S.R. Snodgrass, P.C. Remote Network Security Attack and Penetration Testing

(Internal Network Penetration Testing Performed Remotely)

Snodgrass has historically performed internal network security attack and penetration testing at client sites; however, due to COVID-19 restrictions, we needed to revise this practice. In response, we created minicomputers (herein called Remote Keys) that we ship to our clients that help us function as if we are on site. Clients that have previously engaged Snodgrass for penetration testing are aware that we stress the importance of a mix between automated software and manual tasks. Our software and ability to interact with these Remote Keys ensure that we can conduct our penetration tests in the exact same manner as if on site at the client's location.

How it works:

Clients only need to plug the Remote Key into their network and attach a power supply before it is ready for testing. A preliminary call with clients allows us to determine setup needs prior to shipping the Remote Key.

Once a client receives the Remote Key, we have two different methods (a primary method and a backup method) for connecting to the Remote Key securely. Both methods provide a secure, encrypted channel to communicate with the Remote Key on a client's network. Please note that **no** penetration testing data or traffic is sent to the remote tester over the internet. The connection method is only used to connect remotely to the Remote Key, see what is on the screen, and enable the ability to type commands into the machine. Reports and results of scans **do not** "cross the wire"; they stay on a client's network the entire time.

When testing is complete, any needed reports or data can either be uploaded securely from the Remote Key onto the client's network to our secure client portal (temporarily for the tester to retrieve), or the information can stay on the Remote Key and be shipped back to Snodgrass for retrieval. **By default, Snodgrass prefers to remove the data through use of our secure client portal prior to the Remote Key being shipped, to minimize the risk of data loss.**

Security features:

We have employed the following security features to ensure the safety of your network and data:

Windows 10 BitLocker ABSOLUTE TeamViewer LogMeIn Be Limitless.

BitLocker hard drive encryption – Microsoft's BitLocker ensures that the entire hard drive is encrypted while in transit and in use. If a client opts for us to keep data on the Remote Key during transit back to Snodgrass, BitLocker encryption provides added security, should shipping problems arise. Please note that our preferred method is to remove all data prior to the Remote Key being returned to Snodgrass, to avoid unnecessary risk.

Remote wipe capabilities – Remote wipe capabilities are in place on the Remote Key using Absolute, formerly Computrace (embedded tracking software). If a Remote Key is lost or stolen in transit, we notify the Remote Key, and, in return, if it is connected to the internet, it will contact the authorities and remote wipe the Remote Key. Again, Snodgrass's preferred method is to remove all client data prior to the client returning the Remote Key; however, should the client not desire this method, Absolute provides added security.

TeamViewer connection security – Snodgrass primarily utilizes TeamViewer for secure remote access. The following information comes directly from TeamViewer:

The data centers have implemented state-of-the-art security controls, which means that personal access control, video camera surveillance, motion detectors, 24×7 monitoring, and on-site security personnel ensure access to the data center is only granted to authorized persons and guarantee the best possible security for hardware and data. There is also a detailed identification check at the single point-of-entry to the data center. When establishing a session, TeamViewer determines the optimal type of connection. After the handshake through our master servers, a direct connection via UDP or TCP is established in 70% of all cases (even behind standard gateways, NATs and firewalls). The rest of the connections are routed through our highly redundant router network via TCP or https tunneling. You do not have to open any ports in order to work with TeamViewer. TeamViewer traffic is secured using RSA public/private key exchange and AES (256-bit) session encryption. This technology is used in a comparable form for https/SSL and is considered completely safe by today's standards. As the private key never leaves the client computer, this procedure ensures that interconnected computers—including the TeamViewer routing servers—cannot decipher the data stream. Not even TeamViewer, as the operators of the routing servers, can read the encrypted data traffic. All Management Console data transfer is through a secure channel using TLS (Transport Layer Security) encryption, the standard for secure Internet network connections. For authorization and password encryption, Secure Remote Password protocol (SRP), an augmented password-authenticated key agreement (PAKE) protocol, is used. An infiltrator or man-in-the-middle cannot obtain enough information to be able to brute-force guess a password. The PKI (Public Key Infrastructure) effectively prevents "man-in-the-middle-attacks" (MITM). Despite the encryption, the password is never sent directly, but only through a challenge-response procedure, and is only saved on the local computer. During authentication, the password is never transferred directly because the Secure Remote Password (SRP) protocol is used. Only a password verifier is stored on the local computer. As a defense against brute-force attacks, TeamViewer exponentially increases the latency between connection attempts. It thus takes as many as 17 hours for 24 attempts. The latency is only reset after successfully entering the correct password.

LogMeIn Pro security – Snodgrass's backup method for secure remote access is LogMeIn Pro. The following information comes directly from LogMeIn Pro:

> The communications protocol used by LogMeIn Pro is SSL/TLS (OpenSSL). The same protocol is the standard for web-based commerce or online banking. It provides authentication and protection against eavesdropping, tampering and message forgery. LogMeIn hosts maintain a persistent connection with a LogMeIn server. This connection is secured using SSL/TLS. The LogMeIn server's identity is verified using its PKI certificate. The host's identity is verified based on a pre-assigned identifier and a pre-shared secret. These credentials are transmitted by the host to the server over the authenticated SSL/TLS connection. Users also need to authenticate to every LogMeIn host they access remotely. This is done using standard operating system credentials that are never stored on LogMeIn's servers. Authenticating with LogMeIn.com or (in case of a browser left unattended in the wrong place at the wrong time) authenticating with the host can be subject to brute force login attempts by unauthorized users. Both LogMeIn.com and the host employ simple but efficient lockout mechanisms that only allow a few incorrect logins before locking the account or the offending IP address. LogMeIn.com has granular auditing capabilities available under a user's account security settings. These audit messages will notify users via email when an important change (such as adding a new computer) or a suspicious event (such as an incorrect login) occurs.

Password management – Snodgrass uses different passwords for the host machine and for virtual machines. Additionally, passwords used for TeamViewer and LogMeIn Pro also differ from the operating system and virtual machine passwords and are all set to be complex in nature.

No data on the Remote Key during shipping – Client data is transferred securely to our client portal and removed from the Remote Key before the Remote Key is shipped back to Snodgrass, to minimize risk, should it be lost or stolen during transit.

Added benefits:

Performing a remote internal penetration eliminates our need to charge out-of-pocket expenses. Since we can conduct all testing remotely, we do not need to bill clients for mileage, hotel, and meal expenses, and our team will not need to take up a conference room or desk space.

Contact

If you have any questions about remote network security attack and penetration testing, please contact Jeremy Burris, Principal, Technology Services, at 724-934-0344 or jburris@srsnodgrass.com.