Open your eyes

Tools like TCPDump, Wireshark and Responder in Analyze mode are some of the most important tools I run, and I run them almost constantly while in a target's LAN.

These are my eyes. They allow me to see the environment around me.

Do I want to blend in better? I may look at host names, operating systems, user agents, common protocols/services/utilities used and spoof/change attributes of my host to match the environment around me.

What AV/AM is running within the LAN?

Instead of conducting more intrusive scans, I can watch for ePO and other traffic created by AV/AM within the network to identify what I am up against.

These tools allow me to make better decisions in regard to what and when I enumerate.

Every action I take in LAN raises the probability of being detected.

Instead of taking unnecessary actions or deploying tools which trigger IPS/IDS or stick out as an abnormality, I can enumerate hosts through analysis of the traffic and/or time when I use tools to coincide with periods of heavier/similar traffic to better blend in.

For example, many of the Industrial/Energy sector targets I engaged ran Ferret or a similar utility to collect data on/from the surrounding systems/hosts. Often, this traffic involved Ferret spraying ICMP and SMB traffic at entire IP ranges (some Ferret deployments I saw created waves of traffic that resembled fluxing/spraying worm malware).

What better time to deploy tools like SMBMap or SMBspider then when Ferret is causing it to rain SMB traffic to and from existent and non-existent hosts alike?

Finally, not only are the PCAPs a portable form of recon that you can study outside the target network to better decide strategies/tactics for the next session, but you can also run Predz and net-creds against them, stripping them of credentials, interesting URLS, names of interesting files, hashes, etc.

This makes tools like Wireshark/TCPDUMP akin to others I use in establishing a technique I call Passive Advantage: they serve multiple purposes, are fairly innocuous and can render tremendous results with very little investment of focus/activity when within the target's network(s).

Android…

Android has been an important tool for my success in external pentesting/Red Team engagements.

Often, a lack of awareness or attention create the most vulnerable points in a target's security.

Awareness of the vulnerabilities Android applications (or more broadly, mobile applications in general) can create in enterprise infrastructure definitely seems to be lacking.

For instance, decompiling Android applications can yield tokens/API keys/certificates that can be leveraged to access enterprise infrastructure/resources, especially where Cloud infrastructure is concerned (for instance, AWS, Google Cloud services like Firestore/Firebase, AWS instances, etc.).

A couple of the simplest means to leverage Android apps towards infrastructure exploitation: use Androguard GUI to search for strings such as URIs/credentials or Keyfinder to locate keystores and/or certificates.

There are also more advanced attacks against the perimeter that can be made through using Xposed Framework modules/older versions of Android (5.1 and prior) to bypass certificate pinning and more easily establish certificate substitution (while allows you to fully proxify traffic through Burp and such).

Then there are attacks with tools like Drozer which may allow you to attack content providers (which could harbor backend databases) that may be available.

There are a ton of facets of an Android application that can be used to gain a foothold in perimeter infrastructure or provide unique reconnaissance.

Most importantly, much of the knowledge/tools/techniques to do so can be added to your repertoire fairly quickly.

These skills expand the target's attack surface and give you options.

The more options you have, the more opportunities you have to make the most advantageous decisions possible; at the very least, options give you the opportunity to postpone making a decision that places you at an outright disadvantage.

Even if you do not find an outright vulnerability that effects the perimeter by engaging/enumerating an Android application, in most instances, you are gaining greater knowledge of your target while usually sustaining a position that minimizes the possibility you will be detected (for instance, you can decompile an Android application offline).

Options are advantages.

Passive Advantage

As I have stated before, I believe Red Teaming/Penetration Testing/Hacking are arts of acquiring, applying and improving advantage.

During an engagement, I am always looking to acquire, apply and improve advantages. I study and train to better recognize and maximize the resources within an environment that allow me to gain, use and make the most of those advantages.

Gaining these advantages are more a product of knowledge and experience then an application of tools.

Advantages are the building blocks of tactics/strategy, which I believe are an understated facet of hacking in general.

Without tactics/strategy, an engagement becomes a contest that pits static quantities I possess (intelligence, knowledge of vulnerabilities, capacity to utilize tooling, etc.) vs. static quantities possessed by defenders/the target's IT staff (their intelligence, knowledge of vulnerabilities, familiarity with the environment that will comprise most of the engagement terrain, capacity to utilize tooling, etc.).

Tactics/strategies allow you better/more creatively utilize those static quantities you possess and position yourself to best neutralize/exploit/manipulate those static quantities your target possesses.

One of the tactics I use most is what I call Passive Advantage: using automated tools to gain advantages for you via passive reconnaissance while you attend to other tasks that necessitate greater focus.

For instance, let's say I am decompliling an Android application.

Before narrowing my range of attention/action, I start Spiderfoot (configured for fully passive reconnaissance, targeting the Internet itself but not touching target sites directly) vs. target domains/subdomains, Pagodo auto dorking vs. target domains/subdomains(automated Google dorking vs. the entire Exploit Database collection of Google dorking strings) and Datasploit.

None of these tools need my direct attention past first configuring/running them (until the time comes to analyze the results of course), they never directly touch the target's domain/subdomains (so there is minimal chance these actions will lead to detection) and they are developing/delivering advantages for me while I am working elsewhere to create/improve/evolve other advantages.

When I finally get around to analyzing the results, I then start these/similar tools again vs. other target resources (maybe other domains/subdomains, email addresses of interesting employees, specific IP addresses/IP ranges, etc.).

I am chaining Passive Advantage, creating a near constant flow that finds/refines/contextualizes data specific to the target; the process creates options, while allowing me to better weigh my actions and advantages.

I will keep Passive Advantage perpetually running, which usually results in a process of refining the most applicable data I find: the first series may run against a master domain, then the subdomains found, then specific IP addresses/ranges found; this may shift to a particular employee email addresses/corporate email convention as I look for passwords that may have been disclosed in a recent breach/dump, etc.

Eventually, your mind will get quicker at analyzing the data that you are constantly making available to yourself.

For instance, I have become pretty good at searching/prioritizing the categories Spiderfoot logs results under and focusing my attention on those categories that are likely to aid the situation I find myself in or issue I am facing.

When engaging a target,I want to create offensives rather then just offense; Passive Advantage is a key tactic in establishing/sustaining that strategy.

I want to have as many moves to play as possible throughout an engagement.

OSINT is awesome and its quantity/quality continues to grow

As I have stated before, we live in a world that is hyper communicative, with much of this communication occurring on the Internet.

On the Internet, companies/products want to communicate their value to customers and people want to communicate with other people.

Open Source Intelligence (OSINT) is a byproduct of these online communications, and as the quantity of these communication continue to increase, the resources that yield OSINT will also increase.

In hacking, Red Teaming and Penetration Testing, we weaponize information through the application of our experience, intelligence, strategy, creativity and tooling.

This capacity is a major distinction that separates an experienced hacker from most other users on the Internet.

Our world is permeated by the digital world; more and more often, occurrences in the digital world shape occurrences/behaviors in meatspace.

This has led to a crowded headspace where more and more things are trying to gain our attention.

The more these things try to gain our attention and the more they try to differentiate themselves on the Internet, the more OSINT there is to collect, analyze and then weaponize.

Know thyself and make your attributes/interests work for you.

This game is more about evolution then emulation.

Start out on the paths others blazed, then wander farther and farther off of them.

Let your interests lead you off the path…don't be afraid to get weird, don't be afraid to be wrong and make mistakes.

Don't be afraid to fail.

At some point on my own path, I became determined to make meaningful contributions to the world and came to believe hacking is/was my main mode for making these contributions.

I am not intellectually gifted and this is a field teaming with geniuses.