

Forum:[Hack Forums](#)

Thread: [Real Story of a Pentester #2 - Bloodhound](#)

[BLANK] - February 5, 2018, 7:55 am

INTRODUCTION

I received a lot of positive feedback from the first story, Jenkins, so I thought I would write the second story now. The first story was pretty basic as far as techniques go, nmap scanning, finding an insecure instance of Jenkins administration panel etc. As I hinted in the comment thread I have a much better story to tell. This one will involve more complex technique so I hope you enjoy it.

First I would like to clarify a couple things. This story is based on a PCI Compliance test of a Community College, with the goal of access Card Holder Data, it is an internal network test. Meaning I was provided with entry into the network via a specially crafted computer that was placed on the network. The computer was not a part of the domain (which would make it even easier) but I had the same level of network access as any of the computers on the network. I had no special credentials or access though. This type of test can be summed up as "assumed breach" meaning I am testing from the standpoint of an attacker gaining a small foothold inside the network. We also perform External Network testing which we then assume the position of an attacker trying to get through the external security first but that is not relevant to this story.

GETTING STARTED - TESTING FOR SEGMENTATION

After I connect to the VPN of my attack host I first check to see if I can reach the Card Data Environment (CDE), which I shouldn't be able to do in a properly secure network. I run a basic nmap scan to check if any ports are open on the CDE.

Code `nmap -sS -Pn -n -p- -T5 TargetIP --open -oA target`

Two things become evidently clear as the scan completes. One, I have full access to the CDE, and two the CDE is a Cisco Router. In this instance the customer only uses a router to route credit card data to a third party who will then process payments. Well that complicates things greatly. I attempt the basic ssh connection but the router only accepts certificate connection, certificates I obviously don't have. So here is the challenge, I have to access a Cisco router that uses its own Cisco GUI interface from a location that has both the interface and the correct credentials already installed. No wonder they didn't bother to segment the router off.

I didn't give up though because one thing about the router not being segmented means that everything in the network and every other subnetwork that connects to this network are now in scope to test. Meaning, it is time to own everything and hope I can figure out a way to reach the router.

ATTACKING THE NETWORK

Now that I knew the difficulty of attacking the CDE directly, it was time to start attacking the network as a whole. I first ran a scan on my local subnet and found I was placed with mostly web servers, essentially they put me in a DMZ where they figured I could do little to no harm, that was cute. I attempted to get credentials and other information by first listening to broadcast packets. I spun up Responder and NTLMLrelayx to see if I could abuse LLMNR broadcasting to get some password hashes. Unfortunately this lead to only a few morsels of information that were primarily services related hashes. Normally I prefer living off the land but if I have to brute my way onto the network, fine.

Next I went to the tried and true EternalBlue. I scanned all the servers but only one appeared vulnerable. Unlike a lot of companies this college at least attempted to patch most of their servers. But they did leave one vulnerable. I popped the server but after some enumeration it was clear that the server was not a part of the domain, I grabbed the hashes anyways. Now, one thing I have found to be true in most networks, especially large ones, is that local administrator password is often re-used. So I spun up crackmapexec and ran a SMB Pass-the-Hash check on the other servers in the network, and I got a hit! Actually I got about six or more hits because even though that vulnerable server was not in the domain, it had the same local admin credentials as the server that were in the domain. With CME Mimikatz module I was able to dump clear text users and passwords. And with that, I could RDP into server, connect shells etc. At last I had my foothold on the domain, now it was time to really get started.

ON THE DOMAIN AND BEYOND

At this point I had SYSTEM and Administrator access on several computers but it became clear I was dealing with a network with thousands of host machines, different subdomains, subnetworks etc. It could take weeks if not longer to map out the entire network and figure out where I needed to attack. My goal at this point was to get at least DA but Enterprise Admin would be preferable. Now it was time to bring out the big guns.

I spun up an instance of Cobalt Strike, I added a couple of the computers that I had compromised onto Cobalt Strike beacons for persistence and because it made pivoting through the network a lot easier. At this point I could start manually user hunting with PowerView and other tools (see my Tutorial) but I honestly didn't want to spend the hours that may take to do manually. So I ran BloodHound via Cobalt Strike on one of the web server I had compromised. After about twenty minutes of running, it completed. I moved the xml files onto my host machine, spun up Neo4j and loaded the xml files. The screen lit up with network connections made, at first it was a lot of data. But I filtered the data to show me what I really wanted, Domain Admin.

And I saw it, my path to complete ownership of the network. In just twenty minutes BloodHound found the Domain Admins, where they were logged in, and how I could compromise their credentials. Game on.

GETTING DOMAIN ADMIN

I had to pivot through many different computers. Changing my user tokens as I went. I found that most of the computers prevented psexec so that created a small hurdle. Luckily I have a nice trick that usually works when Administrators think they are clever. WMICEXEC works in most situations if you have credentials or even a hash. For some reason psexec is often flagged by AV or other security, but wmiexec is rarely flagged or stopped. So in some cases where I couldn't just upload a new beacon directly in Cobalt Strike with psexec, I was able to directly gain a shell with wmiexec and then just copy and paste my powershell oneliner for the Cobalt Strike beacon, and walla another box owned.

After about thirty minutes of pivoting through one computer after another I got a Domain Admin account. But I didn't stop there, because one step later I got Enterprise Admin, I was now a god on this network. All computers were at my disposal...but a Cisco box is not that easy. None of the credentials I gathered would work via ssh and I still didn't have the GUI to the router. At this point my work day was over (yea all of the above happened in about a six hour window) and I decided I could take a break.

SERVICE HUNTING

The next day as I was sipping on my coffee (or energy drink) I was pondering how I would go about getting on the router. I started cruising the network, RDPing from one box to another, in search of anything useful. I found teacher computers, student computers, the shop, etc. I found plenty of

interesting information, projects, backup archives...but not until I found a backup server did I finally encounter the Cisco GUI. Awesome I finally found a way to talk with the router! I quickly opened the GUI, typed in the credentials I found and waited...nothing happened, access denied. Damn! So close but I finally figured out my way in. I needed to find a GUI that was actively logged in. How would I do that? Think for a minute, who would have access to that sort of thing? The IT guys, of course! My main point of contact for this project was also their senior network administrator, I will call him Smith. After a quick search I found Smith's computer and after looking through my gathered credentials (which was well over 60 by now) I found Smith's credentials in plain text. Awesome, one last thing to verify...yep his computer was open to RDP.

CRACKING THE ROUTER

I RDP into Smith's computer and held my breath. If he was on the computer at the time then I wouldn't be able to RDP because it would kick him off. AND if he wasn't on the computer and shut the computer down then I wouldn't be able to connect. But it was my lucky day, not only was the computer merely locked (meaning my RDP with credentials unlocked it) but the user was away. The desktop loaded and it was Christmas day. Looking at the program panel I could see dozens of programs opened and logged in already. I saw network spreadsheets, passwords, several different network devices, and just before dispare kicked in...there it was, an open Cisco GUI already logged in and ready to go. I had compromised the CDE! I quickly added a new account on the Router so I could access it via SSH anywhere on the network and do you remember that backup server I found? Before backing out though there was one thing I had to do. It may seem a bit unprofessional but fuck it, I worked hard to get here. I saw that Smith's skype was open, I did a quick search for the second point of contact who I will call John. I opened a message window and typed "Talk to you later, have a good day". Now you may thing, well that isn't much, but can you imagine Smith's face when he sees a message from him that he didn't write...on his own computer?

CONCLUSION

I backed out of the user PC without changing anything else. I RDP backed to the remote server where I knew I wouldn't be disturbed, spun up the CISCO gui and entered in my newly minted administrator credentials. Boom, full access. I did a quick Google search about enabling active TCP dump from the gui and took my proof screen shot. If I was a legit attacker I could sit on that router collecting the data being routed en mass.

I hope you all enjoyed the story!

Nomad.Null - February 5, 2018, 8:18 am

Very nice linkage. Good tip about wmiexec too. I haven't run into many systems where psexec was disallowed but this maycome in handy in the future. :)

_StillAlive - February 5, 2018, 10:15 am

Very interesting story, thank you for sharing it

JELLY?IsH - February 5, 2018, 10:37 am

I love your stories so far, keep posting!

onehitwonder - February 5, 2018, 1:08 pm

Please keep going with your storys!

fuzzypanda - February 5, 2018, 10:47 pm

really good story, inspiring!

CyberStrike - February 6, 2018, 1:57 am

Nicely done, usually I see RDP being used for lateral movement, but this works as well seeing that

they wanted you to go after just one machine and you had to hunt that machine down. It's awesome how even a regular user can pretty much get everything and anything about the AD, BloodHound makes the old days of user hunting which led to many dead ends pretty much obsolete, unless someone just is a glutton for punishment. Also gotta love how large corporations use vnc/rdp so often definitely good for lateral movement. Well done!

Edit: Forgot to write this, but there is always that one machine in every network that either a patch fails or they have not rebooted something sometimes it is a critical piece of the network that they don't want to break and you find it is vulnerable to something which it shouldn't be.

SysAdmin - February 7, 2018, 2:19 pm

A very great read! Looking forward to many more of these stories.

JohnG0tti - February 7, 2018, 4:07 pm

Great story you need to write a book!

hempuk - February 9, 2018, 5:35 am

Nice work on this mate great tip about wmiexec cant wait for part 3

Immy4you - February 21, 2018, 11:01 am

glad to know about your story man
take much efforts for write it down

mach3te - February 24, 2018, 4:48 am

This Story is like music in my Ear. :D