(U//FOUO) Caveat: it's been a couple years since I have attended a security conference(Shmoocn/Defcon/Blackhat). My opinions are not formed from recent first-hand experience, but through previous stimuli to my cerebrum that have been confirmed by 2nd hand experience over the last couple of years. When I first went to Blackhat/Defcon, it was with the wide-eyed anticipation of, "I'm going to go listen to all of the talks that I can, soak up all of the information possible, and become a super-1337-haxxor." What a let-down of an experience that was. You find the most interesting topics and briefings, wait in lines to get a seat, and find yourself straining your ears to listen to someone that has basically nothing new to say. Most of the talks get hyped up exponentially past any amount of substance they actually provide, most of the "interactive sessions" end up in a "oh! woe is the state of the security industry!" chant, and leave the audience no better off than before.

(U//FOUO) If you want to learn crazy new things, more often than not, you won't find it at a talk in a con. Why not walk around NSA, find people in offices that do things you find interesting, and talk to them about how they do what they do(or find a mentor in that area)? Despite stereotypes of the kinds of people that work here, many people are kind and open enough to share their trade-craft with others. We have the luxury of working in a community that has some of the brightest, smartest, and most cutting edge people around, it would be a shame for people to constantly attend cons hoping to learn that "cool new thing", when there is exponentially more knowledge sitting around them every single day at work.

(U//FOUO) Granted, there are always a couple exceptional talks at the cons, but, in my humble opinion, they don't make up for the overall lack of content. So, what good are these conferences? My personal opinion is that their utility is mainly for social interaction and meeting *relatively* like-minded individuals. It's the ability to kick back for a weekend and geek-out with other people. For some, this makes the cost of the con completely worth it, others may be severely disappointed...it all depends on what you expect to get out of it.

Current Mood: 😞 okay

Leave a comment
So, SIGINT is down right cool. As much as we complain about our "Big Data Problem", collection/processing issues, dismal infrastructure/outdated browsers/OS's, our ability to pull bits out of random places of the Internet, bring them back to the mother-base to evaluate and build intelligence off of is just plain awesome!

One of the coolest things about it is how much data we have at our fingertips. If we *only* collected the data we knew we wanted...yeah, we'd fill some of our requirements, but this is a whole world of possibilities we'd be missing! It would be like going on a road-trip, but wearing a blindfold the entire time, and only removing it when you're at one of your destinations...yeah, you'll still see stuff, but you'll be missing out on the entire journey!

So I decided to write a short series (affectionately titled 'I hunt ...') on things that I'm trying to do with data that wouldn't normally be interesting by itself, but by thinking about it in a new way, makes it extremely valuable. My interests lately have been in using passive collect to identify/enable CNE efforts, so that's predominantly what the first few topics will be about.

If there are any topics someone wants to see specifically, let me know. As well, if any of the following information is useful, please let me know and I can put more out. Part 2 - Hunting sys admins coming very soon!
(U) This post is meant to provide a background for *why* it's good to target sys admins in SIGINT. If you already know this, feel free to skip forward to the next sections.

(SI/REL) Being in SID, our overall goal is to produce intelligence to give to decision-makers. How we go about doing that, is whenever a target uses technology to communicate, we collect it, analyze it, and write reports on it. Sounds simple enough...except for the fact that we have to be targeted in what networks we collect. We can't collect everything all the time, so if a target starts to communicate on a network where we are not collecting, there is some manual leg-work that has to be done to steer the SIGINT system in their direction. This is where I must introduce my loyal friend, the sys admin.

(SI/REL) Up front, sys admins generally are not my end target. My end target is the extremist/terrorist or government official that happens to be using the network some admin takes care of. Sys admins are a means to an end. For example, assume your target is using a CDMA device on a foreign network; there may be situations where we passively collect his phone call/SMS out in the wild, but it would be *really* nice if we had access to the local infrastructure where we could monitor which tower he's connected to at any given point in time, or monitor all phone calls/data traffic that his phone generates. Many times, it's difficult to directly target infrastructure...generally we'll need a fair amount of information going into an operation, such as:
* topology of the network we are targeting
* credentials for infrastructure devices
* situational knowledge, such as access lists set up to only allow specific IP addresses to administer certain machines
* an overall knowledge of how the network is put together and configured

(SI/REL) In order to get that, who better to target than the person that already has the 'keys to the kingdom'? Many times, as soon as I see a target show up on a new network, one of my first goals is, "Can we get CNE access to the admin on that network, in order to get access to the infrastructure that target is using?"

"Yeah, that pretty much makes sense, but how are you 'just gonna get CNE access' on an admin?"

(SI/REL) Good question, thanks for asking. Most of the time I'm going to rely on QUANTUM to get access to their account (yeah, you could try spam, but people have been getting smarter over the last 5-10 years...it's not as reliable anymore). So, in order to work our QUANTUM-magic on an admin, we'll need some sort of webmail/facebook selector for them.

"You know, you *could* just look up the 'point of contact' in the registry information associated with their IP space/domain names..."

(SI/REL) Yeah, you could do that. Personally, I haven't had a huge amount of luck with it, because most of the time I end up running across their *official* e-mail address that's hosted on their own network. That's generally not a recipe for success in the QUANTUM world, what we'd really like is a personal webmail or facebook account to target. There's a couple ways you could try this: dumpster-dive for alternate selectors in the big SIGINT trash can, or pull out your wicked Google-fu to see if they've posted on any forums and list both their official and non-official e-mails in a signature block...but what if there was another way to do it?

(SI/REL) Other fun (read:useful) things to get off of a sys admin (from my point of view):
* network maps off of their hard drive
* credentials from text files (or from our key-loggers...potato potato)
* full lists of customers (along with associated dedicated IP allocations is a bonus)
* e-mail with upstream providers detailing how your network is connected to the bigger Internett. For example, if I see they use certain fiber cables to connect to the world, I'll go look in SSO's collect for their traffic. If they use VSAT's, I'll go look for their network in FORNSAT's environment.
* pictures of cats in funny poses with amusing captions

(SI/REL) But all of this boils down to getting an admin's webmail/facebook account in order to QUANTUM it and get CNE access to their box. Next section will detail targeting admins who use telnet...

3 comments :: Leave a comment
(SUE) Okay, this is relatively self-evident. If you want toلبه انتر، this is something that you have to be careful about. If you wish to log in to the router, you have to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet. If you want to log in to the router, you have to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet.

(SUE) All of the information that you need to log in to the router is contained in the router. You can log in to the router from anywhere in the world, but you need to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet.

(SUE) Okay, this is relatively self-evident. If you want to log in to the router, you have to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet. If you want to log in to the router, you have to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet.

(SUE) So, by combining all of the information that you need to log in to the router, you can log in to the router from anywhere in the world, but you need to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet. If you want to log in to the router, you have to be careful about the way you access the router. The IP addresses that are allocated to the router are the ones that are allocated to the router. The router is the device that is used to access the internet.
If you're a professional developer, you've probably used SSH at some point. It's a powerful tool for securely connecting to remote systems. If you're new to SSH, or just want to learn more about it, this guide will help you get started.

**What is SSH?**
SSH stands for Secure Shell. It's a network protocol that provides secure access to a computer. It encrypts all the data sent over the network, including passwords, ensuring that your connection is secure.

**Why use SSH?**
SSH is widely used for connecting to remote servers, especially those running Linux or Unix. It's the standard for secure remote management of servers, and it's used by millions of people every day.

**Setup:**
To use SSH, you first need to set up a connection to the remote server. This typically involves:

1. **Choosing an SSH client:** There are many different SSH clients available, such as PuTTY (Windows), Termius (Mac), and Tsuru (Linux).
2. **Getting the public key:** Most servers require you to have a public key generated on your local machine and added to the server's database.
3. **Connecting to the server:** Use your chosen client to connect to the server using the appropriate credentials.

**Getting Started with SSH:**
Let's start by setting up a basic connection using PuTTY on Windows.

1. **Download PuTTY:** Download PuTTY from the PuTTY website.
2. **Open PuTTY:** Once downloaded, open the PuTTY program.
3. **Enter the host name:** In the Host Name (or IP address) field, enter the hostname or IP address of the server you want to connect to.
4. **Enter the username:** In the Username field, enter the username to log in as.
5. **Click on "Open"** to establish the connection.

**Connecting to the Server:**
Once connected, you can start using SSH to run commands on the server. For example, you can create directories, edit files, or install packages.

**Using SSH Remotely:**
You can use SSH to remotely manage your server. This is particularly useful if you're running services on a remote server and need to access them from your local machine.

**Conclusion:**
SSH is an essential tool for anyone who needs to manage remote servers. With a little setup, you can connect to your server and use it as if it were right in front of you. Whether you're a developer, sysadmin, or just someone who needs to access a remote system, SSH is the tool for you.

---

This is a basic introduction to SSH. For more advanced topics, such as key-based authentication, port forwarding, and tunneling, check out the resources linked below.

**Resources:**
1. [PuTTY](https://www.chiark.greenend.org.uk/~sgtatham/putty/) - A free and open-source SSH client.
2. [OpenSSH](https://openbsd.org/openssh/) - The open-source implementation of SSH.
3. [SSH Tutorial](https://www.tutorialspoint.com/ssh/) - A comprehensive guide to using SSH.

---

**Questions?**
If you have any questions about SSH, please feel free to ask in the comments section below. I'll do my best to help you out.

---

**Acknowledgments:**
I'd like to thank [name] for their help in creating this guide. Their insights and feedback were invaluable.

---

**License:**
This guide is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You are free to share and modify it, as long as you attribute the original work and share any derivative works under the same license.

---

**Update:**
This guide was last updated on [date]. If you find any errors or have suggestions for improvements, please feel free to let me know.
(TS//SI//REL) Happy Friday my esteemed and valued Intelligence Community colleagues! There has been a topic of conversation that has started to rumble beneath the surface of the Cyber-scene lately, it's about router hacking (for this post, I'm not talking about your home ADSL router, I'm talking about bigger routers, such as Ciscos/Junipers/Huaweis used by ISPs for their infrastructure). Hacking routers has been good business for us and our 5-eyes partners for some time now, but it is becoming more apparent that other nation states are honing their skillz and joining the scene. Before I get into it too much, let's go over some of the things that someone could do if they hack a router:

* You could add credentials, allowing yourself to log in at any time you choose
* You could add/change routing rules
* You could set up a packet capture capability...imagine running Wireshark on an ISP's infrastructure router...like a local listening post for any credentials being passed over the wire(!)
* You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels
* You could install a dorked version of the Operating System with whatever functionality you want pre-built in

(TS//SI//REL) There are a plethora of things you could do once you get CNE access to a router...suffice it to say, getting access to a router is very good for the actor, and very bad for the victim. So, we would obviously LOVE to know which countries/actors have access to what other routers (especially if it's our routers). Then the question comes down to:

"How would you identify the fact that someone has CNE access to a router?"

(TS//SI//REL) There are a handful of ways that you can tell if anyone has access to your router. Like, if you are free to log into your own router, you could frequently log in, run diagnostic commands, pull the IOS (or, more generically, the operating system file), hash that file, and compare that to a list of known-good hashes. But, how would you find out if someone has CNE access to a router that you don't own? How would you identify it if the Chinese had access to a router in Zimbabwe? If all you have is passive network traffic that we've collected in SIGINT, how would you do it?

The rest of this post relates to NSA's methods to detect when countries hack routers. We have redacted it to prevent helping those countries improve their ability to hack foreign routers and spy on people undetected.