TOWSON UNIVERSITY

OFFICE OF GRADUATE STUDIES

TOWARDS IMPROVED OFFENSIVE SECURITY ASSESSMENT USING COUNTER APT RED TEAMS

by

Jacob G. Oakley

A Dissertation

Presented to the faculty of

Towson University

in partial fulfillment

of the requirement for the degree of

Doctor of Science

Department of Computer & Information Sciences

Towson University
Towson, Maryland 21252

May 2018

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

TOWSON UNIVERSITY

OFFICE OF GRADUATE STUDIES

THESIS APPROVAL PAGE

This is to certify that the Thesis is prepared by:

Jacob Oakley

Entitled:

TOWARDS IMPROVED OFFENSIVE SECURITY ASSESSMENT USING COUNTER APT RED TEAMS

Has been approved by the thesis committee as satisfactory completing the thesis requirements for the degree: Doctor of Science (i.e., Doctor of Science)

Chairperson, Thesis Committee Signature	Mike O'Leary Type Name	3-9-18 Date
Thesis Advisor, If other than Chairperson Signature	Type Name	Date
Committee Member Signature	Suranjan Chakrabarty Type Name	3.14.2018 Date
Committee Member Signature	Chao Lu Type Name	3-9-2018 Date
Committee Member Signature	SIDD KAZA Type Name	3-9-18 Date
Dean of Graduate Studies	Janet V. Dohany Type Name	3-27-18 Date

Abstract

Towards Improved Offensive Security Assessment Using Counter APT Red Teams

Jacob G. Oakley

Defending against cyber criminals, cyber warfare and cyber terrorism all rely on the mitigation of the motivated advanced persistent threats (APTs) that carry out such campaigns. The only pro-active solution capable of addressing these threats is ethical hacker conducted emulation during offensive security assessments such as penetration testing and red teaming. Many security industry institutions label their products or services as addressing APTs unfortunately there is no agreed upon standard for the proper processes, tradecraft or techniques involved in doing so. Additionally, academic efforts regarding APTs largely focus on reactive monitoring or automated assessment which simulate known attack sequences and do not necessarily represent realistic future attacks. This dissertation aims to provide a standard for addressing APT attacks by counter-APT red teaming (CAPTR teaming). The CAPTR team concept seeks to build upon traditional red team processes to augment the offensive security assessment process. This will allow security practitioners a level playing field to engage and mitigate the threats and vulnerabilities most likely to be leveraged by APTs. Such an assessment counters the outcome of APT breaches by prioritizing vulnerabilities that enable an actor to compromise the data most important to an organization locally and pivoting outwards to points used for access and exfiltration. When an organization identifies critical items that represent unacceptable losses they should be protected as if an actor, regardless of motivation, were intent on compromising them. Adequate identification and protection of critical items via offensive security assessments

originating at such positions represents an approach more efficient and capable of mitigating the impact of an APT breach. In a threat landscape with hyper-focused actors it is the responsibility of the security field to provide an equally focused security assessment solution that goes beyond the attack simulations of traditional penetration tests or red team engagements. This dissertation discerns the need and novelty of the CAPTR teaming concept and ratifies the validity of the assessment paradigm through experimentation as well as case study.

Table of Contents

Table of Figures

Table of Tables

Introduction

Successful cyber-attacks have become increasingly detrimental to victim organizations. In some cases, over 100 Million individuals are affected, and Billions of dollars of damage done. The recent Equifax breach affected 143 Million individuals whose social security numbers and other personal information, in some cases including credit card numbers, were compromised (Haselton, 2017). The company's stock tumbled almost 13% in 24 hours resulting in a loss of nearly 2.275 Billion dollars in market cap (Melin, 2017). Breaches are now becoming capable of leading to actual death of humans whether it is ransomware preventing adequate healthcare from being given (Wace, 2017) or SCADA systems controlling manufacturing and power plants maliciously sent awry (Hinden, n.d.). Increasing the challenges of keeping up with cyber threats, malicious actors have been able to get their hands on tools of ever increasing sophistication and capabilities thanks to leaks of nation state tools such as stuxnet (Mueller & Yadegari, 2012) and wannacrypt (Microsoft, 2017) by entities such as the Shadow Brokers (Perlroth, 2017). Ethical hacker conducted offensive security assessment represents the only true proactive tool towards addressing such prolific threats.

Unfortunately, by attempting to act on level terrain to Advanced persistent threats (APTs), practitioners of offensive security assessment are doing a disservice to their own success and the security of their customers. An offensive security assessment has a set time window and must follow an established set of rules as well as insure the legality of assessment activities. Conversely, APTs such as nation states, crime syndicates and other extremely resourced and motivated actors abide by their own constraints if at all. Such actors can even resort to illegal means such as blackmail, espionage, and physical violence to enable successful cyber operations.

Though known as ethical hackers, offensive security assessors should be doing their best to cheat the competition. Malicious actors and traditional threat emulators alike spend a large amount of time and effort in attacking a whole organization in search of valuable machines and data. Security assessors should instead leverage purple team and operational resources to identify and prioritize assessment of such critical items. Further, offensive security assessors should start their campaigns from the comparative high ground, beginning assessment from high impact items instead of wasting time on the journey to them. It is in this spirit that counter-APT red teaming (CAPTR teaming) aims to shift the operational advantage away from APTs and towards detection and prevention. CAPTR teaming is an offensive security assessment model implementing three novel evaluation attributes.

- Worst case risk analysis to identify scope
- Critical compromise initialization perspective
- Vulnerability analysis and exploitation using reverse pivot chaining

Worst Case Risk Analysis & Scoping

The CAPTR team will work with both operational and security personnel in the organization to determine appropriate scoping for the assessment. The CAPTR team scope is a prioritization of critical items which have a high impact if compromised, regardless of the likelihood of that compromise. This allows for assessment resources to be spent in an efficient and effective manner on a worst-case scenario subset of the overall organization. Successful identification of high risk items requires stakeholders from both functional and security areas of the target organization. The operational staff may know which compromise objects could bring ruin to the organization if breached. However, such operational staff may not know the extent to

which devices and data within the network represent or support those objects which is where the knowledge of IT infrastructure and security staff is equally important to identifying as complete an initial scope as possible. Limiting the initial scope of CAPTR team assessment to high risk objects allows for assessors to focus on a small attack surface comprised entirely of assets of importance and prevents wasted resources being spent on anything but the most consequential attack surface. Adequate identification of priority assets during the scoping phase enables successful evaluation of critical compromise items. This leads to improvement of overall security posture via mitigation of worst case scenario threats.

Critical Initialization Perspective

Initialization perspective is the point of presence from which an offensive security assessment begins scanning and enumerating vulnerabilities. Examples of common Initialization perspectives may be from the internet, external to the organization or from different locations within the organization. The position of the initialization perspective effects many attributes of the security assessment such as the type of attack surface first assessed, the type of threat emulated and threat of identified vulnerabilities among others.

Beginning an assessment with a scope of high risk items from the initialization perspectives of an internet based threat, a compromised DMZ server or even a successfully spear phished internal user machine can hinder the progress and success of assessment. To best address vulnerabilities that may be leveraged by APTs, concessions must be made that those threats already have or will have the ability to penetrate the perimeter and subsequent layers of the organization. With high impact compromise objects identified and the scope created the CAPTR assessment model begins assessment from the priority risk items themselves. This is known as leveraging the critical initialization perspective. This perspective allows a CAPTR team

assessment to perform immediate assessment of high risk compromise objects instead of first spending the time identifying a path to them.

Reverse Pivot Chaining

Reverse pivot chaining is a two-part process for identifying findings that have the most consequence to those initially scoped compromise objects. A localized assessment is performed on each scoped compromise item. Then, these compromise objects are leveraged as critical initialization perspectives for outward assessment of the host organization. This outward assessment is done in an atypically targeted and unobtrusive fashion which identifies tiered levels of communicants and their relationships to the initially scoped items. These relationships ultimately represent a risk link web spreading outwards from prioritized high impact items.

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 ability to leverage escalated execution on these devices also allows the CAPTR team assessor to determine the communication links that allow other devices and users remote access.

live data such as open sockets, running protocols and active users as well as artifacts such as authentication, application and system logging are used to aggregate a list of potential communicants to the initial perspectives and roll them into an expanding scope for the assessment. In an effort to pivot outwards The CAPTR team uses this information for targeted prosecution of communicants instead of widespread remote scanning. If access is gained to tier one communicants, the locally elevated assessment process begins anew and pivoting to next-tier links is then attempted once they are identified.

This reverse pivot chaining establishes a representation of threat relationships into a risk link web with the critical compromise items at the center. Even if remote exploitation of tier one or further outward communicants is not possible the communication link is still identified with an appropriate risk rating commiserate with its potential to enable attacker access to critical compromise objects. Such information is vital to empowering defensive security equities within an organization to mitigate and or monitor the threats identified by CAPTR team findings. This web of risk links is a unique step forward in collaboration between offensive and defensive security teams to improve security posture.

Success of the CAPTR Team Concept in the Real World

The offensive security assessment attributes involved in CAPTR teaming have been utilized alongside multiple real world red team engagements. The red team responsible for long-term offensive security campaigns and adversary emulation in a fortune 500 technology company leveraged the CAPTR methodology to coincide with several red team campaigns. Using the CAPTR team method, extremely dangerous findings to high value systems were discovered in a time window of only several days. This is instead of the weeks or longer taken during red team engagements against the same subset of the company. In several instances the

CAPTR team assessment method was able identify findings in areas that the traditional processes were unable to progress to at all during defined engagement windows. CAPTR teaming provided previously unattainable efficiency in impacting the company security posture by prioritizing assessment of critical items within the specific subsets of the company.

Success of the CAPTR Team Concept in Experimental Evaluation

Academic and industry research on ethical hacker conducted offensive security assessments should include a standardized, portable and repeatable experimental framework for defensible evaluation of different assessment processes. This dissertation outlines one such framework and details its construction and implementation to provide an experimental testbed for measuring the novelty and success of offensive security paradigms.

Comparative evaluation of the CAPTR team offensive security concept was accomplished using this experimental framework. A host organization network was created in a lab and clones of it assessed using traditional red team and CAPTR team methods. These assessments yielded recommendations to the host organization to mitigate identified security threats. These changes were implemented to the respective clones of the original network. Then, both the CAPTR team and red team secured networks as well as a control network with no changes were attacked by a highly skilled APT emulating ethical hacker to test the security posture of the organization.

The experimental data that was collected indicated that the CAPTR team process provided findings unique to those of established offensive security assessment methods. In identical assessment scenarios there was only one finding in common between the two assessment methods out of a total of sixteen. The findings and resulting recommendations from

the CAPTR team assessment ultimately empowered administration of systems that mitigated 400% the overall threat than was done by the red team assessment method. Further, the CAPTR team method protected all initially scoped compromise items throughout the attack campaign where the red team did not.

CAPTR Teaming Concept

The CAPTR team works with an organization to identify items of dire consequence referred to as critical or lethal compromises. CAPTR teaming allows for organizations to evaluate such items of severe impact as a priority during offensive security engagement. Lethal compromise items are not the only type of equity included in the initial scope of a CAPTR team assessment, as any scoped object that is critical, lethal or otherwise important to the organization will be prioritized for evaluation. Lethal compromise items do however represent the epitome of the cost benefit gains an organization can accomplish by leveraging the CAPTR team concept to protect such assets.

Lethal Compromise

Lethal compromise is meant to be interpreted as literal and figurative with regards to the target organization. In a literal sense a lethal compromise item could be a device or data that if affected could lead to a human being dying. This could be something medically related such as gaining access to remotely monitored insulin pumps and supplying lethal doses (Ray & Cleaveland, 2014). It could also be loss of control in a SCADA environment where robotic implements could crush a human or controllers could be tampered with leading to a chemical plant explosion (Narayanan, 2015). In the figurative sense a lethal compromise item is one that can cause an organization to cease to function. This lethality could be due to unpayable amounts