Heather:

Welcome to the Hurricane Labs Podcast. I'm Heather, and today we're going to be talking about hardening your security again, but this time we're going to take a closer look at wireless security. Joining me, I have Tom, Meredith, and Roxy. Thank you for joining me today. So to kick us off, why do we need to have wireless security at all? Why not leave it free for the taking?

Tom:

So I think there's a couple reasons why you don't want that to happen. And a couple that come to mind right away is obviously wireless makes it easier for someone not physically in the same place as you to access your network. And by not physically in the same location, there is some degree of physical proximity you have to be within range and all that, but you don't have to be plugged into a jack in a room, for example, in order to get into the network. So that's one of the first reasons why you want to at least have some way to hopefully restrict someone else who's an outsider from being able to access things. Secondarily though, if you have an ISP, which is pretty much why people are going to be connecting the internet, a lot of times you're responsible for things that happen on that connection. So if someone were to access information, steal content, file transfers, those sorts of things that are against acceptable use policies for your provider that could result in you running into some trouble, because they're using your internet connection, even though you didn't do anything.

Roxy:

And there's also, in incorporate environments, in large offices, you may not necessarily know that somebody is nearby or that somebody is able to access the wireless network that shouldn't be. And so they could get on the network and sniff traffic. They could sit in the parking lot and sniff traffic as well, if it's not encrypted.

Tom:

Yeah. And kind of like that where you don't know where people are. I can actually think of a former client that we worked with that had, I wouldn't say a high-rise, but a multiple story building in downtown Cleveland. That was next to another multiple story building in downtown Cleveland that apparently had more restrictive access to personal devices and all that. So they actually had problems with employees from the other company using their wifi because they wanted to be able to get to stuff. So that's a really good point.

Heather:

Meredith as our pentester here today. What makes you cackle evilly when you're doing a pentest, when it comes to wireless security?

Meredith:

So the thing that I'm most enjoy seeing is places that don't have authentication tied to users. So they're not using something like RADIUS, where access to the wireless network is strictly on a user by user base. If there is one master password and that password is repeated across multiple networks that you have with wireless access, that means that your segmentation is essentially in name only, and that you're going from network A, which is guest network that they give you the password for at the security station has the same password as network B, which is staff. And it makes me cackle evilly and then cry a little bit inside about the lack of security.

Heather:

What about specific zones or areas that need particular attention?

Meredith:

So if you're in a situation where you absolutely have to have some critical infrastructure or critical systems connecting to something wirelessly, you definitely need to have some form of security on those areas. We'll get into the defensive and monitoring a bit later. But just making sure that if you've got a critical area that has a need for wireless, that there is basically adequate coverage and of course you're doing adequate offensive testing against it to make sure that people aren't sitting there stealing the connection and would be able to intercept traffic, things like that.

Tom:

And I think there's... And we're probably going to talk about this a little bit more, but there're different types of uses for wifi. There is authenticated employee wifi, where basically anyone who's there can treat that wifi similarly to what they would, the network connection that's at their desk or in their office. Which from a different perspective, you might not want to treat those things the same way, but we can talk about that more. But then there's also the idea of providing access to employee devices that are like BYOD, personal phones, tablets, anything like that. There's also access for visitors and guests that you need to consider, probably shouldn't have the same access as employees. And then also like you're mentioning Meredith, there are infrastructure devices that might just have to be wifi in nature. It could be sensors for infrastructure, building systems potentially, potentially even, you might have to have kiosks in an area that doesn't have wired connectivity, so it has to have wifi. So a bunch of different types of devices and categories of devices that fall into that. Your wifi, coffee maker, and all those other critical service to keep your employees happy.

Roxy:

And then there's even areas that maybe there's a lot of sensitive data or a lot of information that you want to be kept within that specific area. You wouldn't necessarily want someone to be able to sniff the traffic, even if it's encrypted, because there's still somethings that you can tell from encrypted traffic. So there might be certain areas with a lot of sensitive information or maybe there's people there that they don't want their traffic monitored, because clues can be taken out from even unencrypted traffic.

Tom:

Well, one question I'd ask is what type of clues and I guess metadata about a connection do you see that users might be concerned about or maybe should be concerned about?

Roxy:

Well, the types of connections that they're making, where websites they're going to shows IP addresses, things like that you can put together, a picture of who the user is or what they're doing. And this may be a very, very specific case that I'm thinking of, use case.

Tom:

One thing that comes to mind, at least for me, is I think someone was talking about what they saw in the DEFCON network logs or traffic or things like that from their wifi. Just something as innocuous as Slack channels or organizations, you can get an idea of what someone's doing just by what Slack channels they're in. That's just also something you can figure out what DNS requests. So I think that's a really good point of what information can be exposed just by being on a wireless network.

Heather:

So what sort of things can you do to make it more secure?

Roxy:

Well, one of the most important things you can do is to change the default settings. Because the routers that the ISPs give out, they typically follow the same format when they come up with the network name and the password. And so people could easily... There're certain specifications for the password, and if you know them, you could write a program or a script that runs through all of the possible password character combinations. And sometimes you can just look at the network name and if the network name hasn't been changed, you can tell which ISP they got their router from or which router it is. And then you know what kinds of characters and how many are in the password. And something that a lot of techs do when they install the network is they'll just put something like the phone number, the customer's phone number as the password. So even though they've changed the default password, they've still provided a very predictable password that you could run a script that goes through all the possible number combinations and crack the passwords. So you definitely want to change the default settings as one of the first things that you do.

Tom:

Yeah. And I think, and Meredith, you can correct me if I'm wrong on this, but I think at least, and this might not be a thing with WPA2 anymore, but WPA original edition, at least WPA1, something like that. Well, WPA1, I think, had something where they basically could calculate rainbow tables or something along the lines of that for common SSIDs. And it significantly increased the likelihood of something being compromised because of how the encryption key was based on the SSID, I don't know, am I making that up, Meredith?

Meredith:

I want to say that actually related to WEP not WPA, but I do know what you're speaking of because the rainbow table still exists and it's used in a lot of offensive student training challenges. Because of the fact that it will take about an hour to find the key if given the SSID.

Tom:

Yeah. For some reason it's about, WEP by recall it was trivial to crack it, even without any knowledge of the network, just because of how the RC4 encryption or whatever worked.

Meredith:

Right. You can do it within minutes from a Raspberry Pi to this day with no processing powers needed.

Tom:

The longest part of that is finding a network that's still using WEP I think, which is a good thing.

Meredith:

This is true.

Tom:

Fun fact Wired Equivalent Privacy means it's as secure as a network jack on your wall. That's the intent behind the name. So about the same amount of efforts it takes to walk in and plug something into the wall is the same amount of effort it should take to crack WEP. That's why no one should use it.

Meredith:

Interesting. Similarly, if you do have the physical access to whatever this device is from an offensive side, a lot of companies put their default credentials or their change to default custom password somewhere on a sticker on that router, so that if you have to hard reset it, it will always go back to that password. So one of the things that you can do is go hunt that physical item down and grab that password.

Tom:

Fortunately, I think that's probably more of a home use situation than an enterprise situation, but...

Meredith:

I would certainly hope so.

Tom:

I think another thing we're talking about though, is some of the other ways to secure enterprise wireless, especially where you're dealing with different levels of access and also guest access as well. One obvious thing that comes to mind is network segmentation for that, where your employees and your guests should use different networks, different SSIDs. And also the internet traffic that is associated with that should go out different, at least different IP addresses on your firewall, if not different connections. So that one, you have basically complete segregation of guest traffic from corporate traffic with the exception of VLANs, most likely, which I know that's not perfect, but it's better than nothing at all, obviously. But also if you do run into a situation where there is that activity on your guest network, that results in there being like a cease and desist happening or something like that, you could quickly determine if it's employee traffic or guest traffic just based on the IP address in the letter that you're given. I think something else to keep in mind too, in terms of segregation is deciding what type of access your employees should have when they get on wifi. And if that access needs to be different, then physical, like wired access or not. I think that the way a lot of organizations do that is they treat the wireless and the wired networks the same. And in some cases that can increase the amount of risk if a wireless device were to be compromised, but you can mitigate some of that by having solid encryption using basically certificates on the wifi that are authenticated with a login that the user has to basically have like a RADIUS type connection for that, to make it a bit more secure than just a shared key that everyone can have. Then at least you're tying that access to a user versus just a password that everyone has. I think that's pretty common at the enterprise level these days.

Heather:

What about VPN? How can using a VPN help make your access more secure?

Tom:

So I think, think that is a really great next step. So if you treat your employees connected to a wired network and a wireless network, even, I guess I flopped that. So if you treat your employees connected to a wireless network and potentially even your wired network as still untrusted and just providing connectivity, then you do a significant step to reducing the wireless network and even the wired network as an attack factor. Because if someone gets on an account or gets onto a machine, gets on the network, if they still have to open a VPN to access any critical corporate resources, you've essentially created a second factor of access in order to be able to get to the crown jewels of the environment. So a good example of that is if I go into the Hurricane Labs office, I can't access customer systems just from anything. So there's no different access for being physically at the office or working from home, regardless of what network I'm on. So that's a way that we leverage that in order to better protect customer systems, because there's that separate factor. I think it is an additional step. It's maybe a little bit more of an inconvenience for your users, but when you're protecting assets and infrastructure that you don't want someone just on the network to be able to access, I think it's a really good approach. And likewise, then you have additional monitoring that you can put around the VPN access as well, that you might not have as natively out of the box on the wifi side of things.

Roxy:

Especially with the pandemic, if you have employees working at home and you're concerned if they're going places like coffee shops, or even if it's not during the pandemic and you have employees that are going to coffee shops and airports, and places like that, where people can sit there and sniff the traffic. Then you're going to want all of your employees to use a VPN, even if they're working from home.

Tom:

And I think in that situation, it makes a lot of sense to not even split tunnel that, and just any internet traffic force it through the corporate network and you use the same access controls, any content filtering, any other tools that you have to inspect DNS requests in front of the user, accessing resources, as opposed to split tunneling internet locally corporate resources over the VPN. That can reduce or result in a somewhat inferior user experience though, if someone's downloading files and it also significantly can increase your bandwidth requirements. So there's a trade off for that, of course, just like everything in security.

Heather:

So what if they don't have VPN as an option?

Roxy:

Well, at least you want to make sure that your traffic is encrypted and you're using SSL as much as possible. So when you visit websites, you're going to want to make sure that it's HTTPS. And there are websites that don't have SSL encryption. And you just need to be aware that when you see that you don't log in to... If there's a website and they don't have SL encryption, then just be aware that if you're logging into something on that website, your username and password is being transmitted unencrypted. So most websites nowadays where you have to log in do have SSL encryption, but it's always good to make sure that you're looking out for that when you're not on a VPN.

Tom:

Yeah. I'm thinking, and I'm maybe struggling with this a little bit, but I think it would be hard to find a company that doesn't have a VPN, but has applications that you would log into that don't have encryption. I'm sure it exists somewhere, but if you think of the type of company that might not have a VPN for users, and they use maybe web apps entirely for their employees. Most of that's going to be run by a third party and probably having at least some form of encryption on the login, hopefully two factor authentication to get into those apps. Since it's essentially internet accessible for anyone anyway.

Roxy:

Have you worked at a call center? Yeah, I would hope that most businesses by now would have that down, but I have seen a few places that don't really make security a priority. But it's also good to be careful when you're logging into things like, well, your bank website, I would hope would have SSL. But when you're logging into more personal things as well, even if you're on the guest wifi and you're using your phone, just be careful and make sure that things that might be sensitive or that you might not want that traffic to be picked up on are encrypted. And it's not necessarily just for passwords, but for, I don't know, any kind of traffic that you wouldn't necessarily want people to know about.

Tom:

I think that just comes down to too being aware of what you're connecting to as well. Because your phone is going to be sending traffic, whether you want it to or not, and you can't necessarily stop every app on your phone from doing something, but you can at least decide what networks you connect to most of the time.

Roxy:

Right. Yes. And something to consider is that if you save a network name in your phone and it's a guest network or it's network that doesn't have a password in it, and you have your phone connect automatically. Then if I have a network with the same name as your favorite coffee shop, then your phone is going to automatically connect to it. So that's a very good point to be aware of what network your phone is actually on. Because I can set up... Isn't there the Pineapple that you can set up fake networks or?

Meredith:

Yes, essentially on a lot of things, you have the ability to man in the middle using something like a wifi Pineapple or any type of basically rogue access point that you design yourself to either mimic the SSID of another system, or sit there and intercept the traffic as that, supposed let's just go with Starbucks is your favorite coffee place where you like to sit with your laptop for hours that doesn't require authentication. You basically sit there with a network that says Starbucks. And if your signal is stronger than the Starbucks network itself, people will choose or people's devices that already know the network will default to you instead of Starbucks itself.

Tom:

Yeah. I think that's a really good point. And you could take that even further by just basically spoofing a lot of the very common SSIDs or network names for different locations. So like Starbucks, other national chains that have free public wifi typically will have the same network name. Default names that are open from access point names like the ever popular links as network that we used to all see 15 years ago, everywhere. Airport wifi names that are typically open, if you have common ones of those, a lot of business traveler machines will automatically connect to that. Assuming of course this was two years ago and not the current state of affairs, but still those are still going to be networks that devices will connect to. And you could pick up a lot of information just by having a device that has a lot of SSIDs in it that someone's phone or laptop will connect to and start trying to make requests to. So you could probably figure out what's sorts of services their devices trying to connect to. If there's a VPN, for example, their device will probably try to make a connection to that. Any device management things, Slack trying to make DNS requests, all that. So there is a decent amount of information you can make just by connecting to a wifi network, even if there's not any internet that's provided potentially even more, if there is. And often all you need to do in order to take or have other devices connect to a wifi network is to be the strongest signal. So you can have multiple devices with the same SSID and the laptop or phone is going to connect to the access point that has the best radio signal. Now that's a new connection, you have to do something to kick them off of another network if they're already connected. But that's still trivial to do because it's open in the air and you can basically send a de-authentication signal to those and get them to reconnect. And if you're stronger, you'll often be what they connect to.

Heather:

So here at Hurricane Labs, we work we with Splunk and alerting and monitoring. So what sort of tools do we see from our end of things that can be helpful when it comes to making sure that your wireless stays secure?

Roxy:

Now, Tom did bring up VPN access logs earlier, which that would be from the VPN side. But as far as the router goes, you can look for access logs to the router as well. You can also monitor for the types of devices that connect because the router will know from the Mac address, what type of device it is. If it's a phone, if it's a PC.

Tom:

Yeah, I think probably the first step to doing good monitoring and alerting around your wireless infrastructures to make sure you're collecting the data and logs from your wireless devices. And by wireless devices, I mean wireless infrastructures. So your wifi access points, your network controllers, those sorts of things, typically that can handle syslog traffic and send it into basically Splunk. And you'll be able to get all kinds of information about what devices are connected and where, and then you can start to use that in security use cases. And I think Meredith, since you work on the SOC side things, you're probably going to be the most in touch with what we see clients doing around wifi.

Meredith:

Yeah. It comes down to a very customized view of what your product is, the amount of things that you are logging such as authentications to the access points themselves. The overall network, and then what exactly you would like to see out of it, whether or not it's users attempting to log into SSIDs that they shouldn't be logging into or shouldn't have access to. People attempting to authenticate to the wrong network for either accidental or malicious reasons. And then of course, if you are assigned one area and wish to venture out why exactly you are doing that from essentially a UBA standpoint, that's always interesting to look at as well.

Tom:

And I think tracking things like authentication attempts and failed authentication to your wireless is something that's worthwhile too, which could indicate a potential brute force attack, or just simply a misconfiguration.

Meredith:

That is definitely something I overlooked from speaking for. I know that we do have the monitoring in place for that at some places, but it is certainly a search that we have built out and are able to deploy wherever at will.

Tom:

I think another thing we see is when you have the mandatory password changes and you use authentication that's tied to the user account. It's not uncommon for a user account to get locked out when a device is still trying to authenticate using a password that hasn't been updated. So it's not necessarily a use case of your wireless being compromised, but it's a side effect where potentially even using Splunk to proactively notify users about this happening. So they don't have to call the help desk that could save you a lot of time too.

Heather:

So bottom line what would you say are the most important things people can do or companies can do to make sure their wireless stays secure?

Tom:

So I think one of the big things that comes to mind is if you're providing guest access, treat it as a completely untrusted network. And that sounds obvious, but I think that's a pretty big one because guest networks by definition are open to let people use it. And you don't want someone to inadvertently be able to use that network to get to something they shouldn't. Likewise, on your guest network, if your wireless infrastructure supports mechanisms to separate clients and isolate them, you want to turn that on as well. So that one user can't access another user's traffic. I think on the corporate side of things, having authentication to the network in a way that's tied to the user, and not a shared key is important. And that way the user access is better controlled, and also something that someone could just post a password and anyone who has it can get on. But once someone's on the network using a VPN to access anything critical will provide an additional layer of security, and further tie the access to a specific user. And then finally having solid monitoring and alerting around your wireless infrastructure to detect issues and also monitor user behavior can help not only troubleshoot problems, but also isolate potential issues as well.

Roxy:

Something else that you'll want to do is create guidelines about how your users should be using the wifi, what they should and shouldn't be doing. Do you have a bring your own device policy, that kind of thing. Create guidelines and then make sure that the policies are published and somewhere where employees can access them and that they are educated on the policies upon starting at the company and then periodically or as the policies change.

Tom:

Also, to think as part of your security awareness training, having some information about wireless for your employees is not a bad idea.

Heather:

All right. And that's all for wireless security. Be sure to look at our links, to see our checklist of wireless security strategies that we've talked about today, and we'll catch you next time. Until then, stay safe.

This transcript was exported on Dec 17, 2021 - view latest version here.