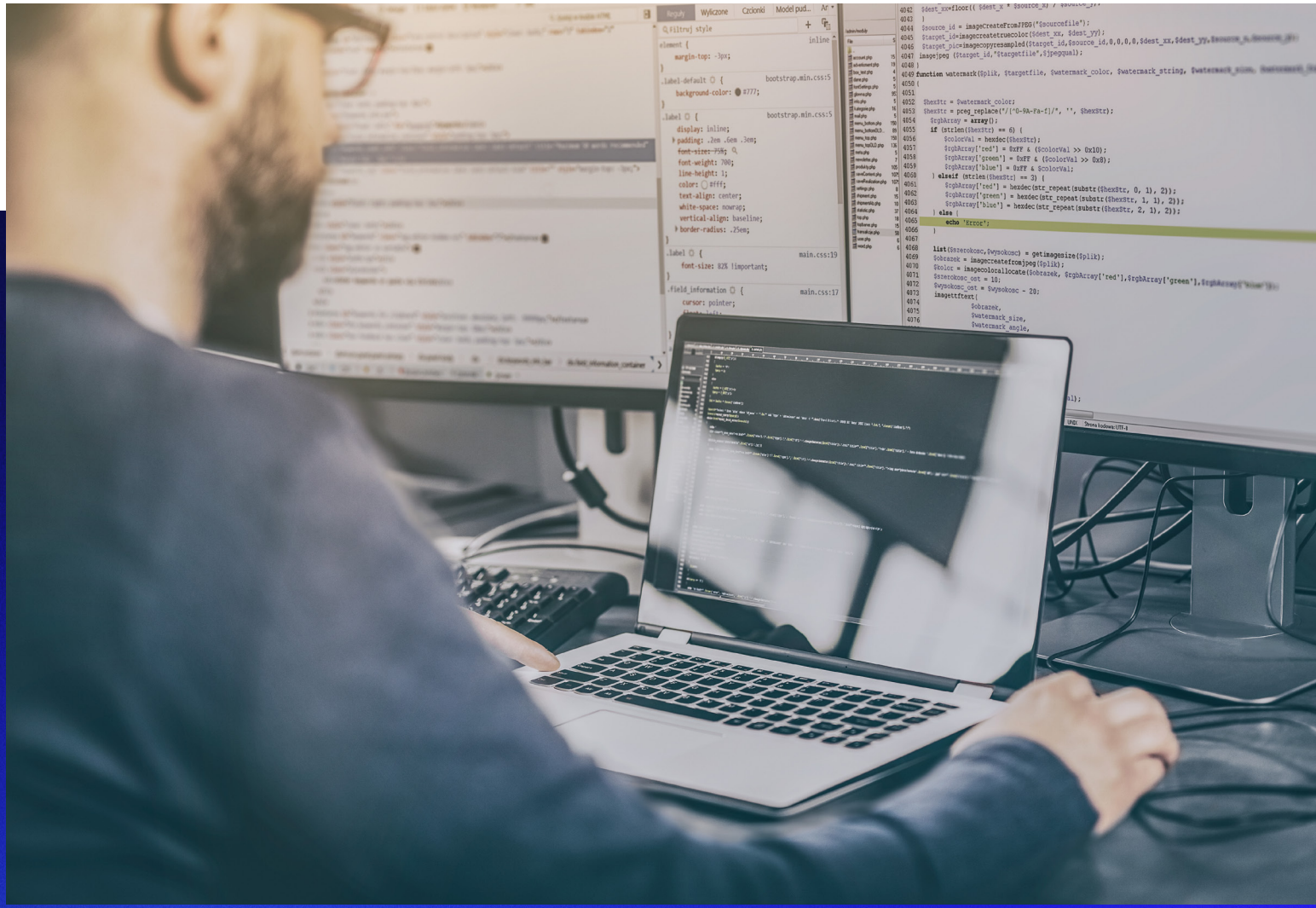
Secureworks®

WHITE PAPER

Red Team Testing A Not So Perfect Engagement



Setting the Stage

Many times, stories from penetration testing or red team engagements are presented as if everything went perfectly with no room for improvement and that every engagement goes just as smoothly. This is not one of those stories. This is a real event; this is what actually happens. In this particular event, not everything went smoothly. There were real world challenges that needed quick thinking and alternative methods to ultimately reach the end goal.

Some context first: this engagement was a Full Scope Red Team test, and everything was in play. The goal was focused on compromising a small number of servers, database servers, email servers and two production systems. Additionally, there were physical targets: a twenty-story building and two remote office locations, one of which was a data center and the other a remote office space.

Many times employees will unknowingly give us a view of computers in the background, including what kind of software is running, all without having to walk up and physically look in the window. If we need more information, satellite imagery can show us high resolution photos of offices or campus design so we know where to look for what before we even show up on site.

Reconnaissance

The engagement started off with the usual process of collecting as much information as possible from publicly available open source intelligent resources: employee names, job titles, email addresses, phone numbers, tenure, etc. Secondly, we took a look at the external network footprint to see what IT space was registered to the company and what the servers were tasked with performing. Next, we looked at social networking websites. In our experience, people love to post pictures of their workspace, especially leading up to the holidays.

Formulating the Plan

From the information gathered, we started putting together plans. On the external network, we found some likely targets: a webmail server, VPN, web access and a mobile web application. From the pictures referenced before, we had a log in screen but not really enough information to act on yet. But it caught our interest and we put it on our list of things to follow-up on. We also built a list of targeted users based on previously collected employee information. The plan of attack was pretty simple: launch a phishing campaign, gather credentials and use those credentials to try to log into the VPN or webmail to help us access the internal network.

We also came up with a physical test plan. We went to check out the headquarters location in person to determine if this was a viable attack vector. The twenty-story office tower was outfitted with security guards, cameras, turnstiles and access control from RFID badges. Just across the street was a café that employees would frequently go to for lunch. It was open to the public and we knew a lot of employees went there for lunch, not just because it was convenient but because inside we could see their employee badges clipped to their belts, purses and lanyards. Based on this, we came up with a plan of attack on a physical side: capture employee RFID badge information, clone those badges, create fake ID cards and essentially walk right into headquarters and find unused office space to plug dropboxes into the internal network.

Putting the Plan in Motion

So we put our external plan of attack in motion. The phishing campaign went out and credentials started coming in. Not a lot, but enough. We used those credentials when we tried to log into the webmail, email and VPN but found it was a two-factor authentication process. This was good for them since we did not have that second factor, so we shut that portion of the plan down. However, the mobile web application did not have a two-factor authentication process, allowing us to log in and validating that we had working credentials. The application itself provided current events information about the company, as well as an interface where you could look up employee information. We could see someone's name, phone number, email address, supervisor and information like general work location, what floor they worked on and in which building. Unfortunately there was no sensitive information, but we collected and scraped the website, pulling all the employee information and saving it to a file.

Capturing RFID badge information has gotten considerably easier over the last few years.

Using some modified readers, we can pick up your badge a few feet away. Additionally, if you are using RFID badge readers to control access to the building's secure areas, we can use the information we collect from one badge and essentially cycle through badge numbers until we find one that will provide us access to that additional secured area.

Once we were on the internal network, we found there was no network access control. The ports didn't get turned off or have any unusual security measures. On the DHCP network, we pulled an IP address right away and we were able to get outbound using open DPN over 443 and straight SSH over a couple of nonstandard SSH ports. This was good news for us since we now had the ability to create a secure tunnel back into these devices and test the internal network from all locations. Now that we were on the network, we started gathering information from the internal side. We had credentials that were collected from the phishing attack, so we were able to quickly build a list of all domain users, associated groups and systems on the network. We began examining network sniffing operating systems, protocols and usage of general network topology. We also started employing additional hash credentials off the wire, using a technique like net files name service, spoofing, link local and multicast name resolution poisoning. These techniques are very powerful and troublesome because they affect protocols that are often enabled by default on the systems. These systems, when looking for a particular resource and don't know how to find it, will send out broadcast packets asking the local network for these resources. With our computer on the network, we're listening for these broadcast packets and when we hear one, we'll respond to it posing as the resource that the broadcast is looking for, and offering to give information in exchange for pass credentials. The credentials are sent along and that's pretty much the end of it from our point of view. We can take those credentials and then attack them offline with a powerful dictionary tag using specialized equipment to try to recover the plain text passwords for the account.

RFID scanning or "skimming" has become common enough that a whole industry of RFID-blocking wallets, sleeves or other products has sprung up to protect consumers.

On the physical attack side, everything went pretty much like clockwork. Everyone had a nice lunch while we captured badge information. We then cloned those badges, suited up and walked into headquarters. We found a couple of unused cubicles where we connected our dropboxes to the internal network. From our point of view, everything was going well.

And Then Everything Went Wrong

Everything was going great until everything went wrong. Little did we know, during our phishing attack, a sharp-eyed user noticed that something didn't look right. Instead of deleting the email, it was reported. It was quickly escalated, our website was shut down and all of our user credentials were changed. We could tell that the device was plugged in and powered up. It was just the outbound connectivity that was out. We still had RFID badges to get us into headquarters, so we walked back in, went over to our device and picked it up and left before internal security could find it and pull it off the network themselves. We thought we were okay since we still had one dropbox and the network was still working, until the middle of the night when the dropbox also stopped working. Since we still had the badges, we didn't know if they would get us into the building in the middle of the night, but thought we might as well give it a shot. We returned to the building and found that we had 24-hour access to headquarters. We headed up to where this dropbox was located, and were pleasantly surprised to find out that it was just broken. Stuff happens— things break in the real world and we had to deal with it at this point in time.

So, now we've gone back into the building to retrieve our broken dropbox. We found we had 24-hour access. The doors inside the building were locked, but they weren't the best locks so we were able to bypass them and recover our broken dropbox while nobody else was there. While there, we decided to look at some of the employee workstations. You may be thinking, "You've lost all your connections, how are you going to enter these workstations?" People still to this day write their user names or passwords on post-it notes and stick them on keyboards, and one of these people happened to be next to our dropbox. So we had their password, their login and we found restrictions.

All their outbound web traffic was heavily proxied. Antivirus was there of course. USB access was unsuccessful. We also discovered that there wasn't full disc encryption. So we went a little bit old school. We re-booted the computer into a different operating system, pulled off some key files that had contained cached or past credentials and saved them. We took these credentials and, much like the ones we pulled off the wire, subjected them to an offline dictionary attack to attempt to recover the historic plain text credentials. As long as we were there, we took a detailed look around and got a better feel for the interior floor plan and general office locations inside the building.

We lost every single user account. To make matters worse, one of our dropboxes was detected. We were working on the device remotely and the connectivity suddenly dropped. This particular device had a built-in wireless access point, so with a little bit of quick thinking, we headed back to the headquarters tower and from outside we tested to see if the access point was functional.

Taking Stock and Creating Another Plan

At this point we've lost our credentials, we lost our internal access and our dropbox was broken. We decided to take stock of what we still had and tried to figure out what we could do with it. From the external software side, we have unique employee information and we've collected the name and office locations of pretty much every employee. We gathered those from the home-built web application using phish credentials. From the internal network, we used those phish credentials to collect user and group information so we could identify accounts, people who are main or enterprise administrators or interesting service accounts. On the physical side, we had largely unrestricted access to the headquarters tower. We also knew employee workstations were not protected by full disc encryption. We could reboot them into different operating systems and pull off some recently stored credentials.

With this information, we developed a final plan of attack, which in the end was effective. We would identify the privileged domain users, correlate that list with the physical locations where these folks were working within the building, head back into the headquarters tower, find their cubicles and workstations, reboot them to a different operating system, pull off the credentials, throw those into our cracked box and try to recover the plain text passwords. When we got a plain text password for one of the privileged accounts, we reconnected to the internal network and compromised the domains we were targeting.

Lessons Learned

After the testing, what sort of recommendations could we provide? As we run through these, consider how many might apply to your organization. You can make an educated guess as to how well your defenses might have withstood our attack. On the external side, there were weaknesses in the in-house built web application. Everywhere we were looking, we ran into twofactor authentication defenses.

This one web app didn't make the cut. If your employees are logging in from the outside, two factor or multi-factor authentication is a good idea. It also looks like this web app could use some additional testing. It really didn't come into play during the actual Red Team engagement, but we did notice some weaknesses in the app that could possibly have been further abused.

Phishing attacks were an effective approach to a point. We got credentials that we were able to use even though our phishing attempt was quickly detected. What would have made the defense more interesting was that this phishing attack was recognized for what it was: the first punch thrown in this fight. Perhaps tracking the activity of these compromised accounts would have been a good warning that this attack is going deeper than it might have initially seemed.

On the internal network, we found that we were able to connect without a problem; there was nothing blocking our attempts to just plug right in and get to work. We were able to get out through this internal network without being restricted. We were able to use several different methods and nothing was shut down, and we were able to pull credentials off the network. These didn't come into play during this specific engagement, but a lot of times they do. False credentials really help to move this type of testing along, which is why we look for it almost right away to connect to the network. So how do we prevent this kind of attack? A network access control solution is a good idea, along with egress filtering, which is a very popular option that we recommend for disabling the net file name server link local multi-task solution. This can be difficult to implement, but it definitely works and is worth considering.

This engagement was a bit non-standard, but a lot of the standard procedures we were looking to perform against this organization were simply being blocked. This attack had the advantage that network connectivity was not really required until we already had that privileged account. We didn't need to keep trying to compromise the device on the network or stay persistent on the network. The downside is that we had to keep returning to the headquarters tower. Over a relatively short period of time, this method carries a risk that security is going to notice us or someone will question what we're doing there. There are pluses and minuses on both sides, but it did end up working.

Red Team's Prescriptive Security Measures from this Engagement

Network level

- Two- or multi-factor login authentication
- Network access control solution
- Egress filtering

Physical level

- Conceal badges when leaving the premises
- Implement Badge readers to restrict access
- Always use full disc encryption
- Don't store login credentials in the workspace!

On the physical side, we found that we can capture badge information relatively easily. In using these captured badges, we had complete access to the headquarters tower 24 hours a day. Once we were in, we could walk up to workstations that were not protected with full disc encryption, so our late night attack worked pretty well. Our recommendations for the physical side get a little trickier. You want employees wearing badges and displaying their badges inside the office space. If you see someone who doesn't have a badge, you need to question why this person doesn't have one and find out if they are someone who is legitimately supposed to be there. On the flip side, we recommend that employees **conceal their badge after leaving the office** so as not to advertise that they are someone who can be targeted to gain access to the building. The badges gave us 24 hour access to the tower; however, security shouldn't have let us straight in after hours, but rather had us sign in and show additional forms of identification. Additionally, **badge readers** should be put in the elevators to restrict access to certain floors. And of course, **full disk encryption is recommended.** We were attacking workstations in this instance, but if your employees use laptops — something that may possibly be left behind in a cab — make sure you have these devices as well protected as possible.

So in the end, we had a successful Red Team test. Not everything went exactly as we wanted it to, but we were able to exploit a number of weaknesses together and simulate a real attack. We are really looking forward to the opportunity to test this company again in the near future. We know there are going to be some changes and we will really have to fight to reach our goal. Red Team testing is an intense, high-profile engagement aimed at getting your organization ready for the worst tactics that a cyber criminal might throw at you. Planning and preparing are an excellent start, but testing can tell you how the fight might go down. Whether you're ready for a Red Team test right now or are preparing for a future engagement, we look forward to working with you to make your organization as safe as possible from intruders. For more information, please visit our Red Team Testing or Network Security Testing webpages.

Finally, here are some thoughts on how the defenders seemed to respond to our attack. Communication between the teams is important. The network technicians detected one of our dropboxes and they turned off the port, but by the time the physical security team had swept the entire floor, we had already gone back in and recovered the box. This delay was due in part to slow communication between the teams. There was not a precise mapping between port numbers and their physical locations within the building. The physical security team spent time searching everywhere, and we used that time to get back in and pull our device out.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp