THE 7 STEP HACK: THINKING LIKE A CYBERCRIMINAL

As the great Chinese war leader Sun Tzu once said, “know your enemy and know yourself.” As practitioners of network security, we must develop an understanding of how cybercriminals think and work in today’s security environment.

Cybercriminals have learned that a vendor with a VPN connection is a prime target for gaining access to a secure network. In only 7 steps, a connection with a trusted vendor can be compromised and transformed into an open door for a malicious attack on your network.

1. Phish a vendor’s PC
   - The vendor accidentally installs malware, which creates a remote access connection.

2. Remotely access vendor’s machine
   - The hacker sees everything on the remote vendor’s system and compromises the system.

3. Use vendor’s VPN connection to scan for vulnerable targets on a network
   - The hacker uses vendor’s legitimate VPN login to look for their opening.

4. Compromise a software application running on a server
   - The hacker finds and compromises one of your applications to gain a foothold into your network.

5. Use compromised server to access an additional secured network
   - The hacker now has the keys to your kingdom.

6. Compromise a critical system that stores sensitive data.
   - Using pivoting the hacker moves laterally around the network.

7. Hacker steals data
   - The system is compromised and the hacker infiltrates your data, source code, or IP.

Feeling confident with your network security?
Put your security to the test with penetration testing and ethical hacking applications KaliLinux [https://www.kali.org/] and Exploit Database [https://www.exploit-db.com/] to see if there are any vulnerabilities in your network.

Give Vendors Access, Not a VPN.
Bomgar’s Privileged Access Management enables security professionals to control, monitor, and manage access to critical systems by privileged users, including third-party vendors. With Bomgar, you can granularly control access from vendors without giving them a VPN, reducing your exposure to a network attack.

BOMGAR™
ABOUT BOMGAR

Bomgar connects people and technology securely, providing leading remote support and privileged access management solutions that strengthen security while increasing productivity. Bomgar solutions help support and security professionals improve business performance by enabling secure, controlled access to nearly any device or system, anywhere in the world. More than 9,000 organisations across 65 countries use Bomgar to deliver superior support services and manage access to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore.

Visit Bomgar at: