Tim Medin (00:08):

... Quick you want to pull the slides up. I'll give you the quick intro. Because one of the rules I've always heard is never introduce yourself if somebody else will do it for you. So we actually have the whole team here. We've got Corey, Mike and myself.

I'll start doing reverse orders to set Corey up. My name is Tim Medin I am one of the folks here at Red Siege. I've been pen testing for a long time. Teach [inaudible 00:00:35] a bunch of stuff like that. Up there are northern representative, the pretty face. We got Mike Saunders, Mike's been pen testing for quite a long time. And then we also of course, we've got Corey here. So Corey's been pen testing for a number of years. He's been with us for... Actually his anniversary is yesterday. Congratulations, everybody, it's Corey, hopefully he'll make it to year three, we'll see.

Congratulations to Corey for that. But Corey came to us, he worked for another pen test firm actually a couple of different ones over the years, very skilled. He's going to walk us through some of the basics of reconnaissance here, some reconnaissance 101. It's always important you're doing a pen test, get some of that basic information about your targets, define that to we got user accounts and Corey is going to rip through that.

We were talking about this beforehand. A quick little story about Corey here. So Corey was sort of prepping these blog posts. There's actually some blog posts, we'll post the links once again in discord redsiege.com/discord. But he was doing some reconnaissance on a company that was essentially defunct and we're trying to post information about a company but not leak too much information. So everybody knows.

And trying to demonstrate OSINT without leaking too much and actually having it be useful at the same time is an interesting scenario. So it was a definitely some good times there. So with that, I'm going to turn it over to Corey so get ready for Corey again if you've got questions redsiege.com/discord, we will pop in and feed those [inaudible 00:02:19] Corey.

Corey Overstreet (02:22):

So we'll jump right in. So for the overview here, there's really two different kinds of recon, there's passive recon and there's active recon. Passive recon is where the target has little to no idea that you're collecting any information on them. Open source intelligence or OSINT would definitely fall in this category. When we get down to the automated OSINT, depending on how they find subdomains or how they interact with the DNS servers for the target, that can start moving into active recon, but it's still usually pretty quiet. And then active recon would be actively interacting with the services for your target. So that would be things that would show up on logs if someone's watching.

So we'll start with open source intelligence on infrastructure. This would be looking for sub domains, looking for information about the services that are available on the internet. Usually, where we start would be Wikipedia. A lot of times the company that has a profile page on Wikipedia, you can find their domain name, you can find information about their mergers and acquisitions. And why that's important would be you could actually see previous companies where there might be legacy infrastructure still laying around. Infrastructure that would have been for the previous companies before they were merged into your current target. And then there again like I said domain names, a lot of times you can infer domain names just from the names of the companies if they're not immediately obvious in the Wikipedia article.

So usually that's pretty high level, but it does give you a lot of information. However, our next stop is usually DNSdumpster. This site just about everything that they offer, will give you some bit of information to help with the next steps of the engagement. So usually the MX records will show spam or malware filters. This will give you an idea of what kind of trouble you're going to have during phishing. Also, what kind of payloads will typically get by if you do have to attach directly to the email and then after that we look at the ASNs. These are typically the IP address net blocks that would be associated with the company. And it's usually a dead giveaway if their name is in the ASN that they own everything in that IP range.

So even if you don't find subdomains that are attached to every IP address in that net block, you can find other infrastructure that may not have domain name and still be fairly confident that it belongs to that company. And then the A records show you the IP addresses and subdomains. There again, you can take the IP addresses and start kind of looking at the neighbors in that IP net block and figuring out other infrastructure that they may have that may not be immediately obvious.

So once we've gone through there, we go to the Hurricane Electric BGP tool kit. This is a website that has tons of information about the net blocks that you find from the ASNs. Once you find these net blocks, you can go through each IP address and look at and confirm that the IP address is still the same through their service that you saw with DNSdumpster. But it'll also show DNS history for IP addresses.

So if the company rebranded, if they changed IP addresses for their main site to another IP address, this is often an easy way to start detailing the history of the DNS so that you might find additional domains or domain names that belong to this company. I was on a red team a few months back and we were able to find their domain easily enough through Wikipedia. We started profiling employee names we found built up a huge list and realized that they were doing all their email through Office 365. So we started going through and spraying to see if the email addresses were valid and if we had the right format, but every single one of them were coming back as invalid.

So we started digging through DNSdumpster and the hurricane electric sites. And we stumbled across a domain name that they had, had before they had rebranded. And when we went back and fed that same list back to Office 365 with the domain before they had rebranded all of a sudden every single one of them we had were valid. And that was an easy way to kind of enumerate what their email domain was at that point.

All right. So usually after we've done a recon through those sites, we move over to Shodan. Usually Shodan has fairly up to date port scans information about the host. So usually you can find all of, I guess the traffic that was recorded when they interacted with the service. So if it was an FTP service a lot of times you'll see the interaction or the response that was returned by the server. With web servers within any service that they put out there, Shodan usually catches them. They also have SSL certificate information. So a lot of times if their SSL certs are getting ready to expire, that might help with a phishing campaign if you want to stand up something close to it, but with an invalid cert, you can also find additional domain names using that.

And then finally, it usually gives a pretty accurate geolocation of the IP address. So say you're going through a net block, you find a few hosts that are associated or in their net block. But you start looking and realize that most of this infrastructure is nowhere near where the company is based out of, it kind of gives you an idea of is this owned by the ISP, or is it owned by the actual company?

Also, you can start determining what kind of stuff they're keeping on prem and what kind of stuff they've moved to the cloud or to some third party service. And then next week, we start going and digging into the SSL certs. Censys.io and crt.sh are great sites for researching what kind of SSL certs they have. A lot of times too with both sites, you can actually find certificates for sites that they may have decommissioned or move to a different place. So it can kind of give you an idea of when the last time that infrastructure was recorded as being online.

There again, you can start enumerating additional subdomains for that company. And you can also find expired SSL certificates. Now, it's not always common to find expired SSL certs. But if it is a service that the company uses pretty heavily, and it's got an expired SSL cert, you could actually use that as part of your social engineering, where if a user has to continually except that the SSL cert is expired, when you stand up something that's also like a self signed cert or something like that, the user would probably click on through and accept that as being a valid host in your phishing campaign.

Another great site is SpyOnWeb. There again, this is a DNS history, but you can do it by IP address or by domain name. So there again, we had a red team where they had rebranded, but they had also acquired something like 35 or 36 companies in the last 10 years. So while we were going through, we started finding all these additional companies that they had acquired, and we were finding the domain names through that. So when we started researching the company, we started finding that all of these domains once we landed inside their network, and we started working through we started actually finding the windows active directory domains that were tied to these domains that we found externally. And we were actually able to move into areas where our points of contact they had never accessed any of that infrastructure.

And we were able to move around through areas of their network where they actually had no visibility, our points of contact, because it was being handled by another group that once they had acquired them, they were trying to keep those functions separate. So they were not getting any kind of feedback on the actions we were doing in that area of the network, and it was allowing us to keep a foothold in the network. So if we got kicked out anywhere else, we actually still had a way back in.

So I created SpyOnWeb in this because we were actually able to find almost 12 active directory domains that our points of contact had never interacted with and then next, we use archive.org. Otherwise known as the Wayback Machine. They usually have pretty accurate moment in time copies of the site. And you can use tools to download a full version of that site. And then you can parse through it offline so that you're not actually interacting with the client or the target site. But you are able to go through their website as if you were anyone else on the internet. And also, another way we use this is once we've downloaded the site, we can stand it up on our phishing domain, and get categorized that way and oftentimes get categorized the same way that the target sites are. And we can use that as our platform to launch payloads or just for our phishing landing pages.

And then finally, we look through job listings, Google, Glassdoor, Indeed, Monster, Zip Recruiter. Employers love to list all the technologies that they use, because they want qualified candidates that are trained on the stuff that they're going to be using. But oftentimes too, as an attacker, we can look through that same list and glean a huge amount of information, like the antivirus, the EDR, malware and spam filters, what kind of environment it is, if it's Windows, Mac, Linux. And we can also figure out what kind of... A lot of times you can figure out what kind of infrastructure they use internally, what kind of programming languages they use, if they're building like internal apps, that kind of thing. So you can get a huge amount of information just from the job listings that they post. All right, so before we move on to employees, Tim, Mike, did you guys have anything to add to that?

Mike Saunders (14:56):

No you're crushing it.

Corey Overstreet (15:01):

All right, so next we would move on to looking for open source intelligence on employees. We're looking for names, we're looking for email addresses, anything we can figure out that would aid us in social engineering efforts. And usually there again, our first stop will be Wikipedia, we'd want to know who the sea levels are, the board members, a lot of times in a red team, a lot of times these guys are off limits, but if they're not, they usually have a lot of power inside the network as well. So or using their names as a pretext against someone else usually gets actions pretty quickly. However, that's usually pretty risky as well, because people are going to be watching for emails impersonating them, but it is good information to have.

Another great thing you can get from Wikipedia would be recent awards and recognition. This would be things like we're celebrating our 50th anniversary as a company. We just got voted number one in customer service, things like that. These things are awesome for phishing pretext. You can use that to a lot of times we'll use something similar to that where like, hey, we pretend we're a third party company saying, "Hey, we're working with you guys as organization, we're throwing a banquet to celebrate your recent award. Here, open this invitation sign up and we'll make sure that you and your family are RSVP'd." You can get a ton of phishing pretext just from looking through a company's Wikipedia or googling for what kind of awards and recognition they've recently received. And then you can also look at the company history.

So if the company history is indicating that they're growing at an exponential rate there again, that's another pretext you can use as a congratulations. And you know we've had a lot of success using those kind of pretext to get our initial foothold into a company. And then our next stop is usually hunter.io. Now this site performs a lot of OSINT on their own, they collect email addresses, employee names, sometimes they get the title and phone number with them as well.

But one of the biggest things too is at the very top of the list, it gives you an email address format for the company, which helps a lot when you're searching for email addresses. Excuse me, when you're searching for email addresses online, and if you're trying to brute force them, you can often take lists of the most common first and last names and generate email addresses that way. So hunter.io is awesome. It's a free service. It gets rate limited a little bit if you use it too much, but for the most part, I've never really ran into that.

And then next is LinkedIn. It's just a huge wealth of information. It used to be, you could go to data.com and go to their connect service. And you could just get massive lists of every employee currently at a company. But they recently shuttered that service. I say recently, it's been like a year or two. So nowadays, LinkedIn is usually the best source for this kind of information.

Unfortunately, LinkedIn is... They've figured out that people are using it for that and they're profiling for cold call lists and stuff. So they've made it a little more difficult to just go on there, search for the company name and start pulling lists of employees. However, there are tools that can start pulling that information. The first would be LinkedIn. This tool by BySec, it scans through LinkedIn. Basically you give it the company name and it figures out the organization based off that and starts pulling any profiles it can find.

More and more recently, the results have been fewer and fewer. But you can still get usually a pretty decent amount of names and it pulls the name, the job title and the email address associated with that organization. Now there's another tool Peasant by Justin Angel of Black Hills. This has similar functionality to LinkedIn where it can search. But another great feature is it can also blanket a target organization with connection requests. So say you stand up a, I guess like a fake recruiter account. You can use that and start blanketing at an organization, and once you have enough connections with that organization, the rest of the list starts opening up. And then you can use Peasant to go right back in and download a list of all the employees email address, that kind of thing.

Now that feature is not purely OSINT at that point, because you are actively interacting with the target organization. But, I mean, we all get hundreds of these just throw away recruiter solicitations every week so, I would say you're fairly safe as long as you build the LinkedIn account correctly, but another way is to use the Gathercontacts, Burp add-on, I think Kerry Roberts made that.

So basically, what you would do is you would set Burp up, and you would configure the add-on and then you would go on Google or Bing, and you would search in LinkedIn for your target domain. And then it will automatically parse out the people's name, their email address, and a lot of times their title and any other information that came up on the cached results on Google or Bing. So that's a great way to gather them as well without actually interacting with their LinkedIn.

And then next, we usually go to the public breach data. You can go through Have I Been Pwned, Dehashed, Pastebin, and there's Torrents, you can get torrents of public breach data out there like the LinkedIn dumps, the MySpace dumps, or more recently, the collections one through five. We're not saying you need to download all this information, but it is out there if you want to grab it and typically you can get email addresses and passwords out of there. Now the passwords usually as soon as a company is notified that there's been a breach or that their addresses were in that breach, they usually force their users to start changing passwords.

However, you can also start noticing trends in the passwords if the users are using some kind of password that seems like it's related to the company that you're targeting. Sometimes you can find patterns that way. But you never know you might get lucky and actually find a user that's still using that same password from six years ago. It happens more than you would think.

All right, so that brings us to the end of that. We'll move on to automated OSINT. So with automated OSINT, these are tools that pretty much you just feed at the domain, you might feed it a few configurations such as maybe a few starting employee names or a few LinkedIn profiles, and you pretty much just click go and let it do its thing.

TheHarvester is usually a great tool. It searches through probably 15, 16 sources. And it does OSINT on infrastructure and employees. You can enhance the results that you get by adding I think it's like six or seven API keys. And I think only one of them's paid, the Shodan key, but it's pretty much set and forget OSINT, you pretty much point it at the domain, let it do its thing and let it spit out the results. But what I have noticed with theHarvester is that it will often get blocked by Google, because you're making too many requests to Google in too short of a time and their automated crawler detection will start kicking out your IP address.

So there's ways around that by using tools that will route your request through multiple sources. But for the most part, you'll get most of the results that you would have gotten regardless. So next is Amass. It's highly configurable. But a word of warning is Amass doesn't provide the configuration file by default, unless you clone it from GitHub. But I would highly recommend that you do because once you do, you can configure everything from which DNS servers they query, I think there's something like 50 different services that you can turn on or off depending on which ones you want to query. And I think it takes 16 API keys. I was able to get just about all of them relatively easily, it took a couple hours to sign up for all the services, and only a couple of them were paid.

But the only problem with the Amass is it only looks at infrastructure. So like subdomains, ASNs, CIDR ranges, it's mainly looking at what kind of infrastructure you have externally not for employee names or email addresses. But it can also do passive or active recon. So you can do passive where it looks at public sources for subdomain names, that kind of thing. But you can also do subdomain brute forcing with Amass. So you can basically just feed it a list of common subdomains and see if it finds anything that way. But it usually returns quite a few results.

And then finally, the recon-ng framework. It's a modular OSINT framework made by Tim Tomes. And what's great about it too is it has a marketplace. So you can actually pick which modules you want to include in your install. So you don't have to use every module that's ever been made. If you want it to be more singular in its focus, you just grab one or two modules and set it up to run towards that. You can also create your own modules. So if you don't find what you need to get what you need done, just make your own.

I believe it's all written in Python. So you can just make whatever module you need. And you can share it back with the community so other people can use it. And it also uses formatted reports. So at the very end, you can decide what kind of report you want it to return and give you all the information or you can search for the results using commands similar to the Metasploit Framework.

And another thing I forgot on here was the fact that you can script much like Metasploit, you can script the recon-ng. So, that it runs all the commands in the order you want them to run in. And basically at that point, once you have the script hammered out, you can use it much like theHarvester, where you just pretty much point it at a domain and let it go. So, that's another awesome feature.

All right. So once we've pretty much built a huge profile of whatever target we're going after, we can start kind of ramping up to some light interactions with the target. We still try not to just beat him over the head because we don't want... A lot of times we're not trying to tip them off that we're actually looking at anything on their network. So the next few techniques will be fairly light interactions with the target. So first up is EyeWitness tool by Chris Truncer over at FortyNorth Security.

It records interactions with web services VNC and RDP. So you can feed it a list of domain names, IP addresses, and you can actually pick which ports you want it to check for if those weren't immediately obvious from scans or other information you've gathered before then, but it'll take a screenshot of the service. And it will record any kind of headers or interactions with that service so that you can review those later. But you can also feed it an XML formatted in meta output, so that if you did run in map scans, you can just feed the XML output to that, and use that as your list of hosts to enumerate.

And then there again, it also provides a formatted report. So this would be something akin to it, it tells you what kind of 200 responses you got, 404s, 403 forbidden, that kind of thing. So that way also not just what kind of service you tried to reach, but what you're going to see if you try to reach it as well.

And then another technique we use is looking at file metadata. So this can often contain usernames, email addresses, operating systems and software suites. So in the metadata, let's say that the file was saved on a Windows computer, the file path would show us C colon users slash and then you've got a username there. And using that information, you can actually go ahead and start building username lists for once you land on the network, you have lists of users who you can convert the email addresses into usernames for further attacks once you get in, excuse me, but you can also get, what kind of operating systems they use, you can figure out if their Windows, Mac or Linux environment.

And the software suites used to create it. So if you're using Microsoft Office, if you're seeing Windows file paths in the metadata, you've got a pretty good idea of what kind of systems you're going to land on once you get in. Now, the only problem with this is you have to download the hosted files to get that metadata. So you can do it one of two ways, you can do it automated or manual. But either way, if there is a red or excuse me, a blue team watching, downloading a ton of files from the same IP address with cURL is going to start sticking out to them, possibly depending on how closely they're watching.

So for the automated route, you can use PowerMeta by dafthack. It's a bow over at Black Hills. This will automatically search Google and Bing for any kind of document, Docs, spreadsheets, PDFs. And then it uses another tool to extract the metadata to a comma separated spreadsheet. So it makes it a lot easier to kind of dig through and start looking at the columns so that you can start seeing what kind of usernames you have, what kind of file paths they were saved at in the metadata, that kind of thing. And then I also use a manual approach. I use the tool link clipper, it's a chrome add-on. And basically what you can do is save every URL link that you would find on a page. I will go to Google or Bing and I would use different search torques to target the domain that I'm looking at, and then look for every kind of file type.

So it'd be like file type colon PDF, dot doc, dot docx, that kind of thing. And then once I've kind of saved up a list of them, I start going through each search result page and downloading that list. Now I have noticed that if you try to up how many results show up on a page, you'll start running into the automated crawler detection for both Google and Bing. So I usually stick to 10 links per page. But I download all those CSVs and then I grip out the download URLs, and then throw them in a for loop in Linux, either cURL or Wget, but I try to throw a user agent on there that will look like a standard web or a standard web browser downloading those files and try to throw some kind of sleep between the requests.

So it's not just blasting the server and downloading everything all at once. And then I'll combine all the files that were downloaded through the manual methods and through the automatic methods, and then run the extract metadata using bows tool and pull the report from there.

Another interesting piece of recon is being able to actually pull the internal domain name for an active directory domain externally. So if they are using an on-prem ADFS site, a lot of times in the source code for that login page, there will be a little snippet of JavaScript code that will correct any submissions and say, "Hey, you forgot to put your domain name on there." And a lot of times it actually has the legit domain there. So if you access the ADFS site, you can actually look at the source and a lot of times find the internal domain name that it's expecting from there.

Now, they're becoming less and less common in my experience a lot of people are moving to the Azure ADFS, which is like your standard office.com kind of a login page. And those don't have the same thing. You oftentimes login with your email address and password from there. But they are still out there.

Another thing is the Outlook web access. Here you'd be looking for either the autodiscover or the EWS like the exchange web services area of OWA and from there, you can actually perform an NTLM authentication against their server. And when you do that, you can actually pull out the internal domain name and the name of the exchange server inside that NTLM authentication attempt. The only problem with this is when you do... If you just throw user and password at that. The only problem with it is it does also include your host name in the request.

So make sure that your host isn't giving away your name or your company that you're... I guess as part of your OPSEC, you don't want to give away any more information than you have to. And then there's also an automated Metasploit module, does the same thing. It makes the NTLM authentication request, but it only grips out the internal domain name. So if you want the name of the internal exchange server as well, it's a lot better to do it with cURL and just parsing through the NTLM authentication request that comes back.

And then finally, you can do third-party port scanning. The list of sites here all will perform port scanning against the target for free or for most of them for free. You can basically just point it at a domain or an IP address and the Geekflare, IPv6 scanner those two will usually look at just the top ports that are available. But T1 shopper will actually give you the full 65k, they ask you not to but I mean you can.

Now HackerTarget is a company that is actually part of DNS dumpster. They have full-on recon services where you can actually point it at a domain and it will return a lot of this information automatically for you. But there is a charge. I can't remember off the top of my head how much that cost, but it will do port scanning, it'll look for subdomains, it can do subdomain brute forcing. It has a lot of features, and then Shodan you can also ask it to get more up to date information. I haven't ever really ran into an issue though, where Shodan information was extremely outdated. Most of the time, they keep it fairly up to date.

So to summarize, a large part of this recon requires zero interaction with the target. You can build a huge profile of a company without ever sending the first packet or phishing email to them. Target organizations often provide a wealth of information. Everything from their job listings to the files that they released with metadata in them. And the services that are unnecessarily exposed to the internet, a lot of these things can give you information that gives you a huge advantage once you find the land in the network.

Automated recon is faster, but manual provides more control over timing and intensity. So if you're trying to go low and slow, if you're trying to fly under the radar, it's better to do the manual techniques. But if you're on a pen test, if you've got a week to figure all this out or even less, throw the automated stuff at it and 99% of what you get is going to be what you need.

And then we recommend too the defense should perform the same steps just to make sure that there's no unnecessary exposures that they have online. So you want to make sure that you're not giving away your internal domain name unless you just absolutely have to, or more email addresses than you really need. So the defense side should approach this the same way as the attacker should and that they're looking for anything that doesn't really necessarily have to be out there to be helpful. All right guys that brings us to the end. That's our team. See if I have any questions.

Mike Saunders (39:20):

I've been looking through the discord, I don't see any questions in discord or in GoToWebinar if you've got questions throw them up in one of the two. Take a look for that. I see a couple people typing in the discord. By the way folks, this was and if you didn't notice, this is actually or probably didn't notice. This is actually Corey's first ever like webcast presentation, whatever for security. Personally I thought he did a fantastic job. So way to go Corey.

Corey Overstreet (39:58):

Thanks.

Tim Medin (39:59):

Hopefully we get some more out of Corey's. Smart dude. Somebody posted yes. Now you've got some OSINT, you know his first name out of Red Siege. Yes. It's also on the website. Leaving internal email distribution list open to the interwebs is not great either. Absolutely, now there's of course there's business cases for some of that but I've definitely seen somewhere where I've know multiple organizations that have done that for like their entire employee mailing list, which is phenomenal for phishing. Great, Corey, of course. Fantastic. I don't see any-

Corey Overstreet (40:35):

Thanks [inaudible 00:40:36].

Mike Saunders (40:38):

Say I wanted to add something just to what Corey was saying about the OSINT. For testers, it depends on the kind of assessment you're doing. If you're doing something red teamy where you're supposed to be not getting caught. You're supposed to be trying to hide, using multiple sources for doing your testing is helpful. So have different machines that you can route your traffic through, whether it's a Digitalocean node that your proxy chaining through or any other kind of virtual server that you're running through. However, if it's not an assessment where you're trying to hide, doing it from one host, so that your client knows what your IP address is, is helpful because they can go after the fact and look at what you've done and correlate it to the traffic that you generated from your source IP.

And they can use that information to help build better detection be like, "Hey, if someone is actually crawling our site and pulling down all the files from metadata, then this is what it looks like." So using that single IP that's known and that you provide to your client for those kinds of instances is useful. If you're doing it for a red team type of assessment, keep track of what you did from which operating host so that, that information can be correlated back at the end of the engagement.

Corey Overstreet (42:09):

Hey, I wanted to address one of the questions I saw flagged by. The [inaudible 00:42:13] asked if this is my mom's basement. I get that a lot. So when my son was born last year, I gave up my office so that he would have a room and I had to move down to the basement. So we lovingly call it the dungeon but we've been looking for a house and we're actually closing next week on one so yay, I get sunshine again. So yeah, it's going to be great.

Tim Medin (42:44):

All right, I don't see any other questions coming in. Any other thoughts or comments? Anyone? By the way, if you guys... Go ahead, Mike.

Mike Saunders (42:54):

I see a question from Cactus about would you email employees for social engineering to gain more information? Absolutely, that can be something that you can do. Emailing employees, I have heard of some really devious red teams that long play using things like third party support. Like let's say you figured out your customer is, I don't know a Dell customer. Using the Dell support forums to build a relationship with your customer. That's a very long play type of social engineering, but that could be effective.

Tim Medin (43:39):

Yeah, cool. So MGO asks a question, what is an OSINT related report look like? So we don't have an example of that. I don't know if there's anything out there. We put that as part of our methodology kind of document that. Everything's sort of publicly available and the hard part is, if you're releasing OSINT information to redacting that, but still making it useful, and it's down near impossible, because you'll leave enough pieces there where someone could put couple of pieces together and figure out what the original thing is. It's a tough game, and I don't know a great way to do that. The only other way is to OSINT yourself but then you know all the answers and it feels like cheating, sort of, in my opinion.

We're calling it a service desk or help desk. Yeah, I've done that before with red teams. Calling like, "Hey, sorry, my computer's taking a while to load, to give me the information. I think it's my antivirus. Mine's terrible. Which one are you guys using?" I used that in the past to get that kind of information. So cool. Any more question... I see a few people typing. By the way, if you want to reach out to us, if you've got any questions, you want to talk to somebody, one of us here at Red Siege. Once you're in the chat or in the questions, just type Red Siege and we will dig through the email and reach out to you if you have questions about services and such.

Another question, are there dark web marketplaces for OSINT info on potential targets? I don't have a good answer for that. I mean, I'm sure there's some. I mean, the breached password information is definitely there. Anybody else got info on that?

Mike Saunders (45:26):

Not I.

Corey Overstreet (45:28):

Yeah, I haven't seen anything like that. But it's something to look for now.

Tim Medin (45:32):

Yeah, exactly.

Mike Saunders (45:35):

So GMFD asked about when we're preparing to do phishing campaigns is there a way to see if we're getting caught? And there is a source and I cannot think of what it's called the site that we've used to gauge the effectiveness of our message, do you remember that Corey? Gives you a score? [inaudible 00:46:01], I know you guys over at Black Hills have talked about that tool before. If you're still on. Happen to know-

Speaker 4 (46:14):

I didn't it would be important to find it. I can't remember the name.

Corey Overstreet (46:17):

I know which one you're talking about, but I can't think of the name of it right off.

Mike Saunders (46:21):

Yeah, I can see it in my head. But there are tools that you can use, it'll help you tell you if you have things wrong, like DKIM and DMARC. All of those kinds of things about your email will also tell you how spammy it thinks your message is, you can actually give it a template of your message. Other things that you can try doing is if you can profile where your client, where their email lives. For instance, if they're an Office 365 customer, you can set up Office 365 really cheaply, buy a domain over at GoDaddy. Sign up for a one month trial of Office 365 for five bucks and then email yourself and see, does it get delivered? If it does get delivered, look at the headers and see the Microsoft anti spam headers that are in there how it scores that can give you some information. MxToolbox I believe that is a... I believe but I could be wrong. I am wrong.

Tim Medin (47:26):

I've used that before I can't remember-

Mike Saunders (47:27):

That is a useful tool, but it is not the one I'm thinking of.

Tim Medin (47:27):

Yeah, it's not one I'm thinking of either.

Corey Overstreet (47:34):

Yeah, Ctrl K asked if we see net blocks that are ISPs, would those be considered in scope? Typically, we try to avoid that. That would be one of the reasons we would use the geolocation data from Shodan is to try and kind of rule out devices that wouldn't necessarily be owned by the client so that we're not just attacking an ISP and kind of muddy in the water real bad.

Mike Saunders (48:04):

The answer to my question was male tester, male dash tester. I just put it in the chat.

Corey Overstreet (48:21):

Zeller asked if there was a workaround for the recently disabled paste in search feature. I'd have to find the site. I'll throw it up in discord in a bit. But there's actually a site that searches a bunch of different paste in sites. And I've used it a lot in the past to kind of troll through a bunch of paste in sites all at once. I'll have to look through my bookmarks and find it.

Mike Saunders (48:50):

I haven't tested this but I believe if you have a Pastebin PRO account you get an API key, you get API access and the scraping API has been disabled. But the Search API has not been disabled. So you should still be able to use API access to search.

Corey Overstreet (49:13):

I'm not seeing any other questions there at all.

Tim Medin (49:18):

I think that's going to wrap us up. I don't see any other questions. Get your questions in quickly if need be. Again, if you want us to contact you, type Red Siege in the goto chat, of course you can reach out to us in the discordredsiege.com/discord. With that, I want to thank you guys for coming. Again thank you, Corey for a fantastic presentation. Keep an eye out. We are going to be doing some more of these. We're all going to be at home for a little bit probably still. So we'll have some more free info out there for you. But with that, I'm going to thank you guys all for attending and have a good day and a good weekend.

REDSIEGE
INFORMATION SECURITY

CONTACT:

+1.234.249.1337
contact@redsiege.com
@redsiege
@rsiege
/redsiege

OUR SERVICES:

ASSUMED BREACH ASSESSMENT

RED TEAM AND ADVERSARY EMULATION

PENETRATION TESTING

WEB APPLICATION PENETRATION TESTING

PURPLE TEAM

MOBILE APP ASSESSMENT