

RAS, VPN, War Dialling, Wifi and Laptop Testing:

VPN Testing

The VPN is an excellent method of providing secure, cost effective remote access for your mobile workers & inter office communications.

However a mis-configured VPN can be a direct route into your network for a hacker, bypassing your security controls & perimeter firewalls

Recent surveys indicate that up to 90% of VPNs may be mis-configured, often allowing compromise.

Test Details

Initial testing of a VPN is performed 'blind': this means that we are provided no information by the client other than the target IP address of the VPN server.

When testing a VPN remotely, first we fingerprint the specific server. Fingerprinting techniques allow us to determine which vendors equipment is used, we can then compile a set of appropriate test cases.

Next we investigate the authentication challenge/response for weaknesses: in many cases this leads to potential for offline key cracking or username enumeration. For example, with an IPSEC VPN, we investigate the IKE Hash in depth. This may lead to cracking of a pre-shared key through brute force attacks.

Certificates and local certification authorities are tested for potential information leakage and associated vulnerabilities.

Weak encryption ciphers are tested for, as these could lead to trivial decryption of the VPN.

Username enumeration is attempted; if this is possible, and no lock out policy is in place, we will compromise the VPN through a dictionary or brute force attack. It will just take time.

Often a username can be obtained during testing of other targets during a penetration test, providing these are in scope. Username mappings may provide a ready list of users.

If compromise of the VPN is not achieved at this point, the client may provide credentials to a test user account on the VPN at their discretion. This allows us to assess the risk presented by theft of user credentials, perhaps through a social engineering attack against the helpdesk, or by compromise from a stolen laptop with cached VPN credentials.

If username enumeration is not possible, we take the credentials to the test user account, first we use the user name & attempt to crack the password.

Finally, we take both username and password, log into the VPN test account with the credentials & determine if a valid user can escalate privilege through the network. User policy is also determined for example lockout and concurrent login settings.

RAS, VPN, War Dialling, Wifi and Laptop Testing:

Any other interfaces to the VPN server are also tested, since these can give access to the underlying server operating system, allowing an attacker to interfere with its operation. Further tests can be carried out targeted at the VPN client as required during the test.

Reporting

A detailed report is submitted, showing the risks and exposures discovered at the various stages of the test. Recommendations will be made towards improving the security of the VPN, often simple configuration changes can dramatically improve VPN security.

War Dialling

Many organisations overlook the security exposure of dial up access to the LAN. SecureTest performs a 'War dial' by dialling every telephone line allocated to the client, looking for modem responses. War dialling is generally conducted overnight to minimise the likelihood of client staff answering the calls.

We have experience of testing a number of different uses to modem connections in otherwise high bandwidth connected organisations. These are often systems to facilitate large scale bank transfers, with the associated risk. Another common use is for printer service organisations querying printer consumables status remotely. As many printers are also network devices, the opportunity for compromise of the LAN via the modem is significant.

After the information gathering exercise, the tester will connect to the modems found, usually using HyperTerm, and attempt to illicit a response from a challenge. If the device discloses any information which could fingerprint the modem vendor, we then attempt the default credentials. Dictionary and brute force attacks are conducted, particularly where a username has been harvested elsewhere during the penetration test, or where only single factor authentication protects a device.

War dialling was known as Demon dialling until the advent of the 1980 movie 'WarGames' in which the lead character, Matthew Broderick, uses the technique to find and connect to the 'WOPR'. Some where along the line, the movie title gave it's name to the test process

Wireless Testing

A wireless assessment primarily involves two phases: wireless infrastructure detection and enumeration, wireless network attack and penetration.

Don't overlook security of the wireless client. Access point impersonation is a very real threat to the mobile worker, read more about it [here](#).

Infrastructure assessment

Network identification involves using best of breed commercial and open source wireless security auditing tools to identify wireless network access points or computers operating in peer-to-peer mode using the 2.4GHz band (divided into 14 channels). A variety of wireless network card devices are used to eliminate vendor-specific compatibility and detection issues. External antennae are employed to extend the range and narrow

RAS, VPN, War Dialling, Wifi and Laptop Testing:

directional spread, enabling accurate pinpointing of wireless devices from significant distance.

Another consideration of wireless implementation addressed by SecureTest involves measuring the signal coverage at strategic points of interest. This is typically conducted utilizing a wireless enumeration tools interfaced with Global Positioning System (GPS). The result of this exercise is typically a geographic map of the area detailing signal strength and loss utilizing a variety of equipment.

Wireless Network Attack & Penetration

Depending on the type of networks identified, and associated security measures, varying attacks are launched against the wireless infrastructure in attempt to circumvent security measures. Measures from MAC address filtering through to use of IPsec VPN tunnels over WEP can be attacked and assessed. Common techniques used to attack & penetrate wireless networks include:

Packet injection used to solicit network responses and aid compromise of 40-bit and 128-bit shared WEP keys Brute-force and dictionary based off-line cracking of pre-shared key utilized with WPA and 802.11i standards Modification of client MAC address in order to circumvent filtering measures ARP spoofing and 'man in the middle' attacks to compromise wireless IPsec VPNs and other security measures. ARP packet re-injection attacks, which can lead to cracking of a WEP key in 1-2 hours

Wireless client enumeration and exploitation

Detection of 'probes' from wireless network clients may reveal networks hidden by traditional means. It is also possible to leverage access point impersonation techniques in order to coax wireless clients into joining an alternative access point. Once joined to this access point, clients may attempt to connect to network resources – revealing any sensitive authentication credentials.

Laptop Testing

Laptop theft happens with agonisingly regular occurrence. Most units are simply re-sold but an end user will doubtless spend time investigating content before rebuilding it. Occasionally laptops are stolen to order to provide a route to hack into the LAN. We quantify the exposure to these threats through a 'stolen laptop' test.

What can the customer expect from this exercise?

Testing mimics how a skilled attacker would attempt to access data contained on lost or stolen laptop. It also explores how it could be used to gain access to the customer's network via remote access settings.

The laptop must be shipped to SecureTest for testing as we require direct access to the unit. A used unit provides more meaningful data than a new one. The customer should rebuild the unit after testing.

Hard drives may be removed and connected to other testing devices to attempt further data harvesting, particularly if the unit has a BIOS password. Laptops are tested on a

RAS, VPN, War Dialling, Wifi and Laptop Testing:

non-internet facing LAN as Windows Update and AV packages will attempt automatic updates during testing.

What techniques will be used?

Device Enumeration: What attached or accompanying devices could be used in the attack? Can the device be booted to another device?

Hard Drive Removal: Where the hard drive can not be accessed via a bootable device the drive is mounted on a separate platform and imaged. The drive can then be examined for interesting documents & data, also analysed for use of encryption.

Wireless: Is the device probing for a wireless network? Using a tool such as Kismet, we can check for probe packets. If so, a local access point can be run to mimic the probed network. If DHCP is set on the access point then the client will lease an IP address and become part of the local network.

Network: If the device has a network card then this will be connected to the local LAN, usually without Internet connectivity, due to OS self update features. The connection will be sniffed and / or DHCP lease observed to ascertain whether the device leases a DHCP address.

Windows 2000/XP Password Hashes: Windows 2000/XP stores the password hashes within the registry, which can be mapped to the files contained within %systemroot%\config\ - during normal operation these files are inaccessible as they are locked by the OS. The hashes are encrypted using a process known as SYSKEY - the syskey is effectively the private key which is stored within the registry and used to encrypt/decrypt the password hashes. Tools, such as LC4 and Rainbow crack, are unable to decrypt the LM hashes without first removing the syskey encryption.