Red team

A **red team** is a group that simulates an adversary, attempts a physical or digital intrusion against an organization at the direction of that organization, then reports back so that the organization can improve their defenses. Red teams work for the organization or are hired by the organization. Their work is legal, but it can surprise some employees who may not know that red teaming is occurring, or who may be deceived by the red team. Some definitions of red team are broader, and they include any group within an organization that is directed to think outside the box and look at alternative scenarios that are considered less plausible. This directive can be an important defense against false assumptions and groupthink. The term *red teaming* originated in the 1960s in the United States.

Technical red teaming focuses on compromising networks and computers digitally. There may also be a blue team, a term for cybersecurity employees who are responsible for defending an organization's networks and computers against attack. In technical red teaming, attack vectors are used to gain access, and then reconnaissance is performed to discover more devices to potentially compromise. Credential hunting involves scouring a computer for credentials such as passwords and session cookies, and once these are found, can be used to compromise additional computers. During intrusions from third parties, a red team may team up with the blue team to assist in defending the organization. Rules of engagement and standard operating procedures are often utilized to ensure that the red team does not cause damage during their exercises.

Physical red teaming focuses on sending a team to gain entry to restricted areas. This is done to test and optimize physical security such as fences, cameras, alarms, locks, and employee behavior. As with technical red teaming, rules of engagement are used to ensure that red teams do not cause excessive damage during their exercises. Physical red teaming will often involve a reconnaissance phase where information is gathered and weaknesses in security are identified, and then that information will be used to conduct an operation (typically at night) to gain physical entry to the premises. Security devices will be identified and defeated using tools and techniques. Physical red teamers will be given specific objectives such as gaining access to a server room and taking a portable hard drive, or gaining access to an executive's office and taking confidential documents.

Red teams are used in several fields, including cybersecurity, airport security, law enforcement, the military, and intelligence agencies. In the United States government, red teams are used by the Army, Marine Corps, Department of Defense, Federal Aviation Administration, and Transportation Security Administration.

History

The concept of red teaming and blue teaming emerged in the early 1960s. One early example of red teaming involved the think tank RAND Corporation, which did simulations for the United States military during the Cold War. "Red team" and the color red were used to represent the Soviet Union, and "blue team" and the color blue were used to represent the United States.[1] Another early example involved

United States Secretary of Defense Robert McNamara, who assembled a red team and a blue team to explore which government contractor should be awarded an experimental aircraft contract.[1] Another early example modeled negotiating an arms control treaty and evaluating its effectiveness.[1]

Red teams are sometimes associated with "contrarian thinking" and fighting groupthink, the tendency of groups to make and keep assumptions even in the face of evidence to the contrary. One example of a group that was not called a red team, but that arguably was one of the earliest examples of forming a group to fight groupthink, is the Israeli Ipcha Mistraba that was formed after Israeli decision-making failures during the Yom Kippur War in 1973. The attack against Israel nearly took Israel by surprise despite ample evidence of an impending attack, and almost resulted in Israel's defeat. Ipcha Mistabra was formed after the war, and given the duty of always presenting a contrarian, unexpected, or unorthodox analysis of foreign policy and intelligence reports, so that things would be less likely to be overlooked going forward.[2]

In the early 2000s, there are examples of red teams being used for tabletop exercises. A tabletop exercise is often used by first responders and involves acting out and planning for worst case scenarios, similar to playing a tabletop board game. In response to the September 11 attacks, with anti-terrorism in mind, the Central Intelligence Agency created a new Red Cell,[3] and red teams were used for modeling responses to asymmetric warfare such as terrorism.[4] In response to the failures of the Iraq War, red teaming became more common in the United States Army.[5]

Over time, the practice of red teaming expanded to other industries and organizations, including corporations, government agencies, and non-profit organizations. The approach has become increasingly popular in the world of cybersecurity, where red teams are used to simulate real-world attacks on an organization's digital infrastructure and test the effectiveness of their cybersecurity measures,[6] and is progressing into the analysis of generative AI technologies such as LLMs.[7]

Cybersecurity

Technical red teaming involves testing the digital security of an organization by attempting to infiltrate their computer systems digitally.

Terminology

A *blue team* is a group in charge of defending against intrusions.

In cybersecurity, a *penetration test* involves ethical hackers ("pen testers") attempting to break into a computer system, with no element of surprise. The organization is aware of the penetration test and is ready to mount a defense.[8]

A *red team* goes a step further, and adds physical penetration, social engineering, and an element of surprise. The blue team is given no advance warning of a red team, and will treat it as a real intrusion.[8] One role of a permanent, in-house red team is to improve the security culture of the organization.[9]

A ***purple team*** is the temporary combination of both teams and can provide rapid information responses during a test.[10][11] One advantage of purple teaming is that the red team can launch certain attacks repeatedly, and the blue team can use that to set up detection software, calibrate it, and steadily increase detection rate.[12] Purple teams may engage in "threat hunting" sessions, where both the red team and the blue team look for real intruders. Involving other employees in the purple team is also beneficial, for example software engineers who can help with logging and software alerts, and managers who can help identify the most financially damaging scenarios.[13] One danger of purple teaming is complacence and the development of groupthink, which can be combatted by hiring people with different skillsets or hiring an external vendor.[14]

A *white team* is a group that oversees and manages operations between red teams and blue teams. For example, this may be a company's managers that determine the rules of engagement for the red team.[15]

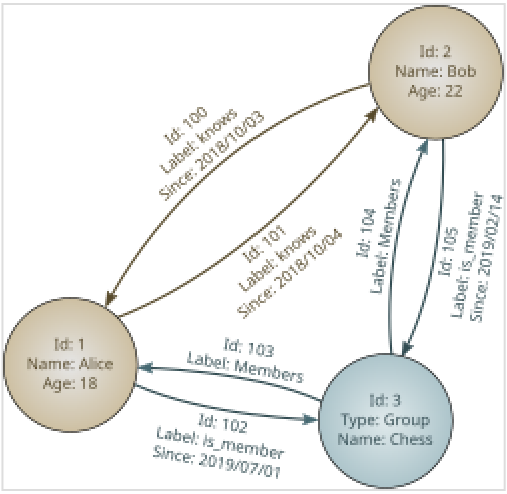
Attack

The initial entry point of a red team or an adversary is called the beachhead. A mature blue team is often adept at finding the beachhead and evicting attackers. A role of the red team is to increase the skills of the blue team.[16]

When infiltrating, there is a stealthy "surgical" approach that stays under the radar of the blue team and requires a clear objective, and a noisy "carpet bombing" approach that is more like a brute force attack. Carpet bombing is often the more useful approach for red teams, because it can discover unexpected vulnerabilities.[17]

There are a variety of cybersecurity threats. Threats may range from something traditional such as hacking the network's domain controller, or something less orthodox such as setting up cryptocurrency mining, or providing too much employee access to personally identifiable information (PII) which opens the company up to General Data Protection Regulation (GDPR) fines.[18] Any of these threats can be red teamed, in order to explore how severe the issue is. Tabletop exercises, where intrusions are acted out over a tabletop similar to how one would play a board game, can be used to simulate intrusions that are too expensive, too complicated, or illegal to execute live.[19] It can be useful to attempt intrusions against the red team and the blue team, in addition to more traditional targets.[20]

Once access to a network is achieved, reconnaissance can be conducted. The data gathered can be placed in a graph database, which is software that visually plots nodes, relationships, and properties. Typical nodes might be computers, users, or permission groups.[21] Red teams will usually have very good graph databases of their own organization, because they can utilize home-field advantage, including working with the blue team to create a thorough map of the network, and a thorough list of users and administrators.[22] A query language such as Cypher can be used to create and modify graph databases.[23] Any type of administrator account is valuable to place in the graph database, including administrators of third party tools such as Amazon Web Services (AWS).[24] Data can sometimes be exported from tools and then inserted into the graph database.[25]



An example of a graph database. For red teams, this software can be used to create a map of an infiltrated network. Nodes (the circles) are commonly computers, users, or permission groups.

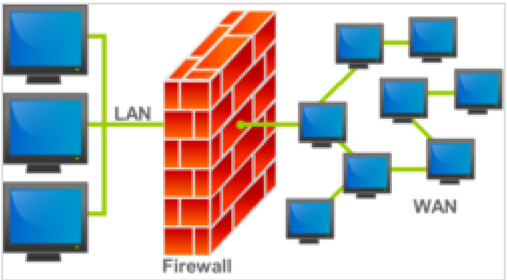
Once the red team has compromised a computer, website, or system, a powerful technique is credential hunting. These can be in the form of clear text passwords, ciphertext, hashes, or access tokens. The red team gets access to a computer, looks for credentials that can be used to access a different computer, then this is repeated, with the goal of accessing many computers.[26] Credentials can be stolen from many locations, including files, source code repositories such as Git, computer memory, and tracing and logging software. Techniques such as pass the cookie and pass the hash can be used to get access to websites and machines without entering a password. Techniques such as optical character recognition (OCR), exploiting default passwords, spoofing a credential prompt, and phishing can also be used.[27]

The red team can utilize computer programming and command-line interface (CLI) scripts to automate some of their tasks. For example, CLI scripts can utilize the Component Object Model (COM) on Microsoft Windows machines in order to automate tasks in Microsoft Office applications. Useful tasks might include sending emails, searching documents, encrypting, or retrieving data. Red teams can take control of a browser using Internet Explorer's COM, Google Chrome's remote debugging feature, or the testing framework Selenium.[28]

Defense

During a real intrusion, the red team can be repurposed to work with the blue team to help with defense. Specifically, they can provide analysis of what the intruders will likely try to do next. During an intrusion, both the red team and the blue team have a home-field advantage because they are more familiar with the organization's networks and systems than the intruder.[12]

An organization's red team may be an attractive target for real attackers. Red team member's machines may contain sensitive information about the organization. In response, red team member's machines are often secured.[29] Techniques for securing machines include configuring the operating system's firewall, restricting Secure Shell (SSH) and Bluetooth access, improving logging and alerts, securely deleting files, and encrypting hard drives.[30]



A network firewall (pictured) can be used to limit access to a private network from the wider Internet. A software firewall, such as a firewall built into a computer's operating system, can be used to limit remote access to that computer.

One tactic is to engage in "active defense", which involves setting up decoys and honeypots to help track the location of intruders.[31] These honeypots can help alert the blue team to a network intrusion that might otherwise have gone undetected. Various software can be used to set up a honeypot file depending on the operating system: macOS tools include OpenBMS, Linux tools include auditd plugins, and Windows tools include System Access Control Lists (SACL). Notifications can include popups, emails, and writing to a log file.[32] Centralized monitoring, where important log files are quickly sent to logging software on a different machine, is a useful network defense technique.[33]

Managing a red team

The use of rules of engagement can help to delineate which systems are off-limits, prevent security incidents, and ensure that employee privacy is respected.[34] The use of a standard operating procedure (SOP) can ensure that the proper people are notified and involved in planning, and improve the red team process, making it mature and repeatable.[35] Red team activities typically have a regular rhythm.[36]

Tracking certain metrics or key performance indicators (KPIs) can help to make sure a red team is achieving the desired output. Examples of red team KPIs include performing a certain number of penetration tests per year, or by growing the team by a certain number of pen testers within a certain time period. It can also be useful to track the number of compromised machines, compromisable machines, and other metrics related to infiltration. These statistics can be graphed by day and placed on a dashboard displayed in the security operations center (SOC) to provide motivation to the blue team to detect and close breaches.[37]

A security operations center (SOC) at the University of Maryland

In order to identify worst offenders, compromises can be graphed and grouped by where in the software they were discovered, company office location, job title, or department.[38] Monte Carlo simulations can be used to identify which intrusion scenarios are most likely, most damaging, or both.[39] A Test Maturity Model, a type of Capability Maturity Model, can be used to assess how mature a red team is, and what the next step is to grow.[40] The MITRE ATT&CK Navigator, a list of tactics, techniques, and procedures (TTPs) including advanced persistent threats (APTs), can be consulted to see how many TTPs a red team is exploiting, and give additional ideas for TTPs to utilize in the future.[41]

Physical intrusion

Physical red teaming or physical penetration testing[42] involves testing the physical security of a facility, including the security practices of its employees and security equipment. Examples of security equipment include security cameras, locks, and fences. In physical red teaming, computer networks are not usually the target.[43] Unlike cybersecurity, which typically has many layers of security, there may only be one or two layers of physical security present.[44]

Having a "rules of engagement" document that is shared with the client is helpful, to specify which TTPs will be used, what locations may be targeted, what may not be targeted, how much damage to equipment such as locks and doors is permitted, what the plan is, what the milestones are, and sharing contact information.[45][46] The rules of engagement may be updated after the reconnaissance phase, with another round of back and forth between the red team and the client.[47] The data gathered during the reconnaissance phase can be used to create an operational plan, both for internal use, and to send to the client for approval.[48]

Reconnaissance

Part of physical red teaming is performing reconnaissance.[49] The type of reconnaissance gathered usually includes information about people, places, security devices, and weather.[50] Reconnaissance has a military origin, and military reconnaissance techniques are applicable to physical red teaming. Red team reconnaissance equipment might include military clothing since it does not rip easily, red lights to preserve night vision and be less detectable, radios and earpieces, camera and tripod, binoculars, night vision equipment, and an all-weather notebook.[51] Some methods of field communication include a Bluetooth earpiece dialed into a cell phone conference call during the day, and two-way radios with earpieces at night.[52] In case of compromise, red team members often carry identification and an authorization letter with multiple after-hours contacts who can vouch for the legality and legitimacy of the red team's activities.[53]

Two-way radios and earpieces are sometimes used by physical red teams conducting operations at night. Something less conspicuous such as Bluetooth earbuds may be preferred during the day.

Before physical reconnaissance occurs, open-source intelligence (OSINT) gathering can occur by researching locations and staff members via the Internet, including the company's website, social media accounts, search engines, mapping websites, and job postings (which give hints about the technology and software the company uses).[54] It is a good practice to do multiple days of reconnaissance, to reconnoiter both during the day and at night, to bring at least three operators, to utilize a nearby staging area that is out of sight of the target, and to do reconnaissance and infiltration as two separate trips rather than combining them.[55]

Recon teams can use techniques to conceal themselves and equipment. For example, a passenger van can be rented and the windows can be blacked out to conceal photography and videography of the target.[56] Examining and videoing the locks of a building during a walk-around can be concealed by the recon pretending to be on the phone.[57] In the event of compromise, such as employees becoming suspicious, a story can be rehearsed ahead of time until it can be recited confidently. If the team has split up, the compromise of one operator can result in the team leader pulling the other operators out.[58] Concealed video cameras can be used to capture footage for later review, and debriefs can be done quickly after leaving the area so that fresh information is quickly documented.[59]

Infiltration

Most physical red team operations occur at night, due to reduced security of the facility and so that darkness can conceal activities.[60] An ideal infiltration is usually invisible both outside the facility (the approach is not detected by bystanders or security devices) and inside the facility (no damage is done and nothing is bumped or left out of place), and does not alert anyone that a red team was there.[61]

Preparation

The use of a load out list can help ensure that important red team equipment is not forgotten.[62] The use of military equipment such as MOLLE vests and small tactical bags can provide useful places to store tools, but has the downsides of being conspicuous and increasing encumbrance.[63] Black clothing or dark camouflage can be helpful in rural areas, whereas street clothes in shades of gray and black may be preferred in urban areas.[64] Other urban disguise items include a laptop bag, or a pair of headphones around the neck. Various types of shoe coverings can be used to minimize footprints both outdoors and indoors.[65]

Approach

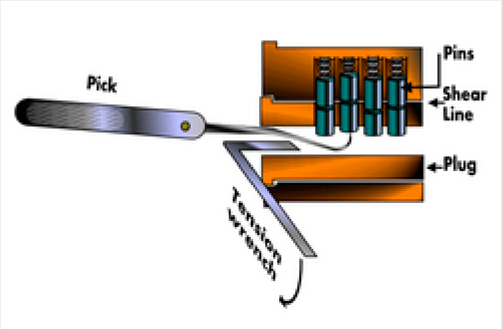
Light discipline (keeping lights from vehicles, flashlights, and other tools to a minimum) reduces the chance of compromise.[60] Some tactics of light discipline include using red flashlights, using only one vehicle, and keeping the vehicle's headlights off.[60]

Sometimes there are security changes between reconnaissance and infiltration, so it is a good practice for teams that are approaching a target to "assess and acclimate", to see if any new security measures can be seen.[66] Compromises during infiltration are most likely to occur during the approach to the facility.[67] Employees, security, police, and bystanders are the most likely compromise a physical red team.[68] Bystanders are rarer in rural areas, but also much more suspicious.[69]

Proper movement can help a red team avoid being spotted while approaching a target, and may include rushing, crawling, avoiding silhouetting when on hills, walking in formations such as single file, and walking in short bursts then pausing.[70] The use of hand signals may be used to reduce noise.[71]

Entering the facility

Common security devices include doors, locks, fences, alarms, motion sensors, and ground sensors. Doors and locks are often faster and quieter to bypass with tools and shims, rather than lock picking.[72] RFID locks are common at businesses, and covert RFID readers combined with social engineering during reconnaissance can be used to duplicate an authorized employee's badge.[73] Barbed wire on fences can be bypassed by placing a thick blanket over it.[74] Anti-climb fences can be bypassed with ladders.[75]



Lock picking is regarded by some physical red teams as an inferior method of bypassing locks, due to the noise and time it takes compared to using lower skill attacks such as shims.

Alarms can sometimes be neutralized with a radio jammer that targets the frequencies that alarms use for their internal and external communications.[76] Motion sensors can be defeated with a special body-sized shield that blocks a person's heat signature.[77] Ground sensors are prone to false positives, which can lead security personnel to not trust them or ignore them.[78]

Inside the facility

Once inside, if there is suspicion that the building is occupied, disguising oneself as a cleaner or employee using the appropriate clothing is a good tactic.[79] Noise discipline is often important once inside a building, as there are less ambient sounds to mask red team noises.[80]

Red teams usually have goal locations selected and tasks pre-planned for each team or team member, such as entering a server room or an executive's office. However, it can be difficult to figure out a room's location in advance, so this is often figured out on the fly. Reading emergency exit route signs and the use of a watch with a compass can assist with navigating inside of buildings.[81]

Commercial buildings will often have some lights left on. It is good practice to not turn lights on or off, as this may alert someone. Instead, utilizing already unlit areas is preferred for red team operations, with rushing and freezing techniques to be used to quickly move through illuminated areas.[82] Standing fullheight in front of windows and entering buildings via lobbies is often avoided due to the risks of being seen.[83]

A borescope can be used to peer around corners and under doors, to help spot people, cameras, or motion detectors.[84]

Once the target room has been reached, if something needs to be found such as a specific document or specific equipment, the room can be divided into sections, with each red team member focusing on a section.[85]

A server room can be an alluring target for red teams. Physical access to a server can help gain entry into secured networks that are otherwise well-protected from digital threats.

Passwords are often located under keyboards. Techniques can be used to avoid disturbing the placement of objects in offices such as keyboards and chairs, as adjusting these will often be noticed.[86] Lights and locks can be left in their original state of on or off, locked or unlocked.[87] Steps can be taken to ensure that equipment is not left behind, such as having a list of all equipment brought in and checking that all items are accounted for.[88]

It is good practice to radio situation reports (SITREPs) to the team leader when unusual things happen. The team leader can then decide if the operation should continue, should be aborted, or if a team member should surrender by showing their authorization letter and ID.[89] When confronted by civilians such as employees, red team operators can attempt social engineering. When confronted by law enforcement, it is good practice to immediately surrender due to the potential legal and safety consequences.[90]

Exiting the facility

The ideal way to exit a facility is slowly and carefully, similar to how entry was achieved. There is sometimes an urge to rush out after achieving a mission goal, but this is not good practice. Exiting slowly and carefully maintains situational awareness, in case a previously empty area now has someone in it or approaching it.[91] While the entrance path is normally taken during exit, a closer or alternative exit can also be used.[92]

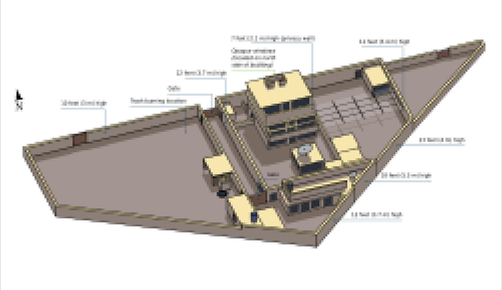
The goal of all team members is to reach the rally point, or possibly a second emergency rally point. The rally point is usually at a different location than the dropoff point.[93]

Users

Companies and organizations

Private companies sometimes use red teams to supplement their normal security procedures and personnel. For example, Microsoft and Google utilize red teams to help secure their systems.[94][95] Some financial institutions in Europe use the TIBER-EU framework.[96]

Intelligence agencies



Terrorist leader Osama Bin Laden's compound in Pakistan. Three red teams were used to review the intelligence that led to the killing of Osama bin Laden in 2011.

When applied to intelligence work, red teaming is sometimes called **alternative analysis**.[97] Alternative analysis involves bringing in fresh analysts to double-check the conclusions of another team, to challenge assumptions and make sure nothing was overlooked. Three red teams were used to review the intelligence that led to the killing of Osama bin Laden in 2011, including red teams from outside the Central Intelligence Agency, because there were major diplomatic and public relations consequences for launching a military operation into Pakistan, so it was important to double-check the original team's intelligence and conclusions.[98]

After failures to anticipate the Yom Kippur War, the Israeli Defense Forces' Intelligence Directorate formed a red team called *Ipcha Mistabra* ("on the contrary") to re-examine discarded assumptions and avoid complacency.[2] The North Atlantic Treaty Organization (NATO) utilizes alternative analysis.[99]

Militaries

Militaries typically uses red teaming for alternative analysis, simulations, and vulnerability probes.[100] In military wargaming, the opposing force (OPFOR) in a simulated conflict may be referred to as a Red Cell.[101] The key theme is that the adversary (red team) leverages tactics, techniques, and equipment as appropriate to emulate the desired actor. The red team challenges operational planning by playing the role of a mindful adversary.

The United Kingdom Ministry of Defence has a red team program.[102]

Red teams were used in the United States Armed Forces much more frequently after a 2003 Defense Science Review Board recommended them to help prevent the shortcomings that led to the September 11 attacks. The U.S. Army created the Army Directed Studies Office in 2004. This was the first service-level red team, and until 2011 was the largest in the Department of Defense (DoD).[103] The University of Foreign Military and Cultural Studies provides courses for red team members and leaders. Most resident courses are conducted at Fort Leavenworth and target students from U.S. Army Command and General Staff College (CGSC) or equivalent intermediate and senior level schools.[104] Courses include topics such as critical thinking, groupthink mitigation, cultural empathy, and self-reflection.[105]

The Marine Corps red team concept commenced in 2010 when the Commandant of the Marine Corps (CMC) General James F. Amos attempted to implement it.[106] Amos drafted a white paper titled, *Red Teaming in the Marine Corps*. In this document, Amos discussed how the concept of the red team needs to challenge the process of planning and making decisions by applying critical thinking from the tactical to strategic level. In June 2013, the Marine Corps staffed the red team billets outlined in the draft white paper. In the Marine Corps, all Marines designated to fill red team positions complete either six-week or nine-week red team training courses provided by the University of Foreign Military and Cultural Studies (UFMCS).[107]

The DoD uses cyber red teams to conduct adversarial assessments on their networks.[108] These red teams are certified by the National Security Agency and accredited by the United States Strategic Command.[108]

Red team operatives during a United States European Command cyber warfare exercise

Airport security

The United States Federal Aviation Administration (FAA) has been implementing red teams since Pan Am Flight 103 over Lockerbie, Scotland, which suffered a terrorist attack in 1988. Red teams conduct tests at about 100 US airports annually. Tests were on hiatus after the September 11 attacks in 2001, and resumed in 2003 under the Transportation Security Administration, who assumed the FAA's aviation security role after 9/11.[109] Before the September 11 attacks, FAA use of red teaming revealed severe weaknesses in security at Logan International Airport in Boston, where two of the four hijacked 9/11 flights originated. Some former FAA investigators who participated on these teams feel that the FAA deliberately ignored the results of the tests, and that this resulted in part in the 9/11 terrorist attack on the US.[110]

The United States Transportation Security Administration has used red teaming in the past. In one red team operation, undercover agents were able to fool Transportation Security Officers and bring weapons and fake explosives through security 67 out of 70 times in 2015.[111]

Red teams are used by some airport security organizations such as the United States Transportation Security Administration to test the accuracy of airport screening.

See also

- Bogdan Dzakovic – FAA whistleblower and member of Veteran Intelligence Professionals for Sanity
- Black hat hacking
- Eligible Receiver 97
- Exploit (computer security)
- Grey hat
- Groupthink
- Hacker (computer security)
- Hacker ethic
- IT risk
- Metasploit
- Murder board
- Vulnerability (computing)
- Wireless identity theft

References

1. Zenko, p. 56
2. Hoffman, p. 37
3. Hoffman, p. 39
4. Zenko, p. 57
5. Hoffman, p. 32
6. "What is red teaming?" (https://www.techtarget.com/whatis/definition/red-teaming). *WhatIs.com*. Retrieved May 14, 2023.
7. Inie, Nanna (2025). "Summon a Demon and Bind it: A Grounded Theory of LLM Red Teaming" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11734899). *PLOS ONE*. **20** (1) e0314658. arXiv:2311.06237 (https://arxiv.org/abs/2311.06237). Bibcode:2025PLoSO..2014658I (https://ui.adsabs.harvard.edu/abs/2025PLoSO..2014658I). doi:10.1371/journal.pone.0314658 (https://doi.org/10.1371%2Fjournal.pone.0314658). PMC 11734899 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11734899). PMID 39813184 (https://pubmed.ncbi.nlm.nih.gov/39813184).
8. "Penetration Testing Versus Red Teaming: Clearing the Confusion" (https://securityintelligence.com/posts/penetration-testing-versus-red-teaming-clearing-the-confusion/). *Security Intelligence*. Retrieved December 23, 2020.
9. Rehberger, p. 3
10. "The Difference Between Red, Blue, and Purple Teams" (https://danielmiessler.com/study/red-blue-purple-teams/). *Daniel Miessler*. Retrieved April 3, 2022.
11. "What is Purple Teaming? How Can it Strengthen Your Security?" (https://www.redscan.com/news/purple-teaming-can-strengthen-cyber-security/). *Redscan*. September 14, 2021. Retrieved April 3, 2022.
12. Rehberger, p. 66
13. Rehberger, p. 68
14. Rehberger, p. 72
15. "White Team – Glossary | CSRC" (https://csrc.nist.gov/glossary/term/white_team). *National Institute of Standards and Technology, United States Department of Commerce*. Retrieved May 23, 2023.
16. Rehberger, pp. 40–41
17. Rehberger, p. 44
18. Rehberger, p. 117
19. Rehberger, p. 132
20. Rehberger, p. 127
21. Rehberger, p. 140
22. Rehberger, p. 138
23. Rehberger, p. 165
24. Rehberger, p. 178
25. Rehberger, p. 180
26. Rehberger, p. 203
27. Rehberger, p. 245
28. Rehberger, p. 348
29. Rehberger, p. 70
30. Rehberger, p. 349
31. Rehberger, pp. 70–71

32. Rehberger, p. 447
33. Rehberger, p. 473
34. Rehberger, p. 23
35. Rehberger, p. 26
36. Rehberger, p. 73
37. Rehberger, pp. 93–94
38. Rehberger, pp. 97–100
39. Rehberger, p. 103
40. Rehberger, p. 108
41. Rehberger, p. 111
42. Talamantes, pp. 24–25
43. Talamantes, pp. 26–27
44. Talamantes, p. 153
45. Talamantes, p. 41
46. Talamantes, p. 48
47. Talamantes, p 110
48. Talamantes, pp. 112–113
49. Talamantes, p. 51
50. Talamantes, p. 79
51. Talamantes, pp. 58–63
52. Talamantes, p. 142
53. Talamantes, pp. 67–68
54. Talamantes, p. 83
55. Talamantes, pp. 72–73
56. Talamantes, pp. 89–90
57. Talamantes, p. 98
58. Talamantes, pp. 100–101
59. Talamantes, p. 102
60. Talamantes, p. 126
61. Talamantes, p. 136
62. Talamantes, p. 137
63. Talamantes, pp. 133–135
64. Talamantes, p. 131
65. Talamantes, p. 287
66. Talamantes, p. 153
67. Talamantes, p. 160
68. Talamantes, p. 173
69. Talamantes, p. 169
70. Talamantes, pp. 183–185
71. Talamantes, p. 186
72. Talamantes, p. 215
73. Talamantes, p. 231
74. Talamantes, p. 202
75. Talamantes, p. 201
76. Talamantes, p. 213

77. Talamantes, p. 208
78. Talamantes, p. 199
79. Talamantes, p. 238
80. Talamantes, p. 182
81. Talamantes, pp. 242–243
82. Talamantes, p. 247
83. Talamantes, p. 246
84. Talamantes, p. 249
85. Talamantes, p. 253
86. Talamantes, p. 284
87. Talamantes, p. 286
88. Talamantes, p. 296
89. Talamantes, p. 266
90. Talamantes, p. 267
91. Talamantes, p. 272
92. Talamantes, p. 273
93. Talamantes, p. 274
94. "Microsoft Enterprise Cloud Red Teaming" (http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf) (PDF). *Microsoft.com*.
95. "Google's hackers: Inside the cybersecurity red team that keeps Google safe" (https://www.zdnet.com/article/googles-hackers-inside-the-cybersecurity-red-team-that-keeps-google-safe/). *ZDNET*. Retrieved June 2, 2023.
96. European Central Bank (March 23, 2023). What is TIBER-EU? (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html) (Report).
97. Mateski, Mark (June 2009). "Red Teaming: A Short Introduction (1.0)" (https://archive.today/20171205132811/https://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20(1dot0).pdf) (PDF). *RedTeamJournal.com*. Archived from the original (http://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20(1dot0).pdf) (PDF) on December 5, 2017. Retrieved July 19, 2011.
98. Zenko, pp. 127–128
99. *The NATO Alternative Analysis Handbook* (https://www.act.nato.int/wp-content/uploads/2023/05/alta-handbook.pdf) (PDF) (2nd ed.). 2017. ISBN 978-92-845-0208-0.
100. Zenko, p. 59
101. United Kingdom Ministry of Defence, p. 67
102. United Kingdom Ministry of Defence, p. 6
103. Mulvaney, Brendan S. (July 2012). "Strengthened Through the Challenge" (https://web.archive.org/web/20130928011442/http://www.hqmc.marines.mil/Portals/138/Docs/PL/PLU/Mulvaney.pdf) (PDF). *Marine Corps Gazette*. Marine Corps Association. Archived from the original (http://www.hqmc.marines.mil/Portals/138/Docs/PL/PLU/Mulvaney.pdf) (PDF) on September 28, 2013. Retrieved October 23, 2017 – via HQMC.Marines.mil.
104. "UFMCS Course Enrollment" (https://web.archive.org/web/20150905181714/http://usacac.army.mil/organizations/ufmcs-red-teaming/enrollment). Archived from the original (http://usacac.army.mil/organizations/ufmcs-red-teaming/enrollment) on September 5, 2015.
105. "University of Foreign Military and Cultural Studies Courses" (https://web.archive.org/web/20150706020123/http://usacac.army.mil/organizations/ufmcs-red-teaming/classes). *army.mil*. Archived from the original (http://usacac.army.mil/organizations/ufmcs-red-teaming/classes) on July 6, 2015. Retrieved October 23, 2017.

106. "Red Team: To Know Your Enemy and Yourself" (https://www.cfr.org/conference-calls/red-team-know-your-enemy-and-yourself). *Council on Foreign Relations*. Retrieved May 24, 2023.
107. Amos, James F. (March 2011). "Red Teaming in the Marine Corps".
108. "Chairman of the Joint Chiefs of Staff Manual 5610.03" (https://web.archive.org/web/20161201105622/http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651003.pdf) (PDF). Archived from the original (http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651003.pdf) (PDF) on December 1, 2016. Retrieved February 25, 2017.
109. Sherman, Deborah (March 30, 2007). "Test devices make it by DIA security" (http://www.denverpost.com/news/ci_5552494). *Denver Post*.
110. "National Commission on Terrorist Attacks Upon the United States" (http://govinfo.library.unt.edu/911/hearings/hearing2/witness_dzakovic.htm). *govinfo.library.unt.edu*. University of North Texas. Retrieved October 13, 2015.
111. Bennett, Brian (June 2, 2015). "Red Team agents use disguises, ingenuity to expose TSA vulnerabilities" (https://www.latimes.com/nation/nationnow/la-na-tsa-screeners-20150602-story.html). *Los Angeles Times*. Retrieved June 3, 2023.

Bibliography

- Hoffman, Bryce (2017). *Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything*. Crown Business. ISBN 978-1-101-90598-2.
- Rehberger, Johann (2020). *Cybersecurity Attacks – Red Team Strategies*. Packt Publishing. ISBN 978-1-83882-886-8.
- Talamantes, Jeremiah (2019). *Physical Red Team Operations*. Hexcode Publishing. ISBN 978-0-578-53840-2.
- United Kingdom Ministry of Defence (2010). *DCDC Guidance Note: A Guide to Red Teaming* (http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/B0558FA0-6AA7-4226-A24C-2B7F3CCA9A7B/0/RedTeamingGuiderevised12Feb10Webversion.pdf) (PDF). Archived from the original (http://www.mod.uk/NR/rdonlyres/B0558FA0-6AA7-4226-A24C-2B7F3CCA9A7B/0/RedTeamingGuiderevised12Feb10Webversion.pdf) (PDF) on October 26, 2012.
- Zenko, Micah (2015). *Red Team: How to Succeed By Thinking Like the Enemy*. Basic Books. ISBN 978-0-465-07395-5.
- Inie, Nanna (2025). "Summon a Demon and Bind it: A Grounded Theory of LLM Red Teaming" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11734899). *PLOS ONE*. **20** (1) e0314658. arXiv:2311.06237 (https://arxiv.org/abs/2311.06237). Bibcode:2025PLoSO..2014658I (https://ui.adsabs.harvard.edu/abs/2025PLoSO..2014658I). doi:10.1371/journal.pone.0314658 (https://doi.org/10.1371%2Fjournal.pone.0314658). PMC 11734899 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11734899). PMID 39813184 (https://pubmed.ncbi.nlm.nih.gov/39813184).

Further reading

- Craig, Susan (March–April 2007). "Reflections from a Red Team Leader" (https://grc-usmcu.libguides.com/ld.php?content_id=37711310). *Military Review*. Retrieved June 17, 2023.
- "Defense Science Board – Task Force on the Role and Status of DoD Red Teaming Activities" (http://www.fas.org/irp/agency/dod/dsb/redteam.pdf) (PDF). U.S. Department of Defense. September 2003. Retrieved June 17, 2023.
- Mulvaney, Brendan S. (November 1, 2012). "Don't Box in the Red Team" (http://armedforcesjournal.com/dont-box-in-the-red-team/). *Armed Forces Journal*. Retrieved June 17, 2023.

- *The Red Team Handbook: The Army's Guide to Making Better Decisions* (https://web.archive.org/web/20191114202232/https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf) (PDF) (Ninth ed.). University of Foreign Military and Cultural Studies. Archived from the original (https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf) (PDF) on November 14, 2019. Retrieved June 17, 2023.
- *Red Teaming Handbook* (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027158/20210625-Red_Teaming_Handbook.pdf) (PDF) (Third ed.). U.K. Ministry of Defence. June 2023.
- Ricks, Thomas E. (February 5, 2007). "Officers With PhDs Advising War Effort" (https://www.washingtonpost.com/wp-dyn/content/article/2007/02/04/AR2007020401196.html). *Washington Post*. Retrieved June 17, 2023.
- "The Role and Status of DoD Red Teaming Activities" (https://web.archive.org/web/20090419081417/http://www.acq.osd.mil/dsb/reports/redteam.pdf) (PDF). *Defense Science Board Task Force*. U.S. Department of Defense. September 2003. Archived from the original (http://www.acq.osd.mil/dsb/reports/redteam.pdf) (PDF) on April 19, 2009. Retrieved June 17, 2023.
- Second public hearing of the National Commission on Terrorist Attacks Upon the United States: Statement of Bogdan Dzakovic (https://www.9-11commission.gov/hearings/hearing2/witness_dzakovic.htm) (Report). National Commission on Terrorist Attacks Upon the United States. May 22, 2003. Retrieved June 17, 2023.
- GAO Red Team reveals Nuclear material can easily be smuggled into the United States years after 911 attack (https://web.archive.org/web/20070310174156/http://www.guardian.co.uk/worldlatest/story/0,,-5714956,00.html)