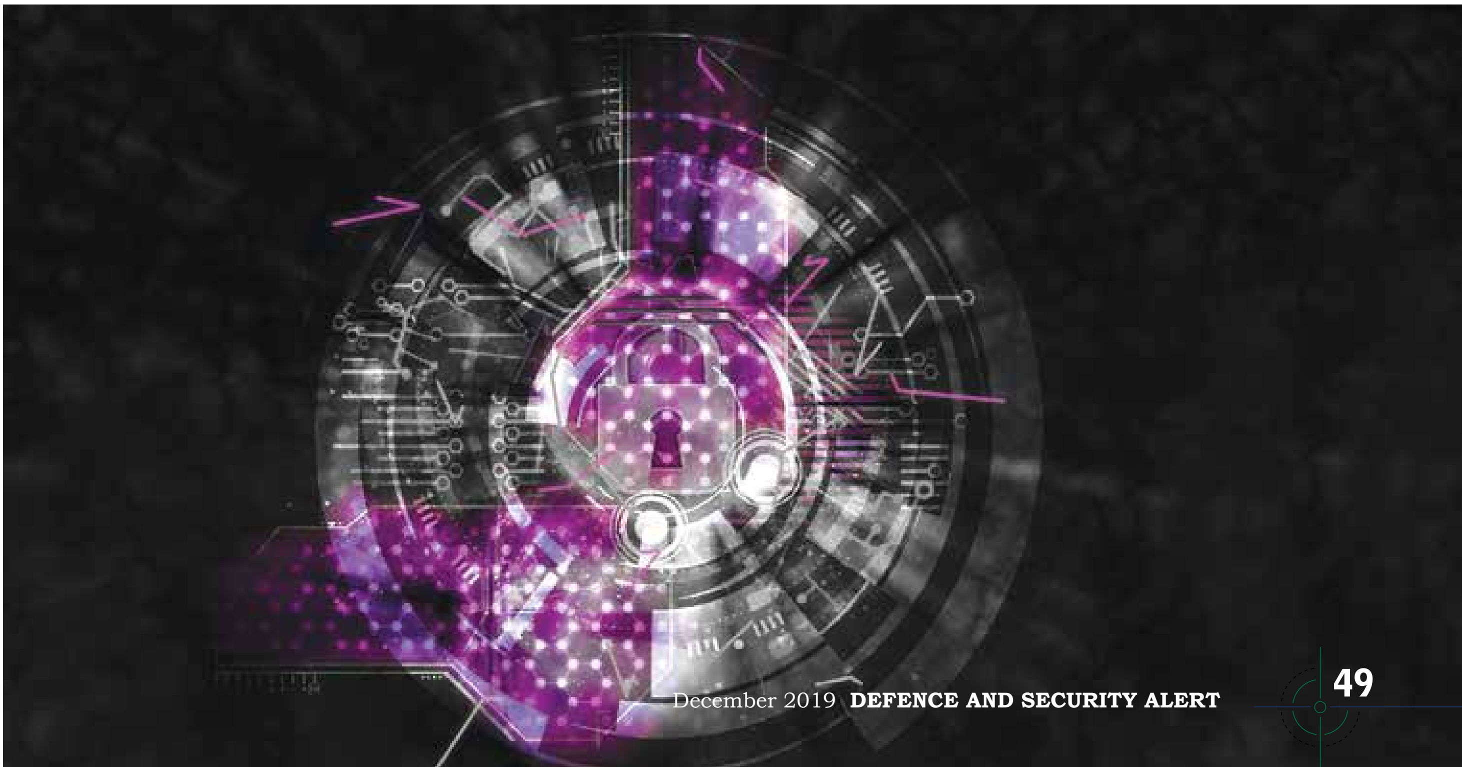
1. Red Teaming Offensive Approach

Earlier the countries have been investing major part of their defence budget to gather mass Intelligence but nowadays each country is putting efforts on specified Intelligence. In the era of technology, any country can only win a war if it is capable of putting down all the most critical and life-living required services of the targeted country. Attacker country can also put down all the services related to defence and misguide a leading battalion by giving the malicious instructions. But everything is not that easy, to get system level access, Intelligence officers have to burn midnight oil continuously from days or months or sometimes bigger target takes years. The main objective of a cyber-attacker is to get secret information of army unit, its current location, and the delegates in joint war exercise and arms supply from ordinance factory, etc.

UMMED MEEL

The writer is a Cyber Expert. He is closely associated with State Police, Air Force, BSF, CDTI, BPRD, CAG and Higher Defence authorities in India for last 5+ years. Ummed has conducted 100+training/workshops for Indian Police of Delhi, Uttar Pradesh, Rajasthan, Haryana and Himachal, etc. and trained more than 10,000 police officers and other LEAs. He has 5+ years of experience in Cyber Security, Vulnerability Assessment and Penetration Testing, Cybercrime investigation, Digital Evidence seizure and Digital Forensics.

Cyber Security Protection.



Cyber Scams.

In order to compromise a target, Intelligence Team initially focuses on the globally accessible resources like web application, social media, servers and computer devices. Pure red teaming concept arrives when the attacker wants to get into the network through social engineering attacks on individuals or physical security breaches. Based on the various cyber surveys we can conclude that defence personnel are the most vulnerable node to get secret information and war planning of an enemy country. The primary objective of an attacker is always to get an access and persistence into victim's mobile or computer devices. After getting persistence, the attacker tries privilege escalation and scans the available hosts into the compromised network. At the very end, attacker will implant a silent backdoor into their server, network, website and computer to maintain access. Almost every country has a single centralised data center to host their critical computer infrastructure. Once attacker gets access of any one server, it may lead to network infiltration and attacker can take over the whole data centre.

2. Red Teaming Defensive Approach

Nowadays defence organisations have started deploying firewalls and anti-viruses on their networks and security guards in their data centers. But apart from this some human errors lead to cyber-attacks which may cause huge impact on the organisation. Under the Digital India campaign, defence organisations have also started putting their departmental and operational databases online. However, every organisation has a dedicated cyber security team but somewhere security teams ignore less effective areas which may result in cyber-attacks. Red team assessment is the only and fool proof method to check physical and human vulnerabilities beyond the technical vulnerability assessment. Red team engagement gives you an opportunity to identify weak entry points and patches the vulnerable node against the upcoming cyber-attacks. Today, the most powerful country is the one which can destroy IT and its enabled services of the enemy country during the war and at the same time could also protect its own critical IT infrastructure against cyber-attacks. Red Teaming is a practice through which you can prepare yourself for the upcoming cyber-attacks.

As per EY Global Information Security Survey 2018-19, these are the top 10 biggest cyber threats to organisations:

Physical security breach is considered as the **biggest attack** in the security department

1. Phishing (22%)
2. Malware (20%)
3. Cyber Attacks (to disrupt) (13%)
4. Cyber Attacks (to steal money) (12%)
5. Frauds (10%)
6. Cyber Attacks (to steal IP) (8%)
7. Spam (6%)
8. Internal Attacks (5%)
9. Natural Disasters (2%)
10. Espionage (2%)

Whenever any security officer does any work, data will probably be stored on his own computer. Even if you have never been trapped by any cyber-attack yet that does not mean you are secured. With the help of outdated software which are running on your device, a cyber-attacker can break into your computer without your knowledge. Similarly, if you use a mobile phone, always check that the application is downloaded and updated from the trusted source only or it is not stealing your data in the background in some way or the other. Security officers should pay special attention to the permissions asked by any application while installation.

Intelligence Gathering

Intelligence through red teaming can get secret information like strength of military personnel, physical location of the battalion, war exercise, war strategy, nuclear weapons and upcoming weapon blueprints and consignments. Organisation stores secret information on their servers and any officer can access data via website or email and he can store it on his mobile or computer. Now attacker could compromise any one of the above said three nodes and will get the same details. So, for every specified military Intelligence, cyber does not have any hard and fast rule. For each target, security professionals require to design a unique threat model. Therefore, in order to protect our country and organisations from cyber war, we have to protect each and every entry node such as our departments, officers, websites, networks, data centers, etc. High quality training is the only solution to avoid man-made errors. From time to time, all the employees of the department should be informed about the newly discovered cyber-attacks so they do not fall prey to those attacks.

Preventive Measures

Cyber Intelligence cannot be stopped but it can be controlled up to a level by spreading cyber awareness. To avoid MITM attack, email and other data transmission mediums should be encrypted with strong algorithms. As far as possible, keep yourself away from social media; avoid giving confidential information on the official page of the department. Never upload photos with uniforms / weapons on social media or any online platform. Neither download nor open suspicious documents received from email. In any kind of artificial emergency, money greed and other abnormal situations, control yourself and do not share any kind of information with strangers. Always use secured internet to open your government email accounts, do not connect your device with public Wi-Fi as far as possible. Use modern intrusion detection and prevention system to prevent cyber intrusions. Avoid connecting the external data traveller devices; it may be a Rubber Ducky or killer USB. In case of any cyber-attack, logging and monitoring of the servers and other devices is essential for incident response.

Cyber Crime Awareness Foundation.