

Forum:[Hack Forums](#)

Thread: [Putting the Infra in your Structure \[REDTEAM\]](#)

CyberStrike - October 25, 2017, 1:40 pm

Foreword: I have been seeing a few threads recently where with the proper infrastructure the poster would not have such hurdles to jump over. Make your day easier by having the correct infrastructure in place. I suggest strongly that you read the RedTeam Structure Tutorial to have a full grasp on the ideas being presented.

RedTeam Infrastructure (Maintained by Infrastructure Team)PhishingServerTeam
(Payload)ServersCommand and Control (C2)Ex-filtration Server

Building Domain Reputation:

Imagine the following scenario, have spent the past two weeks researching a client and the client's employees for a pentest. Part of the scope of this engagement is phishing, will your phishing campaign be successful? Will your emails actually reach the target or will they be filtered by and ISP or maybe through a spam filter? So how do you give yourself the greatest chance for launching a successful phishing campaign?

Building a domain's reputation is important for having a successful phishing campaign during an engagement. You maybe asking yourself "Domains have a reputation?" Yes they do often domains where lots of spam originates from is blacklisted, and administrators often will block these IP's automatically. Domain Reputation determines if your email will actually reach the intended recipient, in the future when IPv6 is more accepted then it will be based on IP Reputation with Google spearheading the push to accept IP based reputation for ensuring that your email will reach the intended target. Currently however domain reputation and some IP reputation is used although Domain is more prevalent. Currently there is a mix of IP and domain reputation being the deciding factor as to deciding if your emails are filtered. Having a legitimacy to your domain is important I suggest having CaaS provider (Content as a Service) to have a legit looking website and thus domain.

Using a VPS on a cloud platform is suggested as it will give you more control over your infrastructure but yet with the protections of your provider. By having legit content and buiding up your domain's reputation this will help when we go ahead and create our C2 server.

First and foremost you will want to only do small campaigns less that 1500 emails per week, in addition you will be creating a sub domain to launch all of your phishing campaigns from, also this sub domain it's only function will be for sending emails from. Also you will want to be consistent as to when you start these campaigns, having a schedule and staying within the limits set forth will greatly increase your chances of success.

Second we will want to appear secure as well as legitimate, for this we will implement a few security feel goods. First you will want to spend money on an SSL certificate from a legitimate issuer of SSL certificates. Second on our server we will implement SPF (Sender Policy Framework) in our DNS, as well as using TLS. Next we register with McAfee Secure thus getting out "Trust Mark", which is for free. Next we need a code signing certificate, sign your malware with a certificate amazing how that works to get your backdoors through AV, this is note too expensive and if you are doing

engagements often then this will be very helpful.

Another thing to pay attention to is emails being bounced back so updating your lists and verifying target emails is crucial for keeping up your sender score. What is a sender score? The sender score is from 1-100, of course 1 is pretty bad and 100 is pretty stellar. Now there are sites such as senderscore[.]com . Also check if your IP has been blacklisted, as in the introduction we know that currently a mixture of Domain and IP Reputation is being used in order to filter emails. Another thing to pay attention to is the silly “free” or “winning” type emails you are targeting a specific target not mass emailing a facebook group with cat pictures. So good information gathering is important which has been discussed above.

Typically in a corporate environment you can garner many people wanting to see new rules, as no one wants to get fired. What good employee wouldn't click an email titled “New Sexual Harassment Policy” with a nice PDF,

BiometriX - October 26, 2017, 12:34 am

Hi sirru5h,

great post! Thanks for sharing your experience and the quality content you provided.
Keep up posting ;)

Greetz BiometriX

CyberStrike - October 26, 2017, 12:43 am

Steps to conducting a successful Phishing Campaign:

Now that we have built up our domain and have the right infrastructure in place it is time to get to work. What do people care about? What attracts people to click on a link or open an email? Well they are people they are motivated by the simple things greed, sex, interests such as hobbies, family, and other things, which you have discovered during your information gathering. If we are to mimic the domain of a target, typo-squatting for example our target is windows[.]com . Well lets think we have a few options vwindows[.]com to a user looking quickly it looks passable we can also use various other UTF's to get around this instead of UTF-8. Either way once we have a passable domain well we need to get their attention perhaps we can send an email from [email=hr@vwindows]hr@vwindows[/email][.]com and our subject “New Sexual Harrasment Policy” or maybe “Fire Drill Today” . These two subjects deal which concern the user here and now. No one wants to accidentally break the rules if they want to keep their job, and the second email deals with the self perservation and that unknown factor of a surprise fire drill where in the target will want to know the procedure as not too look like a fool. Even something like “Want to go for drinks after work” will garner a look as we are working off of a targets willingness for social acceptance. Of course for this to work we would have to know a user at the target or perhaps these people mix their private life with their work life. This is where something like TheHarvester to see if a target is using their work email to sign up for websites. If this is so then perhaps since we have looked at the target's personal social media what if their significant other sent this email. Maybe it can have a link for a bar that sender just discovered, of course this is a fake domain and fake content which of course is ours and using our code signed Java applet to gain entry to the target's work machine.

Team (Payload) Server:

Team Servers? Yes Pentesting and Red Teams are a team event. Using even Metasploit Framework you can have a team server where all users can connect using msfrpc and if you are into cli you can run msfrpc-client to connect to the team server. One may even use Armitage to connect to the team server. While red teaming is often chaotic you can chat much like you would in IRC, in addition sharing of sessions is possible, of course you must remember whatever the first

command issued is the first to be processed. Generally if we look at the Red Team Structure we probably would want our Access Team working in our payload server, of course we will want to have one member of our Post Exploitation Team for dealing with more difficult machines and for hand off this machine providing it is and has been identified as either a high value target or has some sort of infrastructure support feature to on going operations in the target network to be handed off to our C2. The Access team if we remember their job is to get us access and our Post Exploitation Team in conjunction with the Infrastructure Team will be escalating privileges and post exploitation outlined in the Red Team Structure section above. Of course the Infrastructure Team is responsible for ensuring that Red Team infrastructure is fully operational such as the payload server and C2 as well as ensuring that the target machines and network is held by the Red Team. One thing to note is the number of threads being dedicated to a scan for example, too many threads can cause a crash of PostgreSQL.

C2 & Redirects & Xfil:

The C2 is maintained by the Infrastructure Team and is home to both Post Exploitation and Infrastructure Teams, and will be where most of the work is done. There are several options even using Metasploit as a C2 where there would be server other than the payload server is an option, but for ease of use FruityC2 works listening to multiple payloads and is free. FruityC2 uses a web interface it has a very sleek interface dealing with creation of new payloads and allows one to issue commands to multiple clients. PoshC2 is another option and as the name implies it is Powershell based and is quite light weight so it can be deployed in either Windows or Linux, as Linux does have Powershell. It should be noted that even if you use Metasploit as your C2 you may issue commands to multiple sessions. There are multiple C2 servers which one may use including. Another thing to note is that due to our domain being legit and it being either a VPS or a dedicated server we can have our backdoors, which are reverse https connect to that machine with our legit domain that will forward traffic to our sub domain for the C2. Even if the Administrator is looking at the traffic it will look legit since we have content, we have our McAfee Trust Certification logo, and we are using a legit SSL certificate. Also the communication is on the correct port for legitimate communications. Let's say that our administrator is a bit nosy well too bad it is encrypted. Part of the trick here as well is going to be not standing out when it comes to how much traffic is being sent out backdoors can be scheduled to contact back to our C2 at irregular times and during peak hours, I am sure that 20 machines all beaconing back for their instructions at the same time say 0300 would be suspicious at the least. So varying times and having different times for machines to beacon back say twice a day is good to keep suspicions down from a nosy administrator on the target network.

Redirection can also be used for example SOHO devices such as DDWRT routers are a good target to help hide your IP. Let us say that we have several of these DDWRT routers, on different IPs, as they are cheap to purchase and do not have a persistent memory. These SOHO devices do not save the pre-routing or the IP Tables configs so after a reboot there is no trace of our activities on the device. Before ex-filtration we must take a few steps. Firstly in the target network no one machine should be sending out 5 Gigabytes of data so you would want to split up the number of machines within the target network which would be like a set of staging servers for all of the data to be ex-filtrated to our ex-filtration machine. If we gain root on these SOHO devices, then proceed to setup forwarding from our target IP range to our ex-filtration server once again on our legit domain, and perhaps a few other legitimate domains hosted on VPSs or dedicated servers we can split up the amount of traffic being sent. These SOHO devices do not save the pre-routing or the IP Tables configs so after a reboot there is no trace of our activities on the device.

Red Team Mindset:

Understanding how your target functions, how administrators function, and how users function is important. So if our target is for example a software company do we really need domain or enterprise admin? Probably not what if we were able to get into their Dev Ops server where they have source code for their newest software. Is that serious? Darn right it is serious! What about if that data is stolen and sold off to a competitor? What if we get a hold of their pricing for an upcoming bid for a contract? All of these a client would lose money. And generally that is what management will be looking at. Most of the current attacks carried out that we hear about in the news are not sophisticated. Of course no one will admit "I am dumb and didn't patch" or "I am dumb and I just disabled security settings because a perspective client said to run that file". Yet this is pretty close to the level of "sophistication" it takes sometimes to get into a target. The only things that stop you from doing things other than legalities is the scope set forth by a client. Does the client do themselves a favor when they deem infrastructure as critical and it is off limits? Maybe, but not many people offering a free pentest, illegally of course, would care and would target these systems. So we have an environment where the most important targets in a network are not being tested. While now many times we see companies only wishing to be PCI compliant with a checklist and you end up with a 40 hour pentest and really it is 32 hours and 8 hours of writing up your report, you are taking away from the client only giving them what they need, but not what will protect them against a determined attacker.

The mind set of an attacker has to be one of deliberate action, nothing is pointless. A good way to always stay focus is by using "OODA". First we Observe then we Orient next we Decide and last we Act. So what does this mean? If we see a target that has important information we start to formulate our game plan, we may have more than one idea of how to get into that target, we need to have a solid plan and we decide based upon the best information we have, then we act on our plan of attack. Always being ready to do awesome things with whatever resources we have at our disposal. One thing that I rarely see is a pentester showing up and paying attention during the meeting where the sales representative is there getting the contract, I encourage you to go and see your client. This is a chance for you to scope out the target before the engagement.

When cracking passwords make sure pay attention if you got clear text passwords in a file, and integrate them into your dictionary when you are cracking passwords, they maybe the password you are trying to crack. Also in Windows pay attention to the registry as it is a gold mine for information and the only logging generally is if a change had occurred. It should be noted that Microsoft offers an Excel spreadsheet which gives us each group setting for each version of windows and where they are located in the registry. Also the Windows Event log is worth a look. These are things often that people neglect they are busy trying to get how ever many sessions and they want to exploit them all, instead target the important high value targets. Also you don't have to escalate privileges all the time if you can install a key logger or tshark then why would you waste your time? This is part of being oriented and deciding as to how much work you need to do in order to be successful, and thus act upon the information.

Above all remember:

Stay Purposeful
Be Resourceful
Win

I broke up the post and changed the font color to make it easier to read. Thank you for the good words of encouragement.

lwristis - December 11, 2017, 1:02 pm

Incredible release from sirru5h. Someone give this man a medal or an upgrade.

CyberStrike - December 11, 2017, 2:47 pm

lol, Thank you this is old but did you read the article I showed you? Almost the same ideas, except to deliver payloads they are using google drive and all that jazz to get around reputation filters.

/wrists - December 11, 2017, 3:27 pm

Yes, pretty fucking amazing read.

CyberStrike - December 11, 2017, 3:32 pm

I thought you'd like it, once you got the right infrastructure in place everything tends to go pretty quick and much less painless.

/wrists - December 11, 2017, 3:33 pm

As with anything. The right order is essential.

SheSmokes - September 28, 2018, 3:23 pm

Could I include a link to this thread in my thread? It's informative.