REMOTE CONSULTANCY

IRM REMOTE INTERNAL TESTING

IRM is committed to delivering premium services which adhere and exceed national standards of management, process and security under any circumstances possible.

As the development of all technology and networking advances, businesses are enabled more than ever to streamline delivery of services; especially services regarding IT infrastructure, configuration, development and testing.

IRM has developed a solution called Pandora which enables security testing, consulting, and assessment of on-site datacentre servers and office based workstations to be delivered wholly without the requirement of a consultant attending a customer location. Testers are remotely connected to a testing platform and able to work effectively and to uphold IRM's standard of thorough, efficient and secure testing to the utmost quality. It is the same technology that IRM uses when remotely assessing cloud IT infrastructures such as Amazon Web Services and Microsoft's Azure where a site visit would not be possible.

Emerging trends are being identified as moving towards remote and home-based working. Previously such remote production was exclusively for organisations who have invested into preparation and support for such circumstances. IRM has developed its bespoke solution to ensure that we can support any additional requirements for remote assessment, testing and consulting. This in turn enables an uncompromised approach to continuity of services during traditionally disruptive circumstances.

CORONAVIRUS

In light of recent announcements from the WHO declaring a current pandemic of Covid-19, the requirement for continuing to provide services with minimal disruption has become highlighted.

HOW DOES IT WORK?

IRM has worked to build configuration templates for the most common deployment configurations and can assist our customers to deploy the most appropriate design for their environment in a timely manner.

Essentially a secure tunnel is created between IRM and the remote testing device, from which consultants are able to interact with penetration testing tools to conduct an assessment as if they were located physically within the target organisation.

Eagle Tower, Montpellier Drive, Cheltenham, GL50 1TA, UK.
info@irmsecurity.com I +44 (0)1242 225 200 I www.irmsecurity.com

IS IT SECURE?

Yes, IRM employs a tunnel using Secure Shell (SSH) to provide a secure connection between the client and IRM controlled assets. The SSH tunnel helps to ensure the confidentiality and integrity of data is upheld throughout the testing process. Once a tunnel has been successfully established IRM consultants will be able to connect to the remote testing device and then onward to the client network.

At no point are the networks directly bridged to allow arbitrary connections, only the minimum required connectivity is configured.

IRM's remote testing solution will provide the ability to conduct internal infrastructure security assessments without any compromise, ensuring the same service without putting client or consultant at any increased risk.

- Traffic is encrypted preventing interception based attacks.
- Testing will only be carried out during agreed testing times.
- Key pairs will be used instead of passwords to ensure secure authentication preventing man in the middle attacks.
- Encrypted tunnels will be used to ensure security for data in-transit.
- Full disk encryption will be used to ensure data is stored securely.
- Additionally, all data at-rest will be uniquely encrypted to provide layered, in-depth security.

HOW CAN IT BE DEPLOYED?

By early engagement with IRM we can assist you with consultants who have worked in enterprise IT support and cloud architecture to correctly deploy a virtual machine within your environment ahead of time. IRM has expertise within the following environments:

- On-Premises Virtual Machine on Hyper-V or VMware
- Amazon Web Services EC2 Instance
- Microsoft Azure
- Bare metal deployment to a Laptop or Server

At the end of testing, the bridgehead server and the device within the customer environment will be decommissioned. As the bridgehead is fully encrypted, no customer data will remain on any intermediary devices.

Carrying out an internal security assessment remotely provides numerous advantages such as:

- Assessments can be conducted in difficult to access remote locations, or multiple remote sites simultaneously.
- Reduced cost from travel and accommodation expenses related to a consultant visit
- Consultancy can continue despite health concerns from the transmission of COVID-19 Coronavirus.
- Delays to the commencement of testing due to travel can be mitigated as consultants can work from secure IRM locations directly to the customer environment.

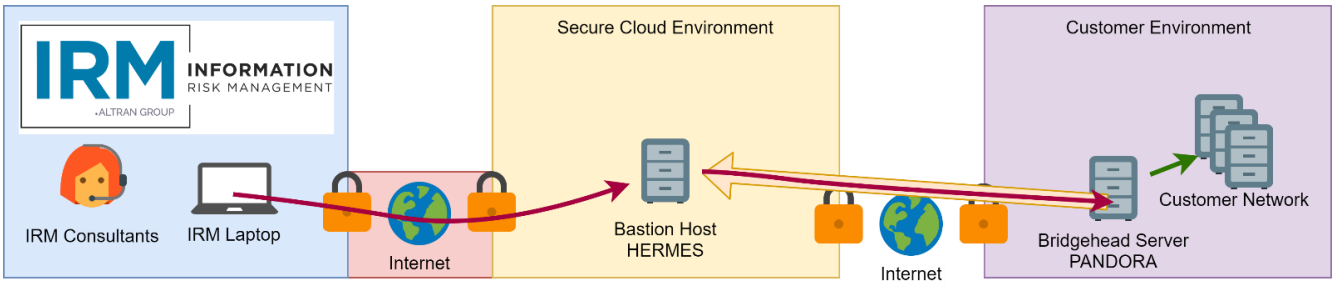
TECHNICAL IMPLEMENTATION

Server Roles

PANDORA is deployed on a customer site and connects out via the internet to a bastion server Hermes over an OpenVPN tunnel, through which a Secure Shell (SSH) connection is established. This server will need outbound internet access to TCP/80 and TCP/443 for tool licensing and software updates and to TCP/443 and UDP/1194 for the VPN tunnel.

HERMES is a bastion server listening for inbound connections. Hermes hosts an OpenVPN server, listening on TCP/443 and UDP/1194, a deployment of Pandora to the customer site will connect outbound from the customer site to the Hermes server. Similarly a reverse tunnel from the Hermes server is established to the Pandora instance on the customer site.

Overview



	OpenVPN encrypted tunnel outbound from PANDORA deployed VM on customer environment to HERMES bastion host in secure cloud environment
	Encrypted SSH tunnel from IRM device to bastion HERMES and a separate SSH connection from HERMES bastion server to PANDORA on site VM inside the outbound OpenVPN tunnel
	Normal Penetration Testing network access to Customer devices
	Firewall Point to Point rule set, only the IP addresses owned by IRM can access the bastion server.
	Segregating Firewall

SOLUTION DEPLOYMENT

Requirements of the customer

Edge Firewall Ports	TCP/80 TCP/443 UDP/1194
Connection Direction	Outbound to the internet
Destination	IRM will provide an IP address for the individual Hermes bastion server
Internal Requirements	ANY:ANY to SYSTEMS TO BE TESTED

The customer will deploy a generic Kali instance termed by IRM as Pandora to the existing customer environment, then execute a configuration script provided by IRM. IRM will provision a Hermes bastion server listening on UDP/1194 and TCP/443 for the OpenVPN software in a secure cloud environment. The Hermes server is hosted on an encrypted virtual machine, and only allows explicitly allowed connectivity.

On the Pandora VM on the customer site, the configuration script will install the required software automatically, and establish an outbound connection to the Hermes server on TCP/443 or UDP/1194 depending on connectivity. IRM consultants will connect inbound to Hermes and then onward to the Pandora server over an SSH connection inside the OpenVPN tunnel.

Deployment

The customer will download and install the Kali Linux penetration testing distribution in to a Virtual Machine within their existing environment, or to physical hardware. Offensive Security provide a Virtual Machine template for the most common virtualisation platforms. VMware, Hyper-V and VirtualBox.

Kali Linux Download	https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

IRM will perform the following steps:

- Create individual Hermes bastion host, exclusively for the use of 1 customer for the duration of the test
- Issue the configuration pack to the customer, including script to lock down the Kali instance with individual authentication details for their allocated Hermes server
- Issue the IP address of Hermes server for customer to whitelist required ports

Once these pre-requisites have been met, IRM can arrange connectivity testing so that in advance of the test date, connectivity can be proven working and any applicable software and updates can be installed.