What's in a Penetration Test?

Penetration testing has become a standard requirement for the majority of our clients, and there are myriad factors that go into a successful penetration testing engagement for both the client and the evaluator. Let's take a look at what commonly comprises a penetration test, and the related testing actions that are performed.

External Penetration Testing

This is generally the type of test people think of when they hear about a Penetration Test. An External Penetration Test is a simulated cyber-attack launched against the target institution and may include both technical and social engineering methods. The rules of engagement can vary, depending on the goals required by the institution. These goals may include gaining access to sensitive (read: customer) data, gaining access to a critical system, or gaining a complete compromise of institution's internal network. The types of External Penetration Tests usually fall into the following categories:

- Black-box. This test is conducted with the penetration tester having no knowledge of the target institution beyond the name and web domain. All targets for attacks (both technical and via social engineering) are discovered by the penetration tester, and attacks are launched without warning to the target institution.
- Grey-box. This test is conducted with limited knowledge of the target institution given to the penetration tester. The type of information provided can vary from engagement to engagement and is normally a list of people and/or devices to be included in the testing.
- White-box. This test is conducted with the penetration tester having full knowledge of the target's infrastructure.

Deciding which approach to take is determined in advance by the institution with the intention of focusing on areas that concern them the most, to evaluate the controls they have in place. While black-box testing provides the most realistic attack scenarios, by their nature they are focused on particular target areas and therefore may overlook other areas where insufficient controls may exist. Grey-box testing would force the penetration tester(s) to allocate time during the engagement to attacking specified targets, while giving up some of the secrecy around what actually belongs to the institution. White-box testing allows the penetration testers the ability to pick and choose their targets, with the benefit of targeting areas that appear to have weaker controls.

Internal Penetration Testing

This is the "assume breach" test, where the penetration tester begins with access to the target institution's internal network. For this reason, the results of the test usually fall somewhere between sensitive information being discovered and a complete compromise of the internal domain. There are different types of threats that can be modeled from this type of engagement:

- Rogue employee – Simulating this threat vector usually requires the penetration tester to have a type of Active Directory (AD) account similar to a lower-level employee, and access to a workstation or Virtual Desktop Infrastructure (VDI) session commonly used at the institution. From here, the penetration tester attempts to gain access to restricted information and elevate their access to an administrator level for AD.
- Successful phishing campaign – Similar to a rogue employee scenario, this simulates a user falling for a phishing attack. The initial access given normally approximates the access a common user who receives a lot of emails, such as a loan processor or Human Resources manager.

- Rogue device – This scenario simulates a foreign device being placed on the network. The penetration tester will usually send the target institution a device if the testing is being done remotely or will bring one with them if performing the test onsite. The rogue device is generally prepared with tools used to attack the internal domain.

An Internal Penetration test is generally conducted as more of a grey-box assessment, as some knowledge of the internal network is almost always required to allow the penetration tester to conduct the assessment. Simulating a successful phishing campaign can come closest to a black-box assessment, but intentionally compromising a workstation can quickly turn into an exercise in bypassing the in-place anti-virus (AV) solution, which can result in less time spent testing the rest of the internal network environment. Nevertheless, this type of assessment can provide invaluable insight into how your internal controls are working, and if there are any opportunities for improvement.

Wireless Penetration Testing

This test strictly focuses on any wireless networks the target institution may have deployed. The goals for this test are slightly different than the other penetration tests and are generally centered on gaining access to the in-scope networks. Testing the networks usually consists of attempts to gather credentials used to access the wireless networks. There are a few authentication protocols used for wireless networks, and WPA2 is currently the only one that should be used for any sort of production network. WEP and WPA, if still in use, should be upgraded immediately. WPA2 can use a pre-shared key (PSK) to grant access to a wireless network, or you can integrate it with AD and require domain credentials to access a wireless network

Depending upon the attack method, the obtained credentials may be cleartext and immediately usable, or encrypted and require decrypting with a password cracking system. For networks using WPA2 with a PSK, capturing an authentication handshake will give the penetration tester the encrypted PSK, and gaining access to the network at this point is simply a matter of time.

Since guest networks often use WPA2 PSK for authentication, the penetration tester may ask for access to the guest network once they have captured the authentication handshake to continue testing. While on the guest network, the penetration tester will look to see if any other clients or subnets are accessible. This can indicate controls may not be working as intended, and a simple PSK may be all that's between an attacker and a corporate subnet.

Networks using WPA2-Enterprise, on the other hand, typically use AD credentials for authentication. These networks frequently have access to sensitive information and corporate resources. Attacks against this type of authentication often consist of attempting to trick a user into connecting to a rogue access point and entering their credentials. The penetration tester can then use those credentials to gain access to the wireless network and then evaluate what information may be accessible.

Which Test(s) Should I Have Done, and How Often?

A good rule of thumb is once per year for an External Penetration Test. This applies to most of our clients, though larger institutions may benefit from having this test performed more often. Most internal environments would benefit from conducting an Internal Penetration Test once per year as well. A Wireless Penetration Test should be performed upon initial deployment of a WIFI network, or when a major change is made to an in-place wireless network.