EXTERNAL VULNERABILITY ASSESSMENTS, EXTERNAL PENETRATION TESTS, AND YOU
INTRUSION PREVENTION SYSTEM WHITELISTING AND ASSESSING FIREWALLS

Mark B. Bell, CISSP, CISA
Executive Vice President of Operations

Introduction

The goal of the Digital Defense External Vulnerability Assessment (EVA) and External Penetration Test (EPT) is to assess the security of those devices on your external network generally available via the Internet. Digital Defense attempts to assess the security of these devices and their associated TCP/IP services to ensure hackers with malicious intent cannot gain unauthorized access to those systems from the Internet through a known vulnerability or misconfiguration. Typical services we observe and assess on external networks include, but are not limited to, public web servers, external mail servers, VPN gateways, etc. This paper discusses two topics that seem to generate a large amount of confusion throughout the industry among IT staff and/or security practitioners: the concept of "whitelisting" and assessing firewalls.

The Importance of "Whitelisting"

In network-speak, "whitelisting" can be defined as a list of acceptable IP addresses, e-mail addresses, etc., given access to a normally restricted network or network service. In terms of EVA/EPT, this applies specifically to IP addresses and Intrusion Prevention Systems (IPS) put in place to protect them. Many organizations have an active IPS or similar technology in use as a detection/prevention control on their network. The purpose of an IPS is to monitor the traffic on a network and identify what it defines as 'hostile', based on a pre-defined set of rules. When the IPS identifies 'hostile' traffic, it blocks the originating IP address of that traffic from accessing the network it is protecting. As network traffic generated during a Digital Defense vulnerability scan or penetration test mimics actual hostile traffic, an IPS will see it as being "hostile" and subsequently block it, resulting in an incomplete assessment of the target network. If a client is utilizing an IPS, we highly recommend they add the Digital Defense scanner and penetration test (if applicable) IP addresses to a "whitelist" on the IPS or other active blocking device. This action allows the scanner and security analyst traffic through to the systems to be assessed, giving an accurate security posture of the external network.

The question is often asked, "Why can't your scanner and/or security analyst go 'low and slow' and try to evade the IPS during their testing?" When Digital Defense conducts a vulnerability scan, we are typically not trying to be evasive. Our goal is to provide a timely and cost-effective solution, yet one that accurately provides the customer with a snapshot in time of their external network security posture. A malicious hacker with unlimited time, motivation, and resources can bypass almost any type of detective and preventive control you may have in place. When a malicious hacker is targeting an organization's network, they have time and motivation on their side. They will, over a period of weeks or months, slowly probe a network looking for vulnerabilities allowing them a point of entry. If the IPS happens to catch and stop them, they simply probe from another IP address – usually another system into which they have hacked. Digital Defense recognizes your time and budget are limited. To emulate a motivated hacker's 'slow and low' technique would greatly increase the cost of the assessment and delay the delivery of results you need in order to mitigate any identified vulnerabilities. This is why we ask to be "whitelisted" in your IPS. "Whitelisting" allows us to condense the time associated with what would normally take hundreds of man-hours and associated capital outlay into something timely and much less costly. A vulnerability assessment and/or penetration test should be viewed as an assessment of an organization's network security, not necessarily an assessment of the detective and preventive controls.

Occasionally, organizations want to test out their IPS and/or their monitoring company to ensure they respond properly to an attack. In these instances, Digital Defense can, by request, run a vulnerability scan prior to being placed in the "allow" or "whitelist" to ensure your detective controls are operational. Additionally, if a controls evaluation is what an organization desires, Digital Defense can perform this evaluation on a consulting basis.

Assessing Firewalls

Many smaller organizations have no external Internet-facing services, such as web, mail, VPN, etc. Typically, they only have a single external IP address representing the external interface of their firewall. Since firewalls are configured to be secure and do not have TCP/IP ports open nor respond to ICMP, or 'ping', traffic, vulnerability scanners will not "see" the firewall and therefore not return any scan results. An interesting dilemma arises from this situation because it is a good security practice for the firewall to be 'invisible' on the network and not respond to vulnerability probes. However, the fact it cannot be detected also means the firewall may not show up in the assessment report. This should not be viewed as an invalid or bad result – the firewall is behaving correctly as designed and configured. However, Digital Defense understands that in some situations, an organization must be able to show examiners/auditors the firewall has been previously assessed. While our reports contain verbiage that takes non-responding systems into account, some examiners/auditors demand to see the host specifically identified in the report. In these situations, Digital Defense can assist in creating a specific rule for the firewall in which it will respond *only* to ICMP requests from the Digital Defense scanner IP address (depending on your firewall manufacturer, creation of a rule such as this may or may not be possible). This will allow the firewall to show up in the Frontline reports and prove to the examiners/auditors an assessment was conducted. Also note, outside of the above configuration change, Digital Defense will not ask you to make any other firewall rule changes that have a negative impact on your external network security.

Conclusion

The above paragraphs should alleviate many of the questions surrounding the use of whitelisting and the assessment of firewalls. Should you have any questions or need further clarification, please feel free to contact Client Support at 888.273.1412 or support@ddifrontline.com.