NETWORK CREDENTIAL MANAGEMENT

BLOG POST 2: WHAT ALL OF US BLUE TEAMERS NEED TO DO

SAM BREJCHA
@SAMBREJCHA
NOVEMBER 2016

Alright, so I lied in my last blog post. I said I was going to talk about delegation models in this post, and I know everyone has been hitting the refresh page on our website to see the article drop. After a lot of reflection and listening to talks on YouTube, I decided to switch things around. My next post will be about delegation models, I promise you that, but for now, I have two very important words for you. Before I reveal these words to you, let me say this: I have never served on a Red Team engagement. My roots are in network maintenance and have grown into IT security. I was born into the world of frustration with incompetent bosses, miles of red tape, and the exhaustion that comes with trying to stay ahead of the curve while Pen Testers walk around like rock stars, so I completely understand your world. That said, I also see what Pen Testers do to us every time, let alone our adversaries. So, please understand what I'm about to say:

GET GOOD

That's it. These two words are worth a mountain of wisdom and best practices. Why am I so blunt, you ask? Tell me, how many Defcon or Derby Con talks have you listened to in recent years? Listen to some. Any of them. In the offensive cyber world, it is assumed that Red Team is going to break through your defenses, that they will compromise a local system to the root level and obtain domain admin. Many speakers say, "let's assume that we have compromised this box and have root access." One speaker I heard said something along the lines of, "If you can't get a call back from a phishing attempt, you are doing something wrong." In my mind, I'm thinking to myself "Why?!" It's 2016, and we haven't hardened our networks enough to even make Pen Testers break a sweat. (That's on all of us Blue Teamers, including myself.) I saw an interview on Security Weekly's YouTube channel with Sean Metcalf (one of 100 Microsoft Certified Masters in AD in the world), and the consensus was that Red Team will always get domain admin.[1]

Again, I understand the situation. The deck is stacked against the blue-collar network administrators. On top of dealing with attacking adversaries, we face change management boards, evolving regulations, ineffective bosses, new and evolving technologies, and expiring certifications and CPE, all the while trying to have some kind of life outside of our profession. However, we signed up to navigate this mess whether we knew it or not. As the saying goes, "Everything that you obtain, you have to maintain." Your organization has obtained a network, and your job is to maintain it. This means that you must constantly improve yourself and your IT bag of tricks.

I feel that the following story applies to many Blue Teamers. I saw a driver pulled over on the side of the road one day with his hazard lights on. As I was feeling particularly charitable, I decided to pull over to see if I could be of any assistance. It turns out that his car had no oil, and I asked him how many miles he had driven since the last oil change. He guessed it to be somewhere between 6,000 and 7,000 miles, commenting that he thought you only changed the oil in the car when the light came on. His ignorance of car maintenance did not prevent the car from breaking down. As shocking as this story may be, it applies to how we sometimes look at our

networks. For example, we only look at event logs when a breach has happened or configure our update servers after our domain controllers have been exploited by MS14-068. Just like that driver, we have a responsibility to maintain the assets we have been entrusted with. We have accepted the responsibility of a network; therefore, it is our responsibility to defend it, regardless of our lack of knowledge and experience. We can only do that by continuously bridging our knowledge gaps.

So, why am I going out of my way to mention this when I'm supposed to be discussing credential security? If your team does not perform Network Security 101, what I say won't matter. If your company does not have a solid patching program, hardened perimeter devices, or any other basic network defenses, then you have bigger issues than fine tuning user right's assignments, establishing PAW workstations, and similar measures. Red Teamers and adversaries will always exploit the lowest hanging fruit and lack of basic security practices will hang lower than anything I will discuss in this series.

I will wrap this up by recommending that you listen to two talks. The first one gives general guidance on how to "Admin Like a Boss",[2] and the second one discusses specifics reguarding Active Directory security.[3] Both are wonderful talks and provide practical, low cost ways to increase the security of your network dramatically. Finally, start becoming involved with IT security. Subscribe to some RSS feeds, or create a Twitter account. Many of the new things I am discovering are coming directly from legends in the IT security world like GentleKiwi (Mimikatz) or HarmJ0y (PowerView and BloodHound). (Personally, I hate Twitter, but if that is what I must do to stay ahead, then I will yield to the Twittersphere.)

I promise that my next blog will talk about delegation models and their importance. For now, though, remember that we as Blue Teamers can do better and have the obligation to be better. Our world evolves way too fast to hang on to the practices of the past. We must up our game if we want to protect the networks with which we have been entrusted. Together, let's make Pen Testers and adversaries alike actually start working hard when attacking our domains instead of ordering their Champaign bottles on day one of the engagement.

1) https://www.youtube.com/watch?v=L8vX56kTsyE&t=851s

2) https://www.youtube.com/watch?v=jKpaaDKVovk

3) https://www.youtube.com/watch?v=uccM2xtE5SA