Defining and Categorizing a Red Team

Boyd White

March 26, 2012

Advisor: Gerald Lawver

Eastern Michigan University

Abstract

"If ignorant both of your enemy and yourself, you are certain to be in peril."

– Sun Tzu

The advanced, persistent threat (APT) and a large population of capable, ongoing cyber criminals are developing actors in the global war against information security. While many organizations have the basic tenets of security in place and regularly test their standard auditable procedures, they are caught off guard by exposed vulnerabilities and risks never brought to the attention of Information Technology (IT) management. A red team approach provides a proven method of risk analysis which uncovers risks and quickly adapts to real world approaches taken by our adversaries. This paper defines core components used by successful red teams and proposes a method for categorizing and implementing red teaming as a set of negotiable services and processes.

Please note: a free copy of the revised version of this document will be available on http://www.openredteam.com along with a manager's overview presentation to further the development of red teams in organizations.

Table of Contents

Defining and Categorizing a Red Team

Jay Radcliffe is a diabetic. Each day he rises out of bed and attaches an electronic device around his waist. This electronic device monitors insulin and auto adjusts delivery levels to issue a safe dosage. One day, while wondering how his device was controlled wirelessly, he suddenly felt an onset of “sheer terror, to know that there's no security around the devices which are a very active part of keeping [him] alive," (Storm, 2011). Jay had discovered that his diabetic device, which helps to keep him alive, could be adjusted from a great distance away to send a lethal dosage of insulin by anyone with a wireless transmitter and a computer. By applying his curiosity to an adversarial mindset, he found a weakness that could save lives, including his own. This is the core process of red teaming: asking a question, finding a problem that no one else noticed, and helping to correct it.

Conventional Risk for Businesses

Risk is defined by National Information Standards and Technology (NIST 800-30) as “a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of the adverse event.” Vulnerability is defined in the same standard as “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach [or policy].”

Before Jay knew that there was a problem with his insulin device there was no known vulnerability. Then, Jay posed a hypothetical adverse event with a high impact with no known threat source (other than himself). He proceeded to build a device and test that idea. Finally, he was able to identify a critical vulnerability. Even though Jay’s risk has no known threat-source, it is quite reasonable to understand the urgency to applying a fix. The example of Jay Radcliff is an

example that highlights the problem of applying security protections to risks and vulnerabilities that are already defined instead of thinking like your adversary.

For business and governments, risks are often thought of as an event compromising confidentiality, integrity, and/or availability of data. These risks are then compared to the overall cost. If the risk is lower than the expected cost, a countermeasure is not worth implementing. If countermeasures do not allow business to function they might not be implemented either. Risks can be accepted as part of business, ignored or rejected by management, transferred to an insurance company, but many more are not known.

Deciding upon risk criticality as a one-time risk rating may not be appropriate; risks and counter measures continue to evolve as technology interacts increasingly with humans and other technology. Consider that throughout time technology inherently brought new risk - even though specific risk vectors were not yet defined. Bringing electricity into the home increased the risk of fire and electrocution. Controls such as fuses, fire extinguishers, among other devices were eventually put in place to decrease risk when implementing this new technology in homes and workplaces. Another historical example is advancing automobile speeds increasing fatalities. To combat this, laws requiring people to wear seatbelts were implemented and automobile manufactures were forced to improve vehicle safety standards. This reactionary approach of safeguard implementation in technology development has been applied for many years with minimal forward thinking thoughts on security.

Today, new devices are being created and implemented which may also have significant risk to the data and services that are being offered. A lot of data is being compromised – so are identities and bank accounts. A report on the 2011 Verizon data breaches details an incredibly diverse set of emerging threat vectors and millions of records being compromised annually.

Exploited risks are not coming without a price tag for businesses either. Forbes recently reported that at the current trend, data loss will account for $290 Billion dollars annually in 2018, or 1.6% of America's GDP (Savitz, 2012). Regulatory fines, multitudes of semi-technical attacks against companies (Smith, 2011), and lawsuits also add to a significant financial impact.

What Red Teaming is Not

There are many guides, frameworks, and tools developed to list the types of tools and techniques which can be used in information security assessments. Two notable examples are the Open Source Security Testing Methodology Manual (OSSTMM) and Open Web Application Security Project (OWASP). The website VulnerabilityAssesment.co.uk also has a fairly extensive penetration testing framework with many tools and examples. Additionally, many small websites have started offering lists of targeted frameworks for technologies such as Bluetooth. However, the sheer diversity of technologies prevents a single source from addressing all methods of attacks and do not approach them from a red teaming point of view, but rather narrowly as their own domain.

The closest guide to red teaming offered to the public to date is NIST 800-115 which includes information on social engineering, penetration testing, and tabletops. However, NIST fails to address is the difference in red teaming techniques and how that builds upon audit, compliance, and security to offer an effective adversarial approach. While auditors and penetration testers perform the tests as prescribed, and often well documented, a red teamer performs security assessments and testing from a unique position to identify new threat vectors or attacks.

These models have also defined a testing methodology to cover some of the same areas in offensive security, but do not document or make an attempt at categorizing a list of adversarial services. OSSTMM offers well thought out audit plans. OWASP provides tests and an

organization focused on uncovering and removing web application issues. NIST defines some social engineering and tabletop exercises. However, none of these models are a catalogue of adversarial services; they do not provide a much needed deeper understanding of why the tests are being performed.

Red teaming is also not about discovering and/or using "zero days" or "oh days" against computer systems. Zero day exploits typically uncover a buffer overflow in a service which has no patch or is unknown to the public. This type of research is necessary and important and may be used in red team assessments, but is a technical, specialized field and not discussed in this paper.

Mindset and Distinction of a Red Teamer

There are many purposes and definitions for red teams (Mateski, 2009) (Meehan, 2007) (Skroch, 2009) (Golandsky, 2011). Most definitions point to red teams as role playing as adversaries or competitors whose goal is to identify threats counter to the consumer's goal. In some cases, red teams are asked to identify and follow the impact in a confined, safe manner to provide the consumer with proof of threats and motivate management into believing and removing the risk[1].

Businesses use red teams to prepare against "hacktivists" and data thieves. Governments use red teams to prepare for state sponsored hackers. Militaries use red teams in wargames to portray adversarial opposing forces (OPFOR). With a diverse set of clients and variations in scope, a solid definition and distinction of a red team may be difficult to create after it has had so many uses in private and public sectors. However, there are other approaches to consider in defining a red team for commercial enterprise, such as defining red team from a service offering.

[1] Red teams do not have the ultimate decision to remove risk, but should work with management so they can provide viable recommendations.

Red teamers are different from regular security personnel. They provide creative, adversarial, "devil's advocate", and/or apply concepts in new ways to determine what information is valuable. Some have described this adversarial approach to that of ninjas, or *Zukin*, using unconventional tests and techniques with permission to determine realistic threats (Wilhelm, T., and Andress, J, 2011).

The general outset for a successful red teamer is to present a safe, but real world example of infiltration and data breaches, and identify what information is vulnerable. Then, evaluate the usefulness of that information to an adversary. Some typical strengths of successful red teams, but not other security professionals, are that they:

- Uncover low hanging fruit missed by regular procedures
- Uncover temporal risks
- Educate the defense team (Tripwire, 2010)
- Redefine how to discover of adversaries
- Review high impact targets for potential concerns
- Provide an unbiased opinion (which may conflict with management or audit viewpoints)
- Provide feedback and methods to mitigate risk

Red teamer analysis can also be described as an alternative approach to conventional security reviews. A paper published by the Central Intelligence Agency (CIA) about re-thinking threat analysis by using alternative approaches contains the following suggestions which are included in a red team mindset (CIA, 2004):

1. Continual – this brings a new mindset and ongoing analysis identifies new risks as well as re-evaluates the evolving threat.

2. Creative – thinking like your enemy and failing to resort to previous audit reports and threat matrices result in new approaches to remediation. Combining creativity and continual progress should inherently require the change of "Coverage" and types of attacks executed.
3. Collaborative – multiple people working on the same problem are able to bring different viewpoints and offer diversity to the team.
4. Counter-intuitive – known risks are being tackled by other groups. Red teams and personnel bring value by finding threats before others know they exist. Also, assets previously identified as low risk can be re-assessed by a red team.
5. Consumer-friendly – by design red teams are adversarial. As such, special care must be taken to ensure feedback is not just "airing out dirty laundry." A focus on reporting should be strongly oriented in value and facts when possible. Additionally, pointing fingers will hardly make a good impression of the process. Special care must be given to include all stakeholders so that no one's opinions are missed.

Red Teams Compared to Advanced Persistent Threat (APT)

There are many parallels between APT and red teams. APT advances on a "continuous area of attack," because, "by the time all the surfaces in a given technology are hardened, the technology is obsolete" (Holmlund, L., Mucisko, D., Lynch, R., Freyre, J., 2011). As previously discussed, technology is ubiquitous, constantly being implemented, and is often filled with flaws as soon as it is implemented. Information security must find a way to leverage the similarity of red teaming services and APT to prevent against this new threat.

How do you prevent APT? Most suggest a similar approach to red teaming exercises[2]. By using a red team it is possible to predict APT threats by analyzing threat intelligence. By gaining an understanding of the enemy it is possible to prevent, detect, or remove them.

Often, exploits used to execute an APT are not particularly advanced or complex. Instead, APT researches the target and chooses exploits appropriately. As suggested by multiple sources, APT executes similar to red teams in that they use the following phases: 1) planning and information gathering, 2) attack and compromise, 3) establish command and control, 4) authorization and credential theft, 5) manual exploitation and information gathering, 6) data exfiltration, 7) maintain presence. Each phase of an APT attack offers a red team test and response by the defense a chance to catch or remove the threat. While not exhaustive or indicative of a complete security program, consider the following prevention and detection capabilities which could be used at each phase to prevent, identify, or remove access:

1. Planning and Information Gathering - while no one method can prevent this activity, solid data classification policy, training, and security awareness may be able to assist employees on what information should not be released. This is true especially if the training focuses on real world attacks with a red team approach. Information about internal vulnerabilities is extremely useful knowledge for adversaries and is often disclosed publically. A company sending out a press release that they just signed a contract with company X to provide security is a huge advantage to an attacker. The APT/red team focus on research is on X products now. Even if a vulnerability does not exist now, it could in the future and information like this should be known by personnel and appropriately safeguarded when possible.

[2] Known shortcomings with red teams are that they are often hindered by time frame, have smaller scopes than APT, and must respect other restrictions placed on testing.

2. Attack and Compromise - traditional defense mechanisms may help prevent a successful attack. Testing responsiveness to attacks performed by a red teamer which appear as an adversary is an important element of detection and response. Since no patch system can prevent the unknown (or zero days), detection as soon as possible can provide clues into what allowed the access and how it can be removed and prevented in the future.

3. Establish Command and Control – a typical defense in depth strategy can detect anomalous data points. Also, while an intrusion detection system might be able to spot the traffic, red teaming can assist in testing and increasing detection capacities if necessary.

4. Authorization and Credential Theft – organizations prepare against this attack by restricting account access and regularly changing credentials. Red teamers test the assumption that unneeded accounts are removed by leveraging unchecked service accounts or privileged accounts given to high ranking officials. If access is logged and monitored, it may be possible to spot anomalous activity. If the defense team did not notice the credential use it may necessary to apply additional information security controls.

5. Manual Exploitation and Information Gathering – more information about an attack could be disclosed through logs or other monitoring techniques in line with defense in depth. Red teamers create realistic expectations of the footprint left in this stage. Logs indicating successful access are difficult to review appropriately and highlight the importance of identifying an issue before this phase of attack.

6. Data Exfiltration – performing monitoring on data access could help prevent excessive information harvesting. Red teamers test this stage of protection by executing data exfiltration techniques used by real world hackers. Successful red team exfiltration could show gratuitous information available copied to network shares. Without previously completing a data discovery project, it can be difficult to know exactly where sensitive information exists. Red teams help show how the information can be gathered and exploited. This can help drive projects which restrict access and remove unneeded information.

7. Maintain Presence – at this point, only advanced methods could detect the intruder unless another indicator becomes more visible, perhaps through another component of defense in depth. Red teams can often maintain presence for a long period of time without being spotted. However, with training and realistic expectations of how a red teamer could be stopped it is possible to increase the chance of detection and removal of a persistence presence.

Creating a Red Team Approach

The first step to create a red team should be to identify the goal of the red team. Considerations at this stage also include whether the organization will implement an enterprise red team or a focused effort. This decision will determine the level of effort required. Next, examine the resources available and compare it to the requirement at hand.

It may be leverage some current resources. Internal audit and security professionals are likely to already be employed in many organizations. Also, in many companies, there is a requirement for annual security training, penetration tests, risk assessments, or any combination thereof. Many of those resources are directly aligned with the development of internal red team processes or modification of current processes to become more effective and comprehensive.

Alternatively, red team services can be purchased exclusively from third parties. This approach can resolve some internal conflicts of interest (e.g. seniority, business department demands versus security department, and department authority) and can expand the testing capabilities of the organization while not focusing employee development of skillsets not core to the business.

Many firms offer security tests as isolated services. For example, most major consulting services offer penetration testing and social engineering and boutique firms provide valuable expertise on specialized attacks which is not available to the public. A good strategy to a third party approach would be to follow the alternative analysis and select a variety of services at different intervals while developing enough knowledge internally to identify shortcomings in the red teaming scope and maintain a historical view of the issues impacting the organization.

While many resources exist for specific technical components, it may be difficult to implement a holistic red team approach as described in this document. However, remember that red teamers are already in organizations. Everyday see vulnerabilities or issues that could harm the company if exploited. A hotel front desk manager knows if the server room is always propped open. This could allow a guest to sneak in and have access to systems with credit cards. An accountant notices when there is gratuitous access to funds that are being managed. These important insights could be obtained for free with little effort by applying the red team approach. Companies should consider augmenting yearly security training with examples of what vulnerabilities look like, the path to report it, and suggest that every employee document one idea annually to improve security. The results could be worthwhile, and while further research is needed to prove the effectiveness: the cost is minimal, empowers employees, and starts everyone on the path to become a red teamer to find problems and solutions every day.

The implementation of red teaming comes with challenges. Some of the important considerations when implementing red team services include:

- Operational impact – red teams can place additional burden on operational teams. Teams must be able to prepare for additional security requirements with communication, data backups, or resource scheduling.
- Legal implications – many of the types of red teaming tests are in emerging technologies where laws may not be fully understood. Also, there are many laws surrounding electronic communications and hacking. Before completing assessments it may be necessary to have legal review.
- Costs – the costs of implementing a red team will vary depending on current resources and the types of test being performed. If outsourcing some of the tests, it will require the business to receive vendor quotes either per engagement or hourly rates. This could lead to variable costs per year and must be budgeted accordingly.
- Deconfliction process – most red team services have the possibility to escalate in severity if not caught, recognized, and handled appropriately. It may be wise or necessary to notify key personnel / third party security service providers that communication will travel. It might also be necessary to create a "get out of jail free" card which has emergency off-hours phone numbers of higher ranking officers in the company who are aware of the test and can confirm that the tester has the authority to conduct the tests requested.

When executing red teaming services completely internally, there are some additional considerations. Not every consideration is required as this will depend on the services

implemented, however, some additional considerations when executing tests with internal personnel include:

- Social engineering – could pose problems for employees who must trick fellow employees and may not portray a real third party with no internal knowledge of procedures.
- Limited personnel / job descriptions – while a separate team could be formed to help meet other requirements (such as audit and penetration testing), this may not be a cost effective approach. Some organizations may have trouble asking employees to perform additional work that is not documented in a contract and not a core skillset required for the job.
- Limited experience – internal personnel may not have exposure to a variety of techniques, skills, reporting, and unbiased, broad experience in red team testing.
- Organizational reporting structure – the budget and reporting line may not have executive support and might not be able to touch on all business areas. Red teaming is often successful at transcending business lines to find low hanging fruit which might not belong to the group initiating red team services. Successful inter-division communication of these issues may be difficult to receive buy-in to fix.
- Impact – internal personnel sometimes are less effective at proving issues need to be remediated. Organizations may think risks are lower due to the inside knowledge of its employees and required information for the exploit to be successful. Outside firms show that internal knowledge gained from

employment may not be necessary and show a real outsider's thought process.

Considerations when executing red team services with a third party include:

- Costs – variable costs with red teams can range greatly and could be difficult to budget year to year.
- Lack of internal growth – executing solely with third parties does not grow internal team members to identify their own potential problems and solutions.
- Ease to eliminate / forget – third parties could be removed quickly from an organization with no continual process put into place to monitor changing risks.

Some companies may wish to start a red team by procuring a third party through a vendor selection process or request a proposal for an initial service to pilot the program. This helps drive the processes needed for executive support, coordination, scheduling, identifying resources, and choosing tests. Training could be considered as part of the requirements for the engagements to give employees an opportunity to grow.

The most important element in creating an effective red team is how results are handled. Reports are valuable tools, but if the proper support and reporting structure is not obtained, reports and recommendations may become "shelfware". Also, identifying common patterns of issues is a key sign that a root cause exists that needs attention. Root causes should be addressed systematically on a continual cycle with a core group of individuals overseeing the project. Red teams help uncover risks; sometimes the risks are indicative of fundamental elements missing

from an organization. By maintaining a core group of individuals and management support, the red team exercises can help resolve the larger gaps contributing to the vulnerabilities.

Categorization of Services

In this section, I propose an initial list to make life simpler for the creation, cataloging, and sharing of red team techniques and tools. Also, I provide a mechanism to document and communicate risk associated with executing the activities. It was developed by researching multiple red team testing engagements and created to accommodate many scenarios presented.

The services are so categorized in because the reporting structure, owners, and responsibilities of these sections are often clear to delineate in an organization. The three categories selected are electronic (remote), physical (close access), and social engineering. Each category by itself is not a suggestion for a comprehensive red teaming exercise. Most projects should consider two or three categories at a time to test the effectiveness of an attack. For example, by combining a social engineering email and an electronic (remote) backdoor system connection, the red team may be able to discover sensitive information and weak internal detection capabilities. The cause of the electronic attack was network based and may require additional patches or firewall rules. However, the social engineering attack was successful due to lack of personnel control and/or training and awareness.

Over time, I would like to see a list of services grow and mature to better facilitate the red team approach for comprehensiveness. The list is not intended to catalogue the complete list of threats or attack vectors, rather assist in successful communication of the framework for testing expectations and simplify the complex variety of engagements that can be assessed.

Electronic Services (Remote)

Electronic services exploit systems such as phones (Plain old telephone service (POTS), fax, web, wireless, or any electronic technology which allows remote access where a person typically is farther away from the device accessed than physical requirements. OSSTMM has broken wireless into a separate electronic category, which may be required due to the growing diversity in wireless services. However, wireless testing skillset is similar, the responsibility for the equipment often lies with the same group, and the remediation items often reflect configuration considerations not related to physical controls (Physical) or security awareness (Social Engineering).

Typical electronic services include:

- Penetration testing
- Web application security testing
- Hardware testing / software integration
- War dialing
- Open source research
- Open source electronic reconnaissance

Physical Services (Close-access)

Physical tests are an examination of facilities. While this could be an attack against an electronic facilities system, these tests specifically require local access to facilities to perform. Examples include warming a poster board and sliding it underneath a door to obtain access from a heat sensing motion detector. While this test tricks an electronic system, physical proximity and personnel risk are involved in the test. It requires an actual human to be local to the test being performed and may raise the risk of performing the test.

Tailgating is a physical concern due to the lack of mantrap, but is most often a social engineering test due to subverting awareness of personnel and not due to the lack of a man-trap. Circumvention of the mantrap would be a physical service if social engineering is not required to test. For example, dismantling the system by unplugging the power located on the outside of the trap would be a physical test, not a social engineering test. Lock picking is a traditional physical attack.

Types of Physical Services which can be executed are[3]:

- War driving
- Lock picking
- Alarm avoidance and access
- Rogue trusted insider
- External surveillance review
- External (facility) information gathering

Types of Physical Entry include:

- External to internal
- Internal to restricted
- Semi-trusted (conferences, public meetings) to internal
- Secondary dependency (cleaning, security, data hosting, etc.)
- External theft / attack
- Wireless review
- Dumpster diving (if physically protected)

[3] Many physical services are often conducted at the same time. However, in some cases an organization such as a bank may want to test a specific lock type or door.

Social Engineering

Social engineering differs from electronic attacks because it involves exploiting a person to make an attack successful. Social engineering can be combined with an electronic attack or occur in combination with a physical attack. Social engineering tests include tests directly initiated by the tester and executed by proxy. The most well-known example might be sending an email with a link to a compromised website. Leaving an infected thumb drive in an employee parking lot for an unsuspecting employee to pick up would be another example. Each of these examples does not require physical presence in a meaningful way. If badges are gates are used to allow access to the facility, then a physical test may also be required. In each of these examples, there is a combination of an electronic (remote) service which requires a person (Social Engineering) to execute. A pure social engineering example is calling an employee and asking for a password, then using the password in an online e-mail login attempt.

Examples of social engineering include:

- Social media
- Phishing
- Phone calls
- Physical networking and information gathering
- Local area intelligence gathering
- Tail gaiting
- Dumpster diving (if not physically protected)

The Risks of Assessing Risk

A concern with executing red team assessments is a lack of understanding and communication when it comes to the risk associated with executing certain tests. Although risk levels can be subjective, it seems to reason that a common method should exist for communicating risk from an internal perspective and an external perspective.

In order to create an initial guideline for corporations, I propose examples of adversarial tests be used for each category. These tests are then rated by the information security professionals from both sides on a scale of obtrusiveness and general hesitation to allow performance of the activity. I have suggested non-obtrusive items be ranked a 0 and highly obtrusive items be ranked 8-10 on a 10 point scale (Figure 1). Items marked "not suggested" are marked with a 10 due to the limited real world practicality and/or may not be ethical or legal. A letter, "R", can be used to ask for clarification. Answers can be discussed prior to engagements as a point of reference to discuss tolerance of testing levels and required coordination to proceed.

An example response (Table 1):

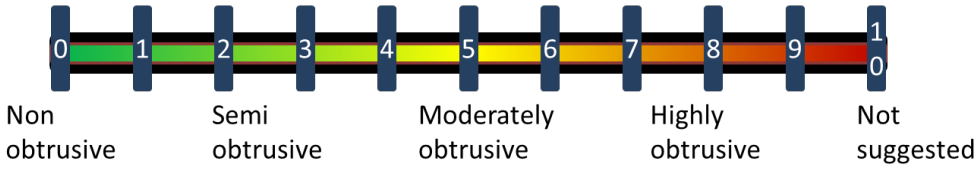

Figure 1

Answer	Question	Category
0	Open source intelligence – gathering information about a company, processes, subsidiaries, products, or business objectives from an available digital resource. Resources could include databases (with or without credentials), government sites, archiving sites, etc.	Digital
0	Company provided information is gathered by accessing publically available websites, search engines, etc.	Digital
0	External information is gathered by visiting third party databases, news sites, etc.	Digital
1	Aggregated open source information is determined which confirms	Digital

Answer	Question	Category
	sensitive information.	
3	Wireless device information is monitored from an entirely public place which is not conspicuous.	Digital
R	Slow automated and non-invasive or manual efforts	Digital
5	Guessing few/default passwords on web services	Digital
8	Attempting to brute browse website addresses manually	Digital
4	One-at-a-time phone dialing to detect services – no social engineering	Digital
7	Cross site scripting checks	Digital
7	Local attacks against client side code, mobile code, etc.	Digital
9	System exploitation and code execution (buffer overflow)	Digital
7	Efforts which are likely to alert an affected party if they are monitoring	Digital
8	Efforts which have a low to moderate chance of service crashing as an unintended byproduct of remote code execution or remote attack.	Digital
7	Web application scans with a commercial scanner	Digital
4	External network infrastructure application scanner	Digital
8	Brute force password guessing	Digital
9	Efforts likely to lead to denial of service or business continuity	Digital
7	Likely affecting sensitive or high priority electronic systems (e.g. commerce site)	Digital
10	Potentially causing harm or likely disrupting customers, clients, or other humans	Digital
9	Destruction of electronic information considered to have value (e.g. software license or production data). (ex. dropping a database table)	Digital
0	Surveying the landscape, reviewing the address to determine other building tenants, sometimes taking telescopic photos or reviewing satellite imagery.	Physical
8	Attempting to use the restroom in shared spaces, closely surveying the inside offices from a close distance, taking photos of offices from a close distance or external window.	Physical
8	Surveying personnel about their job when entering a shared space if in a place such as a mall or busy street, asking to use the restroom in an office, walking into the reception area to deliver cards, wirelessly surveying the premises.	Physical
5	Surveying personnel about their job when entering a shared space if in a place such as a mall or busy street.	Physical
5	Asking to use the restroom in an office.	Physical
5	Walking into the reception area to deliver cards.	Physical
6	Wirelessly surveying the premises.	Physical
9	Prearranging a meeting with a fake magazine company and interviewing executives, Tailgating into the facility and locating network jacks	Physical
10	Placing surveillance equipment on the premises, capturing digital cards' signal and replicating it for later use in an attack.	Physical
10	Using a method to walk in after hours: including, taping a door catch to	Physical

Answer	Question	Category
	prevent it from locking.	
10	Breaking a window.	Physical
10	Falsifying a job application to gain employment and inside access.	Physical
7	Dumpster diving in a public receptacle.	Physical
10	Faking medical illness to gain entry or escape.	Physical
0	Striking a conversation with an employee in a casual environment such as a nearby coffee shop or bar.	Social Engineering
3	Asking about personal items, vacations, or items not directly related to sensitive functions, but could be construed as suspicious.	Social Engineering
2	Phone calls asking for sensitive information such as usernames which might be reported.	Social Engineering
9	Directed phishing attempts with malicious payloads or requests such as resetting a password.	Social Engineering
8	Phone calls which ask a user to use a remote administration tool, or another technique that is capable of achieving sensitive information and/or could be disruptive or cause concern of possible alarm and suspicion.	Social Engineering
10	Tailgating to gain physical access *(*in most cases as a social engineering task, and not facilities review unless the use of mantraps is required.)*	Social Engineering
10	Social engineering friends and family	Social Engineering
10	Planting evidence of crimes	Social Engineering
10	Impersonating law enforcement	Social Engineering
10	Breaking into a home or apartment	Social Engineering
10	Using evidence of a true embarrassing circumstance to blackmail into compliance	Social Engineering

Table 1

Tabletops and Thought Exercises

This category of red teaming services is in contrast to the other services in that it is not a test at all and the only risk associated with this type of test is political where an exercise could result in a loss of capital and time with no noted benefit. Political risks can be avoided with modification to the methods to include all departments during the project initiation and include a round robin exercise where suggestion authors are not shared.

Example services include of this category include:

New Design Process Review – prior to implementing a new process there is a review by multiple parties to determine risks and identify possible modifications. Diagrams and technical follow-ups are incorporated into final official or unofficial recommendations.

Walkthroughs – a scheduled time where a manager or observing party walks through a current process to determine how the process could be or is manipulated. Ideally, the walkthrough would be completed by management from another department who would apply an adversarial mindset to the process and ask questions along the way. The walkthrough could be a hypothetical system compromise or a trusted insider turning rogue.

Red Teamer Training – a training event where employees are introduced to the idea of red teaming, tactics, and how to spot issues. After the training, a follow-up questionnaire could ask each employee to submit one potential risk they believe could be an issue and how the issue could be resolved.

"Visio" Penetration Testing – is performing a whiteboard review of a network or process to determine protection strategy, defense in depth, and spot weaknesses. This approach may assume that the hacker has "0 day" technology for one or more systems and/or has insider information about how the organization works.

Suggested Follow-up and Next Steps

Red teaming is a great approach to an important question in information security: what do we need to protect and how. However, the current information security market has been flooded by a "panacea" of penetration tests and audits. Changing actors and technology requires a revolution in adversarial testing and thought process. While penetration testers and audit tests are

getting better at their respective sciences, there is a wide range of risks which are never reviewed and consequently never managed. The law of diminishing returns could be applied to this cycle of performing traditional attacks and expecting to enhance security.

Because of the broad approach that red teaming can function, there needs to be communication about the types of tests that can be performed and what the risks are with performing the tests. More research and collaboration amongst organizations is needed to identify successful integration strategies and tactics of the alternative risk analysis. There is also a need to catalogue a list of services provided by the alternative risk providers. Finally, there is empirical evidence needed to identify the value in which adversarial tests are most effective and valuable.

If these tasks can be accomplished, I believe red teaming will be a great step towards true security. Security may become a forward looking process in technology and not something to deal with when security has time to catch up to the hackers. Security teams should get to know themselves as well as their hackers and red teaming is a great way to get to know each other.

References

Armitstead, L. (2011, July 29). *Big Four Accountancy Firms Furious at Prospect of Competition Probe.* Retrieved from http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/8671184/Big-Four-accountancy-firms-furious-at-prospect-of-competition-probe.html

Baker, Liana B., Finkle, J. (2011, April 26). *Sony Playstation Suffers Massive Data Breach.* Reuters. Retrieved from http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. (2009). *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1.* Cert. Retrieved from http://www.cert.org/archive/pdf/11tn013.pdf

Central Intelligence Agency (2004). *Rethinking "Alternative Analysis" to Address Transnational Threats.* Retrieved from https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm

Craig, Susan (2007). *Reflections from a Red Team Leader.* Military Review. March-April 2007. Retrieved from http://www.au.af.mil/au/awc/awcgate/milreview/craig.pdf

DCDC. (2010, February). *A Guide to Red Teaming.* Retrieved from http://www.mod.uk/NR/rdonlyres/B0558FA0-6AA7-4226-A24C-2B7F3CCA9A7B/0/RedTeamingGuiderevised12Feb10Webversion.pdf

Defense Science Board Task Force (2003, September). *The Role and Status of DoD Red Teaming Activities.* Retrieved from http://www.au.af.mil/au/awc/awcgate/dod/dsb-redteam.pdf

Deloitte. *Vulnerability Management Services.* Retrieved from http://www.deloitte.com/view/en_IE/ie/services/enterprise-risk-services/ers-service-offering/technology-assurance-and-advisory/vulnerability-management/index.htm

DHS. (2011, March 23). *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Retrieved from http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

Dzakovic, Bogdan (2003, May 22). *Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks Upon the United States.* Retrieved from http://www.9 - 11commission.gov/hearings/hearing2/witness_dzakovic.htm

Derene, Glenn (2008, June 30). *Inside NSA Red Team Secret Ops with Government's Top Hackers.* Retrieved from http://www.popularmechanics.com/technology/how-to/computer-security/4270420

Eisenhauer, Margarret, P. Esq., CIPP (2009, February, 23). *The Privacy Book Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risks*. Retrieved from

http://www.privacystudio.com/Links%20posted%20to%20web/Casebook%20Feb-23-09.pdf

Ernst and Young. *EY Services.* Retrieved from http://www.ey.com/GL/en/Services/Advisory/Advisory_Services?preview&selection=tab-it

Ernst and Young (2011, March). *Countering Cyber Attacks.* Retrieved from http://www.ey.com/Publication/vwLUAssets/Countering_cyber_attacks_March2011/$FILE/Countering_cyber_attacks_March2011_GL_Adv.pdf

Federal Trade Commission (2007, June 25). *Fair Information Practice Principles.* Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Gringer, S. (2001, December 18). *Social Engineering Fundamentals, Part I: Hacker Tactics.* Retrieved from http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Golandsky, Y. (2011, May 3). *Red Team Testing Methodology.* Retrieved from http://www.security-art.com/sites/default/files/Security%20Art%20Red%20Team%20Testing.pdf

National Institute of Standards and Technology. (2009). Fips Pub 199. Federal Information Processing Standards Publication. Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley Publishing, Inc.

Herzog, P. (2010, December 14). *OSSTMM 3 – The Open Source Security Testing Methodology Manual.* Retrieved from http://www.isecom.org/mirror/OSSTMM.3.pdf

Holmlund, L., Mucisko, D., Lynch, R., Freyre, J. (2011). *Cybersecurity Watch: Organizations Need More Skilled Cyber Professionals to Stay Secure.*

Huerer, Richards J. (1999). *Psychology of Intelligence Analysis.* Retrieved from http://permanent.access.gpo.gov/lps20028/www.cia.gov/csi/books/PsychofIntelNew.pdf

KPMG. *Risk Advisory Services.* Retrieved from http://www.kpmg.com/HU/en/WhatWeDo/Advisory/RiskAndCompliance/Risk-and-Compliance-IT-Advisory-Services/Pages/default.aspx

Lauder, Matthew (2009). *Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces.* Retrieved from http://www.army.forces.gc.ca/caj/documents/vol_12/iss_2/CAJ_Vol12.2_07_e.pdf

Mateski, Mark Dr. (2009, June). *Red Teaming: A short introduction (1.0).* Retrieved from http://redteamjournal.com/papers/A%20Short%20Introduction%20to%20Red%20Teaming%20%281dot0%29.pdf

McClure, S., Scamcray, J., Kurtz, G. (2009). *Hacking* Exposed 6. McGraw Hill Professional.

Meehan, Michael K., (2007). *Red Teaming for Law Enforcement.* Retrieved from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=1111&issue_id=22007

Mitnick, Kevin D., Simon, William L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, Ind. Wiley. Retrieved from Eastern Michigan Online Library

Peake, Chris (2003, July 16). *Red Teaming: The Art of Ethical Hacking.* Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/red-teaming-art-ethical-hacking_1272

PWC. *Security Consulting Services.* Retrieved from http://www.pwc.com/us/en/it-risk-security

Savitz, Eric. (January 1, 2012). *Forbes. The $100 Billion Problem No One Is Talking About.* Retrieved from http://www.forbes.com/sites/ciocentral/2012/01/02/the-100-billion-problem-no-one-is-talking-about/

Scarfone, K., Souppaya, M., Cody, A., Oregbaugh, A. (2008, September). *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Skroch, Michael J. (2009, November 2). *Model and Simulation of Red Teaming.* Retrieved from http://redteamjournal.com/wp-content/uploads/2009/12/msrt0.3-2nov2009-sand2009-7215J.pdf

Smith, Gerry (2011, July 27). *Anonymous, LulzSec Call for Mass Boycott of Paypal.* Retrieved from http://www.huffingtonpost.com/2011/07/27/anonymous-paypal-boycott_n_910745.html

Sophos (2011). *Security Threat Report: Mid-Year 2011.* White paper internally distributed.

Sinai, Joshua Dr. (2003, February 12). *Red Teaming the Terrorist Threat to Preempt the New Waves of Catastrophic Terrorism.* 14th Annual NDIA SO/LIC Symposium & Exhibition. Retrieved from http://www.au.af.mil/au/awc/awcgate/documents/sinai.pdf

Stoneburner, G., Goguen, A., Feringa, A. (July, 2002). *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Storm, D. (2011). *Black Hat: Lethal Hack and wireless attack on insulin pumps to kill people.* Retrieved from http://blogs.computerworld.com/18744/black_hat_lethal_hack_and_wireless_attack_on_insulin_pumps_to_kill_people

Stuttard, D., Pinto, M. (2008). *The Web Application Hacker's Handbook.* Wiley Publishing. Indianapolis.

Tripwire (2010, October 14). *Mind the Gap.* Whitepaper retrieved from email correspondence from SC Magazine.

U.S. Department of Health & Human Services. *Health Information Privacy: The Security Rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

U.S. Department of Health & Human Services. *(*2003*,* February 20*). 45 CFR Parts 160,162, and 164 Health Information Reform: Security Standards: Final Rule.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Wilhelm, T., Andress, J. (2011). *Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques. Elsevier*. Burlington, MA.

Verizon. (2011). *2011 Data Breach Investigations Report.* Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf