

Forum:[Hack Forums](#)

Thread: [Red Team Structure \(Post Exploitation\)](#)

CyberStrike - October 1, 2017, 5:53 pm

Red Team Structure For Post Exploitation:

As many of us know during an engagement especially with a large client the work load would be a bit daunting for one person, and with a time crunch of deadlines set forth by a client (and your boss) it needs to be a multi-person event. This is pretty close to how I like my post exploitation teams to be at the very least three people, usually four, no more than eight. The following is a break down of each team and responsibilities/duties. In addition targets for monitoring after successfully taking over the network.

(Quick disclaimer some of these tactics may not be in the scope set out by the client of course respect their wishes. eg: phishing using compromised employee credentials or changing configurations)

Teams:

We require three teams with various roles and duties.

Access Team

1. Access Team

1. Get foothold onto target
2. Expand Foothold

The Access Team has the duty of getting toe holds and foot holds onto network machines and assets. It is important that the Access Team have the tools which they want and are maintained by the Infrastructure Team. There should be no target network information left on the target network and this information should be kept off site to limit damage if target network resources are reclaimed by IT staff.

Post Exploitation

2. Post Exploitation Team

1. Data Mining
2. Monitor Users
3. Keylogging
4. Information Gathering

Monitoring the network (Post Exploitation Team) is important as to discover various important factors in the target network. Using Tshark/Wireshark on a compromised machine on the network is one of the best ways to do this so the pcap file can be saved and analyzed later. What we are looking for is passwords, protocols, and times of high traffic. Active Directory and other protocols such as NTLM send passwords over the network which can be intercepted and cracked offline. The protocols in use in a network can show what other services and network resources are being utilized on a target network, and give the Access Team the data they need in order to further attack the network and resources. Times of increased network activity can help hide attacks and scans with in

the target network. In addition xfil of data should be done when at a slow rate when network traffic is high as not to attract attention by slowing down network services on a target network. During non-peak times the xfil of data can be sped up just a fraction as not to attract attention. It is important that IT staff of the target network are monitored as to when they log in (date/time) also if the IT staff is logging in remotely into the network during network problems, when they are not on duty.

3. Infrastructure Team

1. Maintains Access
2. Manages Resources held on target networks
3. Persistence on targets
4. Setup infrastructure for further attacks

Infrastructure:

1. Tools for further attacks
2. Email/phishing servers
3. Target specific payloads
4. Facilitate Xfil of data
5. Redirects to servers

The Infrastructure Team is responsible for many duties to ensure a successful engagement. Tools to continue an attack should be placed on compromised machines around the network. Tools which will be required maybe flagged as a virus so antivirus must be disabled as well as UAC. Since most antiviruses that detect certain tools and flag it as a virus, and UAC would allow you to install the tools needed. Nmap should be placed on non-payload servers so if the traffic was to attract attention the administrator would focus on the machines doing the scans. A compromised email server can and should be used for active phishing attacks, using valid emails of management and IT staff of the target. Payloads to attack a network or resources also should be kept on a seperate machine in the network, the payload server. Data being xfil'd should also be stored on multiple machines which have no resources.tools already being used or that are critical to further expansion of the network resources an Access Team is going to be utilizing. Data to be xfil'd is kept on several machines throughout the network for staging so even if one is lost not all data being xfil'd is lost. Another thing to pay attention to is not sending too much data out and attracting attention by the amount of bandwidth being used, hence also why multiple machines would disperse the traffic and be less noticeable. Having machines that redirect traffic would help hide the machines that are being used for attacks and scans. IP Forwarding on Windows is easily accomplished and should be utilized. Generally xfil'd data will be sent to a VPS with a built up legitimate domain that there would be no reason for filtering to occur. In addition on xfil'd data must be encrypted before transfer, perhaps even compressed unless.

Team Communication

Team communications are important in order to ensure that everyone is on task as other teams will be depending on your work. For communications we may use a company/private IRC server with SSL/TLS which is internal facing and accessed through VPN. Also each team will be having their own respective channel in larger teams for smaller teams one channel maybe used. Files xfil'd will be shared by the team in a repository which all team members have access to on company server for the specific engagement. Dradis is required as tasks and information can be shared and marked off by team members after completion, also hosted within the company servers.

The importance of strong communications is very important to the success of an engagement of a target and subsequently of the network and resources. Each team will have a leader who is responsible for ensuring team members are performing duties. In addition the team leaders will be

reporting to the Engagement Leader, who will be in charge of all operations and ensuring that duties are carried out.

Targets for monitoring:

Targets:

1. IT Staff
2. Management

Monitoring of IT Staff is required to prevent detection, as well any possible password changes, new configurations, also preempting any possible actions by IT Staff to re-take gains with in the target network. Management is to be monitored for business intelligence as well as their other activities.

Methods for monitoring include keyloggers, remote access tools, and monitoring of emails and personal work communication of targets. At each network segment there must be two computers setup with wireshark and logging all data. Any computer which is multi-homed must also be monitored using a packet capture software. All files such as keylogger and pcap files will be xfil'd daily and before deployment a sha256 hash of the file must be noted as well as the machine that will be hosting the file/tool. You will have to stop tshark/keylogger then copy the file to your local machine then delete the file from the target machine, and finish by restarting the service tshark/keylogger.

Edit: More on post exploitation Infrastructure and Post Exploitation will follow. Hope you all enjoy.

Moralitas - December 27, 2017, 3:04 pm

How long are your engagements? 4 people should be maximum, 8 is way too much. Also dividing teams by pre and post exploitation doesn't seem like a very efficient way to run a red team. Why not train the access people to also do the post exploitation?

CyberStrike - December 27, 2017, 5:51 pm

(Dec 27, 2017 04:04 PM)Moralitas Wrote: [\[CITE\]](#) How long are your engagements? 4 people should be maximum, 8 is way too much. Also dividing teams by pre and post exploitation doesn't seem like a very efficient way to run a red team. Why not train the access people to also do the post exploitation?

Engagement length can really vary from 1 week to one month, usually two weeks is good sometimes contracts stipulate "holding" onto resources. 4 people is really that optimal number too many people means people are not being productive and ends up being inefficient. I agree it is best to have people say in the access team go ahead and complete post exploitation, but if it comes as a trade off between the time spent doing post exploitation and having momentum in the attack. For example if say for persistence we are going to be using application shimming, to stay a bit below the radar, and the Administrator account has not fallen it would be better to have the access team continue on to other machines, expanding our foothold. Perhaps they may get the machine where the Admin may have logged in or we are able to capture a HVT (account/machine) so we can continue on.

Moralitas - December 27, 2017, 9:11 pm

Your engagements are pretty short. It's a bit unrealistic IMO to do a full adversary emulation in less than a month. I'm guessing you're on a consulting company's red team. Anyway thanks for sharing.

CyberStrike - December 28, 2017, 1:38 am

Pretty much you hit the nail on the head, down the road I would actually like to start up my own company doing full on long term pentests and adversarial simulations. I appreciate you taking the time to read and I appreciate the feed back, thank you.

