nccgroup

Shutterstock: Royalty-free stock photo ID: 654030355

Apr 17, 2020 10:36 BST

Black Team War Stories: The Tipping Point

Industry: Research and Development

Sensitive Assets: Personally Identifiable Information (PII)

Objectives: Determine an attackers potential post breach activities

Client's Expectations: Breach is assumed simplistic

==========

Background

The tipping point, as I have coined it, is the moment during a physical assessment when you identify the cracks in what initially seemed an impenetrable fortress and the tower of cards starts to fall. This is where you get your first entry point. It's at this moment you gain access and your other objectives start rolling in. This is something shorter engagements fail to demonstrate.

==========

The Target

NCC Group was recruited to assess one such fortress as part of a two-site engagement.

Two ground teams had been deployed to assess the buildings sequentially. Team 1 acquired access card imagery and were successfully able to breach and achieve their objectives. This put some friendly pressure on Team 2 to achieve their site objectives.

Despite significant intel from Team 1, the second site appeared to be a different kettle of fish altogether. The second site had a completely fenced perimeter, a staffed main entrance with barriers, security perimeter sweeps and access cards that could not be easily cloned to open doors, this was not going to be an easy breach.

==========

Recon

The most important part of any physical assessment is the recon.

Understanding your target is key to a successful breach; footfall, entrances, security cameras, security staff, shift times etc. We had been monitoring the target site for several hours and had only seen staff enter the building through the access-controlled barriers, past the security desk.

Team 1 had provided our own facsimile access cards and we had devised a plan to overtly approach the main entrance, attempt to tailgate the barriers

and present our cards if challenged. This would be noisy and could raise our profile though - we want to be the grey men, go unnoticed and blend into the environment. There had to be another way...

A secondary building was attached to the main site via an enclosed walkway with no access controls between the two. It had its own perimeter door that we had been observing but no one had entered or exited all morning, it felt like a dead-end. Suddenly at 1230, a staff member approached the door and entered, followed shortly after by another two. We identified the secondary building was a canteen and while footfall was low and only used during lunch hours, it was another entrance into the target site and didn't require us to pass security. This was our tipping point.

==========

Breach

The next day, armed with our fake access cards and our tools we headed to site. We had noticed staff heading for the canteen door took a different path from those going to the car park so positioned ourselves to intercept in key locations -the door shut quickly so we needed to be quick.

We waited, the canteen began to fill but no one seemed to be using the door, as time passed we adjusted position to not rouse suspicion. Just as we were considering other options we spotted a target heading towards the building using the path we had previously observed during recon. It was go time.

The target opened the door just wide enough to pass through, we were able to catch the door but not without our target noticing. They requested we scan our access card - we had identified the card technology but our cards only looked like theirs, it wasn't going to work. We obliged, scanning our fake card.

beep

Despite being unable to clone an access card, we had still identified the RFID technology in use and printed onto some blank cards using that same technology. This meant the reader would acknowledge our invalid card and present a red light to signal failure, but the audible cue of that beep was all the target needed to validate us. We were in.

==========

That's a Wrap!

The NCC Group Black Team was able to gain access not just through the latest tools and gadgets but also by understanding human patterns, how to

act like we belong and understanding what opportunities to take. Without spending time on recon and intelligence gathering, it's just a 'smash and grab' with a high chance of detection and failure. The Black Team takes the time to study a site and identify where ingress security is weak and exploit with stealth and precision. This better provides a realistic simulation of a real breach attempt and results in useful data to increase the security of the site we assess.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750