CHAPTER 6

Strategic Cybersecurity

Strategic cybersecurity is accomplished through orienting every facet of cybersecurity efforts, expenditures, technologies, and personnel toward the immediate and long-term strategic goals and outcomes of the organization they protect. Imagine you were the Chief Information Security Officer (CISO) or otherwise in control of the cybersecurity apparatus of an organization. Let's say this organization is a sneaker company. You get called into the CEO's office and she is sitting there with the entire board and ownership of the sneaker company. She looks you in the eye and she tells you this:

> Your budget for the next year will be five million dollars. I want you to spend it on cybersecurity things that will enable me to sell the most sneakers possible. I do not care if we get hacked, how bad we get hacked, or even who or what in the company gets hacked. I just want to profit as much from sneaker sales as possible year over year and continue operation for as long as possible and those are the only measure that I will evaluate you on moving forward.

J. G. Oakley et al., *Theoretical Cybersecurity*, https://doi.org/10.1007/978-1-4842-8300-4_6

OK wow, that would be quite the statement from organizational leadership, but what if it happened? What would that look like? What would you do with that challenge? The answer, in whatever form you give it, would be strategic cybersecurity. This is because in response to such a challenge, any solution given would be aimed at improving the strategic outcome of the sneaker company, profit as much as possible from sneaker sales and operate for as long as possible.

There are a lot of ways to approach this challenge from a cybersecurity perspective and a lot of novel ways to implement cybersecurity solutions. Maybe, as the CISO, you decide to focus on profit by minimizing downtime. Maybe we focus on longevity by protecting the trade secrets of our shoe company. The thing is, if, as an industry, we can be successful at strategic cybersecurity, we will not only improve the totality of our body of work, but we will also improve external support for our efforts and appear as an enabler and not as a tax or cost that an organization or its operational units must pay.

As we have just discussed, the areas and aspects of an organizational attack surface we choose to focus on are as numerous as the threats faced. Since they are largely tailored to the specific organization, I will not waste time trying to exhaustively compile a list of cybersecurity problems to tackle that are directly tied to strategic cybersecurity. Instead, we will walk through several cybersecurity implementations that are strategic in nature, regardless of what type of organization they are applied to simply because of their methodologies and implementations.

What It Is Not

Since the term cybersecurity strategy is a well-known and possibly overused one, I just wanted to take a moment to point out that it is vastly different than strategic cybersecurity. Cybersecurity strategy is a near and long-term plan to achieve cybersecurity outcomes and goals, which do not necessarily align directly with an organization’s own strategic mission.

A Move Toward Resiliency

Our sneaker company example certainly plants the seeds of theoretical cybersecurity exploration. We can easily see that there are many ways we could change the way we look at cybersecurity as an industry and a body of work if we had this kind of organizational support. My stance is that we are currently at the infancy of this sort of process, and it will require a lot of evolution in thinking and is probably generational in forming. We need to change a lot of bias about threats, cybersecurity, and how we view being networked and on the Internet in general for statements anywhere near like our fictitious CEO said to be commonplace.

Still, I think there has been a subconscious shift to address the lack of strategic cybersecurity in the vast growth in cybersecurity resiliency technologies, businesses, approaches, and efforts. As a society and industry, we are beginning to realize the basic truth that if someone really wants to hack you, they eventually will and that there are too many threats with too much variance to completely mitigate for any organization. Therefore, the natural response is to not focus less on stopping every attack but more on coping with as much damage as possible. This lets you be threat agnostic and focus more on things an organization does know in the things it can't live without, how long it can survive in various circumstances, etc.

Resilience in this sense and efforts and technologies to improve it are certainly strategic in nature since they are based on knowledge about the organizations ability to operate and not so much on what threats exist. In my mind this shift is extremely valuable to our industry and to our customers as it leaves less room for showmanship, lying, and bamboozling through scare tactics so common at conferences, tradeshows, and websites of cybersecurity vendors. Instead of trying to scare a customer into buying protection from APTs who are probably never going to bother targeting them in the first place, let's start helping our customers weather as many storms and as fierce of storms as we can and not sell hurricane insurance to companies in Switzerland and stop marketing avalanche prevention services to companies in Australia.

On Cybersecurity Insurance

Since I have spent much of this book atop my tower of soap boxes, I think we can throw one more on the pile. It feels it is important to point out the problem that cybersecurity insurance poses. It may seem like a natural fit for strategic cybersecurity and an improvement to resilience. And why not? Insurance lets an organization simply buy down risk with predictable dollars by shifting less predictable risk and expenditures it to an insurer. So, what's the problem?

It turns out there are a few. Firstly, any time you mix both technical jargon and legal jargon, the opportunity for misunderstanding, misinterpreting, or misrepresentation is extremely high. If you are an organization that doesn't feel strongly enough about your cybersecurity competencies that you want to just buy down risk through insurance instead of fixing it though technology, policy, and people, do you really think you would be able to articulate the technical arguments necessary when the insuring organization says you didn't live up to the requirements necessary to maintain coverage for a given hack?

That and other problems with cybersecurity insurance to the customer aside, there is also the issue of the attackers. In normal insurance, there is certainly insurance fraud and there is also a long history of enforcement and protections put in place. When you try to insure against cybersecurity attacks, and specifically ransomware and ransoms though, aren't we in a way encouraging the attackers as well as informing them on the right amount of ransom to request to result in payout most likely? This line of questioning has been explored by others in our profession more experienced and widely known than myself, and all of it so far has been interesting reading. I just wanted to touch on it in this chapter since I think it is a natural progression of thought along the lines of strategic cybersecurity and its manifestation in general terms through a shift toward resiliency.

Counter-APT Red Teaming

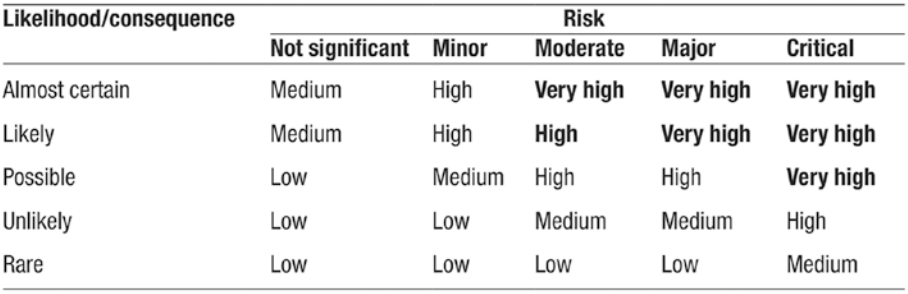
Counter-APT Red Teaming or CAPTR Teaming is a strategic offensive cybersecurity paradigm that leverages outcome-oriented scoping, criticality-supported initialization perspectives and reverse red teaming methodologies to strategically implement pro-active, offensive cybersecurity assessment. This theoretical cybersecurity idea was one I proposed, experimented on, and validated for my doctoral dissertation and is covered ad nauseum in that document and to a detailed degree on the book *Professional Red Teaming* as well. The following is enough of an introduction to the concept to illustrate an example of how strategic cybersecurity can show up in the offensive cybersecurity sector of our industry. The following chapter will have more defensive oriented example material on how strategic cybersecurity might be incorporated on the blue side of things in support of an organization's strategic goals and outcomes.

Outcome-Oriented Scoping

The identification of scope by the CAPTR team is a multi-part process focused on identifying those items that pose lethal or critical impact if compromised. The scope in a CAPTR team assessment is intended to allow assessment resources to home in on a limited and prioritized subset of the overall organization. Scoping the assessment this way is necessary if the selected initial assessment assets are to enable the CAPTR team engagement to be successful. The scope of a CAPTR team engagement is more outcome-oriented than in a traditional red team assessment as productivity and cost benefit are directly tied to appropriate identification of critical or lethal compromise items that meet the threshold for inclusion. This is done by using appropriate personnel to perform worst-case scenario risk assessment, centrality analysis, and adequate prioritization of potential targets.

Worst-Case Risk Assessment

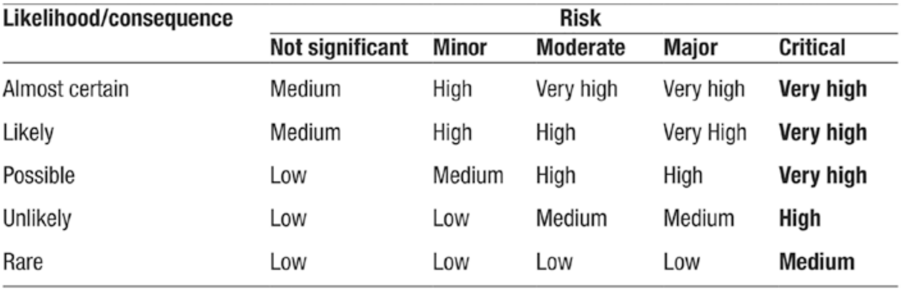
Traditionally, in risk management and asset prioritization, the leadership of an organization will use a standard risk matrix to determine which items present the highest risk (the bolded regions in Figure 6-1) and to address those first.



Likelihood/consequence	**Risk**				
	Not significant	**Minor**	**Moderate**	**Major**	**Critical**
Almost certain	Medium	High	**Very high**	**Very high**	**Very high**
Likely	Medium	High	**High**	**Very high**	**Very high**
Possible	Low	Medium	High	High	**Very high**
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Low	Medium

Figure 6-1. *Red Team Risk Focus*

The CAPTR team helps the organization leadership understand that the likelihood does not matter for critical or lethal items and to assume compromise is possible and probable. This is done to afford the greatest mitigation of advanced threat actor activity. If an APT is intent on targeting such items within the organization, it is only a matter of time until these items will be at risk. This should move risk prioritization toward addressing those items that fall in the critical column of a typical risk matrix such as in Figure 6-2 (bolded regions), as the worst case is assumed and the likelihood of attempted and eventually successful compromise by an APT is accepted to be almost certain.



Likelihood/consequence	Risk				
	Not significant	Minor	Moderate	Major	Critical
Almost certain	Medium	High	Very high	Very high	**Very high**
Likely	Medium	High	High	Very High	**Very high**
Possible	Low	Medium	High	High	**Very high**
Unlikely	Low	Low	Medium	Medium	**High**
Rare	Low	Low	Low	Low	**Medium**

Figure 6-2. *CAPTR Team Risk Focus*

Survivability

Essentially, the question being asked in CAPTR team scoping is, what losses can this organization not afford to sustain. Determining the correct answer to that question involves all facets of the customer organization as well as the offensive security expertise maintained by assessors. Much like in traditional red teaming, the operational as well as security or infrastructure-oriented staff are needed to appropriately identify the scope. One immediately identifiable difference is the inclusion of the offensive security professionals in developing the needed scope. As we discussed earlier, typically, the scope is defined by the customer before the assessment and it acts as more of a constraint than an enabling attribute of the engagement. There is also a specific order to the involvement of personnel as well since the shaping of a CAPTR scope is an evolving process that ends with asset prioritization and a risk apogee.

CAPTR Team Critical Initialization Perspective

As outlined, the CAPTR team's use of critical perspective starts at a point or points of presence that are identified as posing the greatest risk to the organization. The focus of an assessment from this perspective is to identify vulnerabilities local to such devices that would enable an attacker to compromise the critical item. The assessment can then be expanded to the points in the organization that would allow an attacker to pivot to the critical items and continues outward. This fourth perspective is aimed at mitigating the impact of a breach regardless of its source. No matter the vulnerability that allowed an attacker in or the locality of an insider threat should affect this assessment perspective. Beginning security assessments at the goal of a compromise instead of assessing the potential starting points provides an enhanced ability to mitigate a myriad of threats. This perspective differs from the internal initialization perspective in that it starts at the CAPTR team scope-identified points of lethal or critical compromise, not simply an unspecific privileged or unprivileged access within the organization. This critical initialization perspective is illustrated in Figure 6-3.

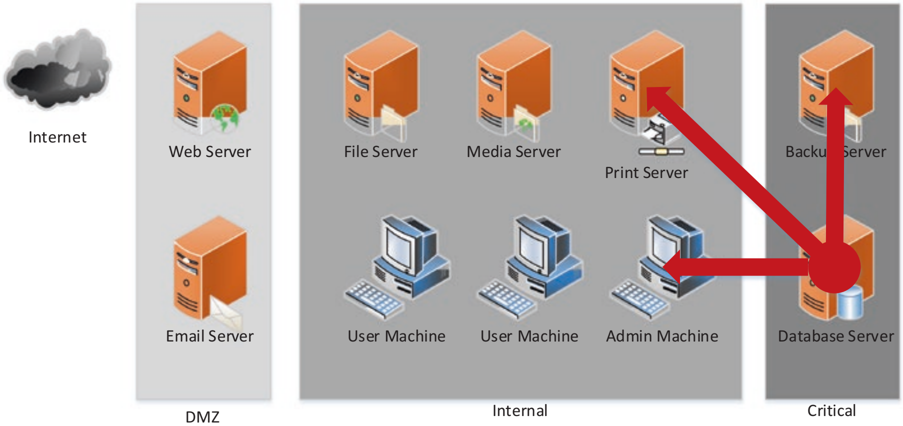


***Figure 6-3.** Critical Initialization Perspective*

This differs from traditional attacks that are more likely to begin from external perspectives or internal unprivileged perspectives resulting from attacks like spear phishing which are shown in Figures 6-4 and 6-5, respectively.

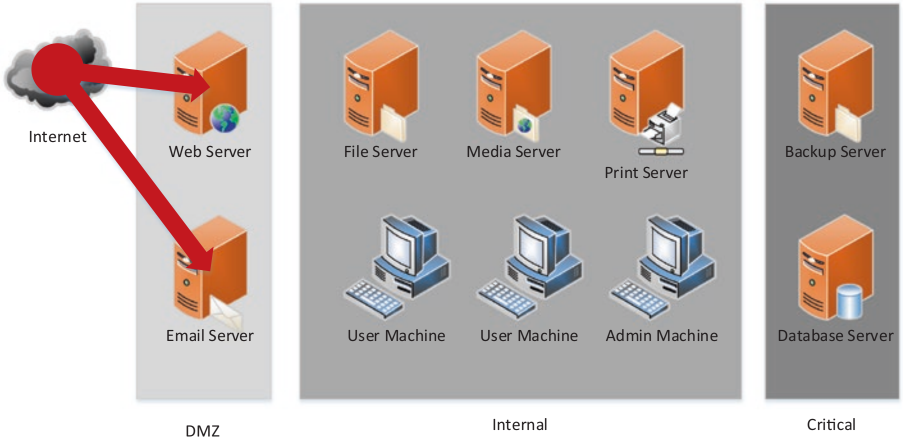


Figure 6-4. External Initialization Perspective

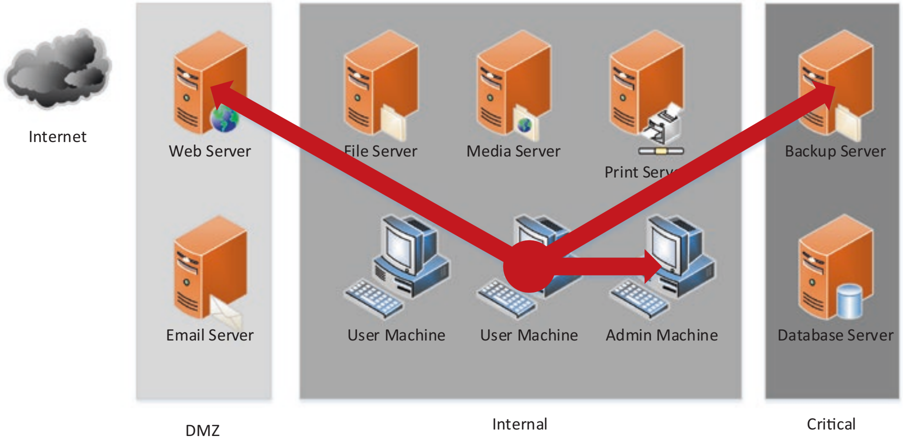


Figure 6-5. Internal Initialization Perspective

Reverse Red Teaming

With the targets selected via the CAPTR teaming-specific scoping methodology and the most appropriate launch point established using the critical perspective, execution of the assessment can begin. Reverse pivot chaining is a unique way of assessing from the critical perspective that creates a reporting mechanism utilizing reverse risk relationships to provide extremely high-cost benefit to such engagements. The process of reverse pivot chaining will be established in this chapter as will the benefits and presentation of the results it can yield.

Reverse Pivot Chaining

Reverse pivot chaining is the process of leveraging local, passively gathered intelligence from initially scoped items to define the access vectors likely to be utilized by attackers and to appropriately expand the CAPTR team scope toward improving efficiency of higher risk exploitation and access pathways. Reverse pivot chaining focuses on identifiable communicants that surround a given machine instead of the entirety of the encompassing network. This methodology sacrifices quantity of targets assessed for precision target selection and evaluation.

Local Assessment

Local assessment of the scoped critical objects is done using elevated privilege under the assumption that an APT could eventually achieve such context during a compromise. Local privilege escalation vulnerabilities and local misconfigurations that would allow an attacker to ultimately affect the confidentiality, integrity, or availability of the compromise object are assessed at the very onset of the CAPTR team engagement window. Further, this local context is used to identify potential remote access vectors such as code execution exploits or poor authentication configurations. With access to locally stored data and operating system functions, the CAPTR team assessor can efficiently identify access vectors an attacker would use against the initially scoped items without having to perform potentially risky blind scanning and exploitation.

The best way to underscore the benefits of this method are through a simple example using the following network. CAPTR teaming's outcome-oriented scoping defined the Linux file server constitutes a lethal compromise to the organization, and assessment will be carried out using the critical initialization perspective of starting with access to the server as shown in Figure 6-6.

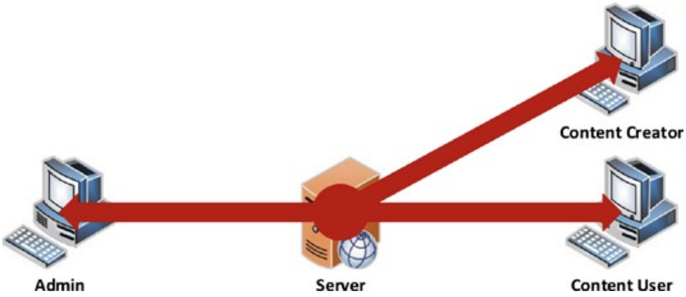


Figure 6-6. *CAPTR Team Assessment Directionality*

After running several situation awareness commands, much like those covered in the operational best practices chapter, the assessors have use of locally available, native operating system commands to determine much about the machine deemed as a lethal compromise object in the organization.

The assessor has learned that the kernel version used by the Linux server is out of date and vulnerable to a local privilege escalation vulnerability. the ability to transition from an unprivileged user to a super user on such a critical machine in the organization constitutes an extremely dangerous risk. This risk is also one that would have gone undiscovered in other assessment models had they not completely and successfully compromised devices in the network leading to and including this machine, which could potentially reside deep within a target organization. CAPTR teaming immediately assessed the lethal compromise item and, within the first few moments of establishing situational awareness, found a critical reportable item without even proceeding to outward exploitation and expansion of the assessment.

Initial situational awareness commands also informed the assessor that there were three machines communicating with the lethal compromise item. There was one computer, presumably an administrator, which was found to be using SSH to remotely access and administer the box. This information was found on the filesystem itself. Logs and files related to the SSH protocol were found in the user's directory on the machine, and the user's activity in the command history of the device showed activity typical of an administrator. Without the local privileged perspective used in CAPTR teaming, this information may have never been discovered, and if it had, it meant that typical red team assessment had remotely exploited several devices as well as having run a potentially dangerous kernel-level privilege escalation exploit to get privileges to view the same information that the CAPTR methodology began with.

The established connections to the machine that the assessors identified through native operating system commands indicated the presence of the other two communicants. One was accessing a read-only web file share on port 80 that the Linux server was hosting and the other was accessing a file transfer server on port 21. Further inspection led the assessors to identify that the file transfer server was used to put files on to the Linux server for other users to view and download. Through further local intelligence gathering, the assessors also found that the file transfer ability was not limited to a specific location such as the web file share directory and that a remote file transfer could overwrite several unprotected scripts that were being executed with superuser privileges by the machines scheduling mechanism.

No exploitation has been performed, and we already have the following extremely valuable findings to report upon within less than a day of assessment:

- Local privilege escalation using kernel exploit
- Remote code execution as superuser due to:
    - Poorly configured permissions of world writeable scheduled jobs being executed as superuser
    - Unconstrained file transfer server.

Analysis of Local Intelligence

The assessment has also identified the three tier one communicants of the lethal compromise item. With these targets identified, the CAPTR team must perform analysis to identify which order to conduct assessment of these hosts. This prioritization is also valuable to the reporting that will come later in identifying which links are most dangerous. These risk links are constituted by the source, the destination, and the method and privilege of communication. It is possible to have multiple links between devices. For example, if the admin machine could access the lethal compromise by either SSH as an admin user or file transfer as an unprivileged user it would mean that an attacker needs less privilege gained on that tier one communicant to then attack the lethal compromise object. As we continue on this example, I am only providing some simple decision points for prioritization and assessment. Each actual scenario will impose its own unique attributes to any offensive security assessment and the decisions of the assessors may drive the engagement differently. This scenario should clarify the process and not be taken as guidance on how exactly to make risk-based decisions, as all risks and every organization vary.

The risk links identified via local assessment of our scoped lethal compromise item are shown in Figure 6-7 and listed as follows:

- Superuser on 10.0.0.2 can access 10.0.0.1 as superuser using the SSH protocol
- Unprivileged user on 10.0.0.3 can access 10.0.0.1 as an unprivileged user using FTP
- Unprivileged user on 10.0.0.4 can access 10.0.0.1 as an unprivileged user using HTTP

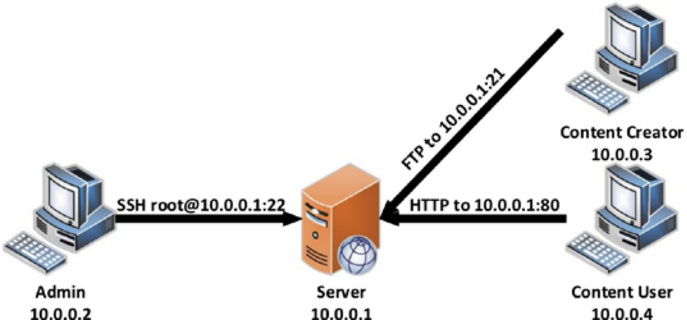


Figure 6-7. *Communication Links*

The first risk link constitutes the most risk to the lethal compromise item as it provides immediate interactive access as a superuser to the lethal compromise item. Any attacker able to compromise that tier one communicant poses grave danger to the Linux server. The FTP link is ranked second as it provides unprivileged access; however, it also allows for files to be moved to the lethal compromise server, and given what we know about the identified local privilege escalation vulnerabilities that are present, it is a potential, yet more complicated path to remote interaction. The HTTP link is last because it is a read only ability for unprivileged users to download data from the privileged host and would require leveraging of an additional risk link to pose much danger to the lethal compromise item.

Reverse Pivoting

At this point, the assessors have established a prioritized list of targets which will be rolled into the scope of the CAPTR assessment. These targets will be assessed remotely for potential access vectors and vulnerabilities using well-known or custom scanning and exploitation tools. Any successfully compromised tier one communicant will then be subject to the same local intelligence gathering that was performed on the lethal compromise item, but with one difference. In addition to identifying information related to remote communicants that may access the device, it is also analyzed as its ability to be a spreader. In this sense, both outside in, and inside out communication pathways become valuable to the CAPTR team assessors.

We have initially identified the admin machine as the highest risk link to the lethal compromise item, but what if, upon reverse pivoting, it is identified that the machine used for content creation, which FTPs to the lethal compromise server is accessible by ten other machines and it has a remote code vulnerability of its own. Further, it is administered using the same account and source machine as the lethal compromise site. As such, any successful access and privilege escalation on the content creation box would lead an attacker to gain the superuser credentials due to the key being stored for convenience on the device. The other two tier one communicants were not found to have remote access vulnerabilities so certainly the content creation machine should now be considered the highest risk within the organization.

The chaining together of this iterative reverse pivot process allows the assessor's to surgically establish a web of risk relationships and identify attributes of those communicants that may prioritize them as attack vectors. It is also important to remember that CAPTR teaming is another tool in the chest for offensive security practitioners. It does not assess the whole network a lethal compromise item resides in, but it is a focus on likely communication paths. Also, it is important to remember that many advanced attackers are likely to do their best to blend in with and leverage established communication methods to achieve compromise. The extremely efficient focus on those items specifically lends credibility to this CAPTR process even though its methodology is a reversal of traditional red team and attacker directionality.

CAPTR Reporting

Using the previous example as an analogy for actual targets which may be much larger, it should be readily apparent that the reverse pivot chaining process will result in a web of risk links between hosts that converge on the lethal compromise item(s) established by the outcome-oriented scoping. One of the benefits of this methodology is the safety that can be maintained by the assessing party. In fact, a CAPTR team assessment need not exploit a single vulnerability to be extremely effective. In a high-risk environment where traditionally red team activity is frowned upon due to the risk it introduces, CAPTR teaming can be a great alternative. Instead of attempting remote exploitation of tier one communicants, the assessors could simply use administrative access provided by the host organization to perform the local intelligence gathering on each tier one communicant to identify their capability as a spreader and which devices further out in the network act as tier two communicants. Though this method lacks the proof of concept of actual exploitation, it can be efficiently and safely be performed by assessors with the attacker mindset and skill set to the benefit of the host organization.

Web of Reverse Risk Relationships

Accumulation of the risk link data throughout the engagement allows for a logical representation of the web of risk relationships in the organization that lead back to the initially scoped items. In earlier chapters, we discussed that the CAPTR scope may consist of several devices. The same logic is applicable and local assessment can be performed on them in a prioritized order, the tier one communicants are just made up of the total list of hosts that communicate to any or one of the initially scoped items. Here specifically, the ability to be a spreader is important as any tier one communicant, or even initially scoped item for that matter, that communicates with multiple lethal or critical compromise items in the initial scope becomes an elevated risk. Though logical in nature, the web or reverse risk relationships can easily be turned into a graphical representation of organizational risk capable of communicating to even non-technical managers where the focus of the organization security apparatus should be. As the web becomes bigger, it also allows an organization a unique view at cumulative risk cardinality. The identified risk of a given machine or a reverse link to the lethal compromise item and thus the greater organization is continually evolved through the engagement as tiers of communicants are assessed and the aggregation of links to significant spreaders and higher risk items becomes apparent.

Math Is Hard

I will touch on this because I think an organization deciding to undergo CAPTR team assessment could also tailor the results to be extremely useful in a quantitative analysis of risk relating to the initially scoped items. I am no math whiz, but a definition of weight for the risk posed by having a given amount of communication links, vulnerabilities, and capability as a spreader could certainly lead to mathematical analysis and representation of the web of reverse risk relationships and the cumulative risk cardinality of machines. The reason I did not provide what I think this would look like is because it should be different for every organization. When possible, though, taking the CAPTR process and applying metrics to quantitatively establish risk using the results could be invaluable to addressing organization risk that comes from critical or lethal compromise items.

A Discussion on CAPTR Reporting Cost Benefit

Identifying potential vulnerabilities that are present to the lethal threats within an organization by leveraging less resources in an expedited assessment window is the apex of the CAPTR team concept. Prioritization of initially scoped compromise items and then the efficient assessment of those items and their communicants using the CAPTR team method represents a widely applicable cost benefit over traditional assessment methods. The reporting mechanism enabled by the relational risk data the CAPTR assessment gathers regarding initially scoped items and paths of potential access to them enables security and monitoring teams. Further, non-technical management is empowered to make cost-effective, security-related budget decisions utilizing the risk link web. As an example, candidates of CAPTR team assessment, take the organizational diagram in Figure 6-8.

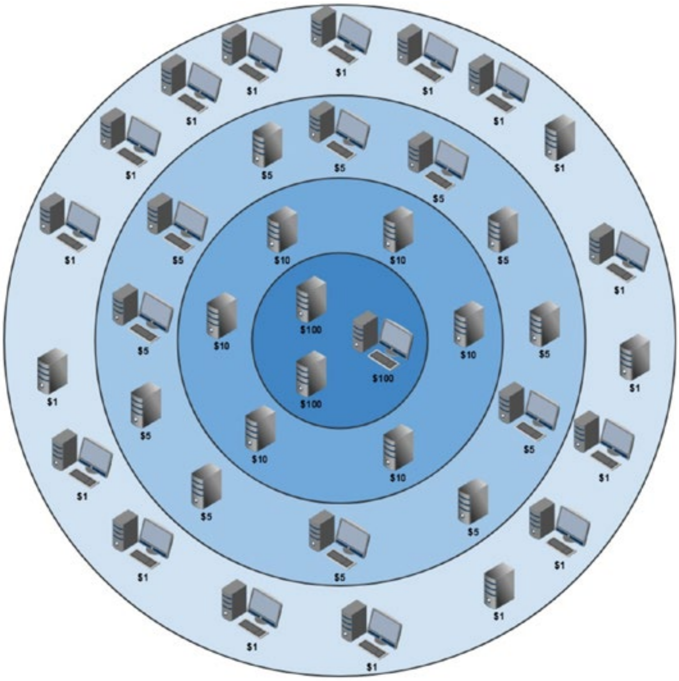


Figure 6-8. *Organization Object Risk Values*

This is a diagram of organizational resources separated into bands based on their cost to the organization if compromised. This is a simplified depiction and the US dollar is simply representative currency of the risk value the objects have to the organization. There are three objects with a risk value of $100, six with a risk value of $10, 12 with a risk value of $5, and 18 with a risk value of $1. The total risk value for all the objects in the organization is $438.

Figure 6-9 shows overlays of the previous diagram showing the likely outcome of scoping for both a CAPTR team engagement and a traditional offensive security engagement such as red teaming or penetration testing.

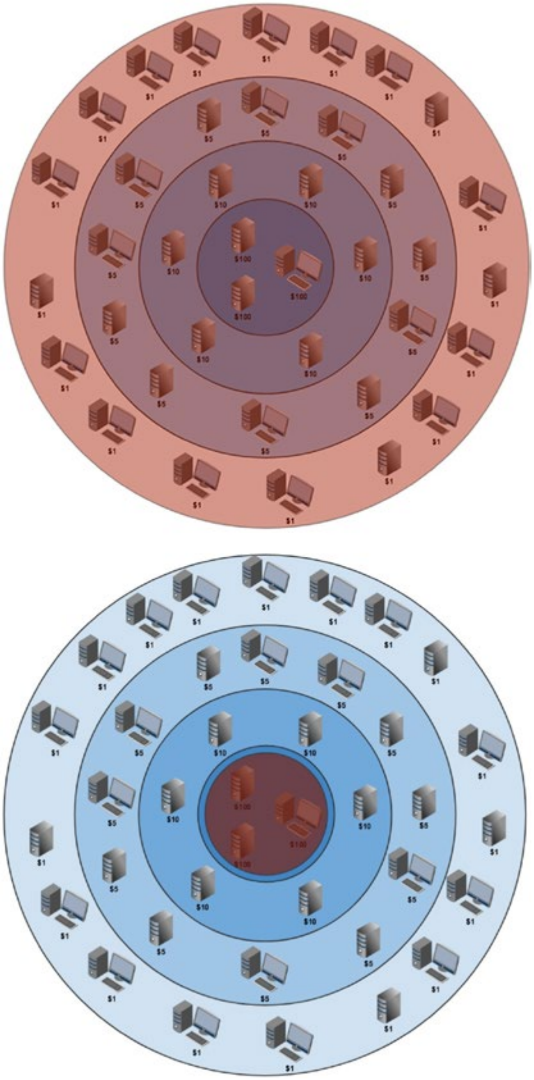


Figure 6-9. *Traditional Offensive Security Scope and CAPTR Team Initial Scope*

On the left is a representation of typical scoping for a traditional offensive security engagement. Since the aim of such engagements is to simulate an attack on an organization in an effort to uncover any weaknesses (Choo et al., 2007), the entire organization is subject to assessment and therefore included in the scope if possible. The CAPTR team scope is limited to items of critical importance which, in this case, are the three objects in the organization with risk values of $100. Although high value items are included in both scopes, it can be certain in the CAPTR team assessment that they will be assessed. In the traditionally scoped engagement, the likelihood that every item is assessed is highly dependent on the assessors' skill and the window of time allotted to the assessors. Next consider the following representations of example findings from both types of engagements.

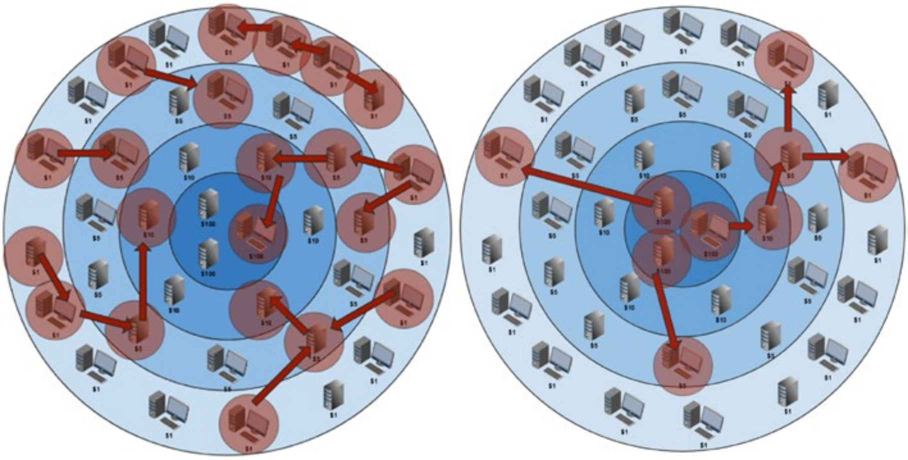


Figure 6-10. *Traditional and CAPTR Team Example Findings*

On the left are example findings resulting from the scope used by traditional offensive security assessments and on the right are the findings resultant from the CAPTR team assessment. The red circles over objects represent their compromise during engagements and the red arrows depict a pivot to another device via information found on the previously assessed host. In an effort to assess weaknesses in the entire organization, the traditional assessment method did compromise one of the high value targets as well as many others. This shows the potential for a traditional assessment to compromise and progress to many hosts within the organization, but perhaps not to all of those identified as being particularly high in value to the organization. Conversely, the scope of the CAPTR team assessment allows for those high value systems to be assessed from an elevated privilege at the onset. This initial scope also leads to the identification of communicating hosts that pose potential access vectors an attacker could take to attack the high value items. Those are then assessed and compromise if possible and the process then continues for the duration of the assessment window. This method potentially compromises fewer hosts than traditional models; however, the value of compromised assets is likely much higher. Also, by identifying communication relationships between lower value objects and high value objects, the CAPTR team model can identify which low value hosts actually pose a high value risk to the organization due to their risk relationship with the critical items in the overall web of compromise carried out by the team.

In Figure 6-10, the traditional offensive security assessment of typical scope resulted in a compromise of 21 objects in the organization with a sum total of $171 in risk value associated with them. The CAPTR team assessment of its initial scope resulted in compromise of nine objects in the organization with a sum total of $323 in associated risk value. These are just examples but illustrate potential outcomes of processes using traditional and CAPTR Team offensive security methods. In similarly timed engagement windows, CAPTR teaming would realistically lead to the assessment and compromise of at least those most valuable items included in its initial scope totaling $300 in risk value. To identify findings with this level of impact, the traditional offensive security assessment would have to go on long enough to engage at least two of the three high value items as well as all others within the organization.

To understand the benefit the CAPTR team process provides in translatable recommendations to host organizations, again consider the CAPTR team example findings in Figure 6-11 shown larger as follows:

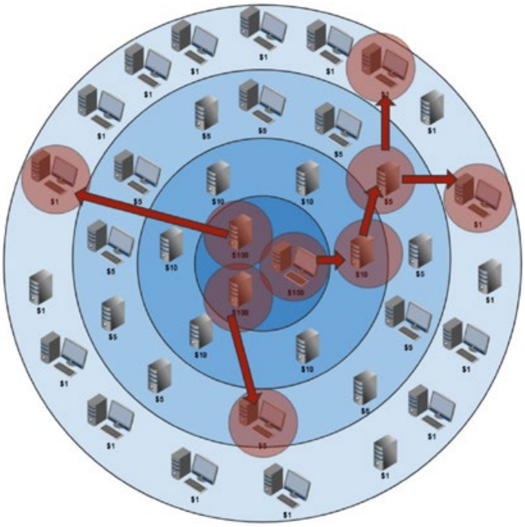


Figure 6-11. *CAPTR Team Example Findings*

The findings in Figure 6-11 will be discovered in an order that reflects their distance from those initially scoped critical items and their different communicants. Findings on the high value items are of grave concern to the organization and should be addressed quickly. The next tier of hosts comprises those that directly communicate with the initially scoped items. In this diagram, for example, an object with a risk value of $1 is found to directly communicate with a high value item from the initial scope. The risk web provided by mapping communicating hosts and their tiered relationship to the critical items allows even non-technical managers to easily understand the value of fixing the identified $1 object. At face value, a vulnerability in a $1 value object may be simply accepted instead of mitigated as part of the risk analysis based on offensive security findings. This is due to the fact that the organization might not view spending $10 to fix a problem on a $1 machine a worthwhile investment of resources. The CAPTR team model, however, represents its results in such a way that the $1 machine vulnerability is actually identified as being a potentially $100 problem due to its relationship with the initially scoped critical items.

Now a potentially unaddressed critical vulnerability is prioritized in a way reflecting its ability to impact the overall risk value associated with an organization.

Application of Strategic Cybersecurity

So we have learned what the concept of strategic cybersecurity is and we have walked through how CAPTR teaming is a way of strategically implementing the practice of offensive security. The following is a contrast between what a traditional approach that might be taken in the application of offensive cybersecurity practices to our example sneaker company compared against using a strategic approach via CAPTR teaming assessment.

The Classic Approach

As outlined in the description of what and why CAPTR team assessments are, we described that in large part, scoping and initialization are points of potential improvement in what would be described as traditional red teaming or penetration testing events. In a classic offensive security application, leveraging such testing, the same would hold true. The CISO of our sneaker company would seek our offensive security assessment to identify potential gaps in their network security posture for improvement. This would likely be done for one of two reasons. Offensive security assessment such as penetration testing may be a regular part of the organization security framework, such as for information assurance certification, or the organization has recently been breached and wants to assess its posture in a post remediation.

Regardless of why such services are procured, the process is essentially a scope of targets, and a timeline is agreed upon between the consumer and producer of the offensive security solution. Typically, the scope, time, and number of resources put on this test will be driven by the CISO's budgetary allocation. This means mileage may vary and if the test is being done to check a box of "yes we have done our annual penetration test or red team event," then the solution is usually focused on how cheaply this can be accomplished. What this usually leads to is short, low-resourced assessments that focus on scoped targets accessible from the external initialization perspective, that is, the organizations external network perimeter. The result is often little findings, and even when vulnerabilities are discovered, they are on systems of lesser consequence or higher replicability due to the nature of them existing on the external side of the organizations security posture. Therefore, a classic approach provides a traditional offensive security assessment whose results are likely to be of little consequence to the organization. In fact, the goal of such assessments is more a function of compliance than for the discovery of actual vulnerabilities.

The Strategic Approach

Using a method like CAPTR teaming allows for even short, low-resourced offensive cybersecurity assessments to be tailored toward providing the most cybersecurity cost benefit with regards to the organization's strategic goals and outcomes. If the onus is on having done an annual penetration test, why not do one that does as much as possible to support the organization's strategic mission?

In this strategic approach, the CISO would go through the outcome-oriented scoping and worst-case risk assessment used for CAPTR teaming. The offensive cybersecurity assessment would then be targeted at critical assets, directly supporting the organization's strategic tasks, and achieving its strategic goals. Since time is not wasted on more trivial externally scoped assets, any findings are likely to be of high consequence and directly inform remediation efforts aimed at protecting strategic assets. In this strategic approach for offensive cybersecurity, CAPTR team assessments would allow or sneaker CISO to not only check the compliance box for having done the annual assessment but potentially finds issues in strategic assets, such as servers running intellectual property like proprietary sneaker design software that gives it a leg up over its competition and allows it to stay in the infinite game longer by protecting such attack surface as a priority through targeted vulnerability assessment of those strategic targets.

Summary

This chapter served as an introduction to the concept of strategic cybersecurity. Examples like that of our shoe company CISO will hopefully become more the norm as theoretical cybersecurity concepts such as strategic cybersecurity are more common. This will only be possible through improvements and encouragements in the cybersecurity industry that result in more theoretical cybersecurity research for the sake of improving cybersecurity and its application. We also covered how the family or sector of cybersecurity that is offensive cybersecurity can be tailored to enable strategic cybersecurity. With unique scoping, initialization perspective, and reverse red teaming methodology, Counter APT Red teaming allows for offensive security to be implemented in a way that is aimed at protecting an organization’s strategic goals and outcomes and less on protecting it from every threat.