Unleash The Infection Monkey: A Modern Alternative to Pen Tests

Written by: Ofri Ziv, Daniel Goldberg

The Infection Monkey is GuardiCore's inhouse, open source tool for testing a data center's resiliency to perimeter breaches and internal server infection. By mimicking a human attacker and acting like a controlled piece of malware, the Infection Monkey provides actionable insights and the ability to verify security policies across the organization.

Testing methodologies can't keep up

The modern operating assumption is that at some point, your network will be breached. We believe that a data center should be built in a way that assumes that breaches are inevitable and as such, designed to be resilient to post-breach incidents.

Dozens of tools exist to test your defenses including vulnerability scanners, SQL injection testers, XSS testers and compliance scanners. However, there are no tools specialising in testing propagation across the network. While pen testers do address lateral movement and data exfiltration, these tests are costly and often challenged by the rapid changes modern network undergo. By the time the recommendations arrive, they're frequently out of date.

How it all started

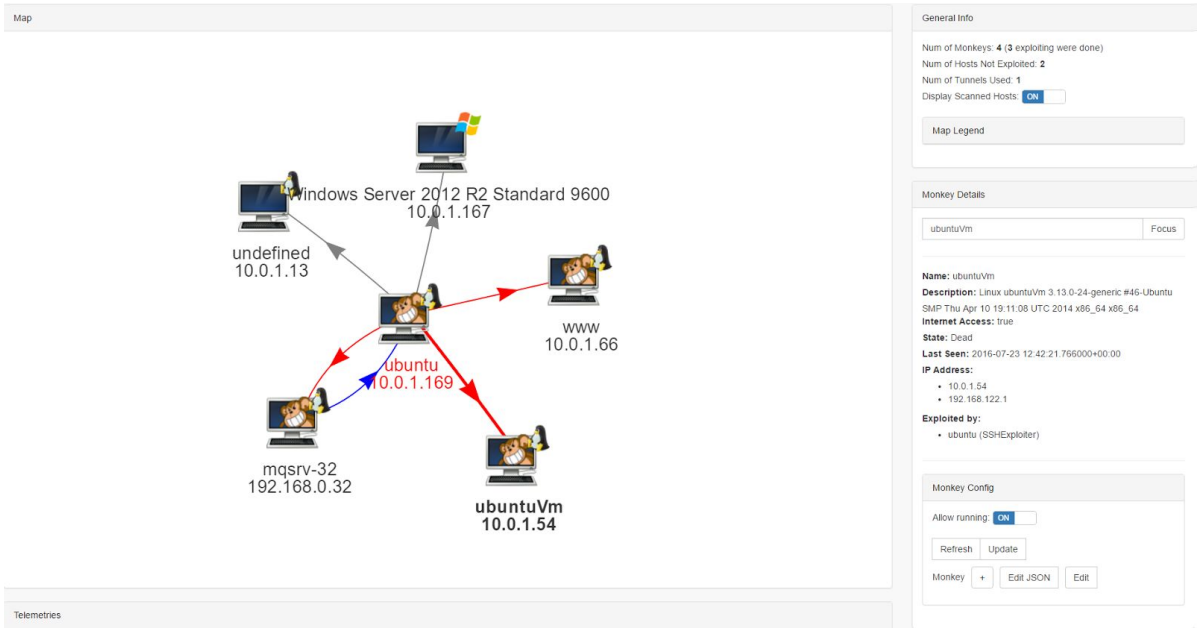
Oddly enough, the idea of proactively breaking the network to test its survival wasn't born in the security industry. In 2011, Netflix released Chaos Monkey, a tool that was designed to randomly disable the company's production servers to verify they could survive network failures without any customer impact. "The name comes from the idea of unleashing a wild monkey with a weapon in your data center (or cloud region) to randomly shoot down instances and chew through cables -- all the while we continue serving our customers without interruption", the Monkey designers wrote in a blog post published July 2011. Netflix's Chaos Monkey became a popular network resilience tool, breaking the network in a variety of failure modes, including connectivity issues, invalid SSL certificates and randomly deleting VMs. Today performing a destructive testing of this type is still considered a strong benchmark of network resilience.

Inspired by this concept, we've created our very own Infection Monkey, suited for security professionals. Our Monkey is designed to test the resiliency of modern data centers against attack and give security teams the insights they need to make informed decisions and enforce tighter security policies.

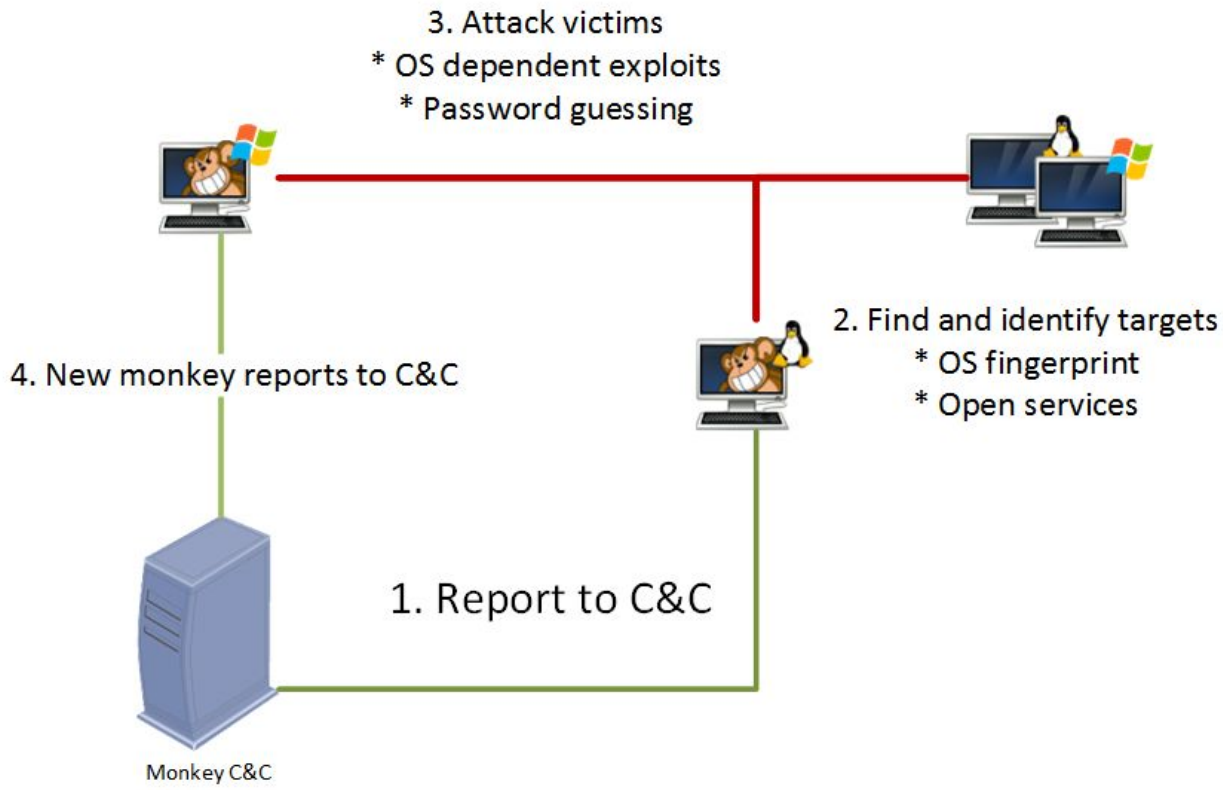
How the Infection Monkey works

The Infection Monkey's high level concept is simple. It is designed to locate accessible machines and attempt to exploit them using a variety of methods including intelligent password guessing and safe exploits, simulating an attacker and not an automated scanner. All this with the intention of being detected by each and every security system.

The Infection Monkey provides detailed information about the specific vulnerability abused and the effect vulnerable segments can have on the entire network, Any progress in lateral movement by the Monkey is an indication of a security failure that should be fixed.



After infecting a machine, the Monkey sends telemetry from the machine and requests a configuration from the C&C server. If there is no answer it searches for a configuration file and if that fails, it uses a failsafe configuration. Next, the Monkey starts scanning the configured IP ranges and tries to attack accessible machines.



Network reconnaissance

After startup, the Monkey starts scanning the network. After detecting active machines using either ICMP ping messages or checking for active ports, the Monkey attempts to fingerprint the machine. After fingerprinting, the Monkey matches attack methods to the target and attempts to attack the machine.

Here are a few examples of the methods the Infection Monkey uses to propagate itself:

SSH

The Monkey attempts to infect machines with open SSH ports using brute force user/password dictionary. If successful, it will upload a matching binary to the remote server and execute it.

MS08-67 Conficker

Given that Windows Server 2003 installations on client networks are still prevalent, we've also designed the Monkey to find unpatched machines that are still vulnerable to the exploit made famous by the Conficker worm.

We're using an existing exploit of MS08-67 customised to work on Windows Server 2003 SP2 (the most common version still in use). Running the exploit delivers a standard portbind payload (created by Metasploit) that allows backdoor commands. Using this payload, we upload a copy of the monkey which is then executed using SMB. In the end, the Monkey is responsible for deleting the backdoor and leave the system in the same state as before.

WMI & SMB

Propagation over SMB and WMI using stolen credentials is a strong favorite in lateral movement. Both attempts use a known user/password list to copy the Monkey over to the target host using SMB.

At this stage the flow splits. The **SMB method** creates a service on the victim machine that executes the dropper. The **WMI method** executes the Monkey directly using the Win32_Process object.

RDP

RDP propagation is attempted by brute forcing a login using a user/password list.
Once successfully connected, the Monkey manually inputs commands just like a human attacker would, downloading and executing a Monkey Binary from an HTTP share using VBS or the BITS service from the attacker.

Bypassing network segmentation

When the Monkey starts running in the newly infected machine, it connects to the C&C server and continues on infecting machines, unless the configuration tells it otherwise. While self propagating, some machines are not accessible to the C&C server. In these cases, the Monkey can set up a series of tunnels, allowing it to create a connection back to the C&C server. This allows the Monkey to propagate through segmented networks, simulating the sort of proxies a real attacker would configure.

Controlling the Monkey

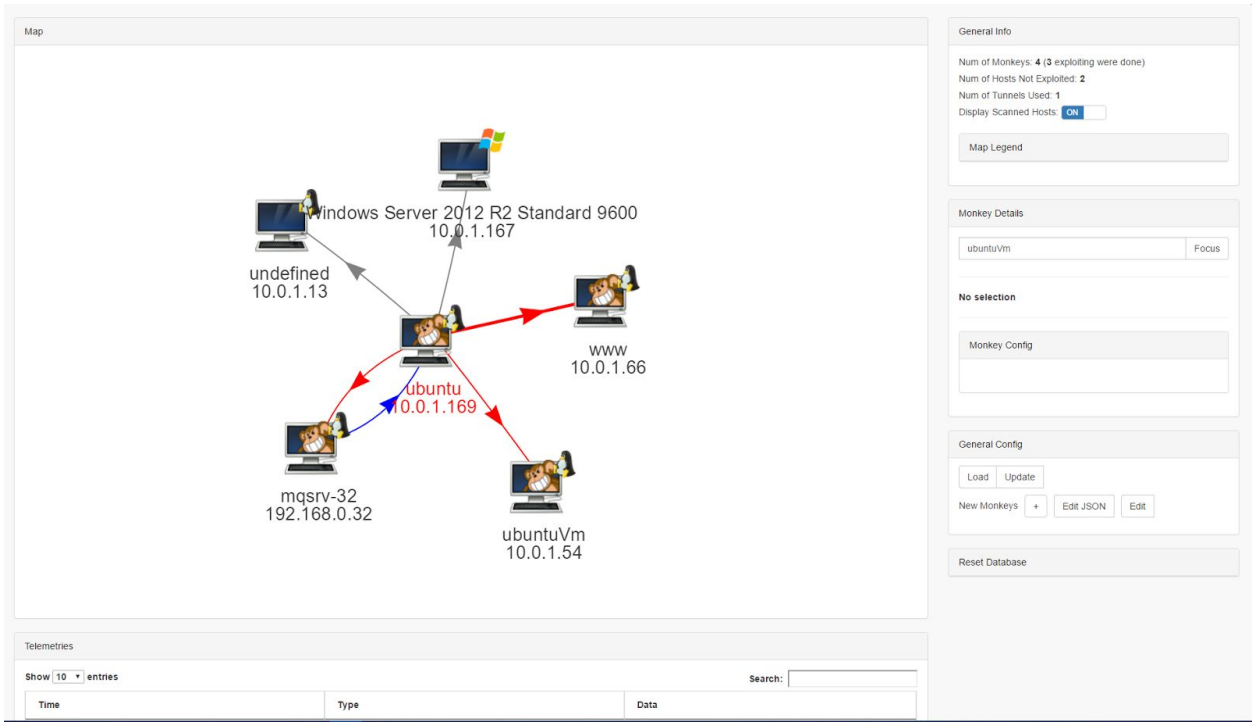
The Monkey has an easy-to-use GUI and is built to integrate with network orchestration tools such as vCenter, making it easy to deploy for IT professionals.

Its Command and Control interface helps administrators run tests using two main tools: **Monkey Island**, a simple web interface to keep track of active monkeys in the network and

Monkey Business, an easy to use tool for creating infection points in virtualized environments, allowing for easy automated testing.

Monkey Island

Monkey Island is the web based C&C interface that keeps track of the different Monkeys on a network and targeted machines.



Overview of the network as visible by the Monkeys

Using the Monkey Island interface, you can:

- Modify the Monkey's configuration file, preventing or allowing specific attacks or modifying known passwords.

Monkey's configuration file

- View the Monkey's full telemetry log and keep track of each operation the Monkey performs, including collection of system info, scanning and successful exploitation.

Telemetries

Show 10 entries

Search:

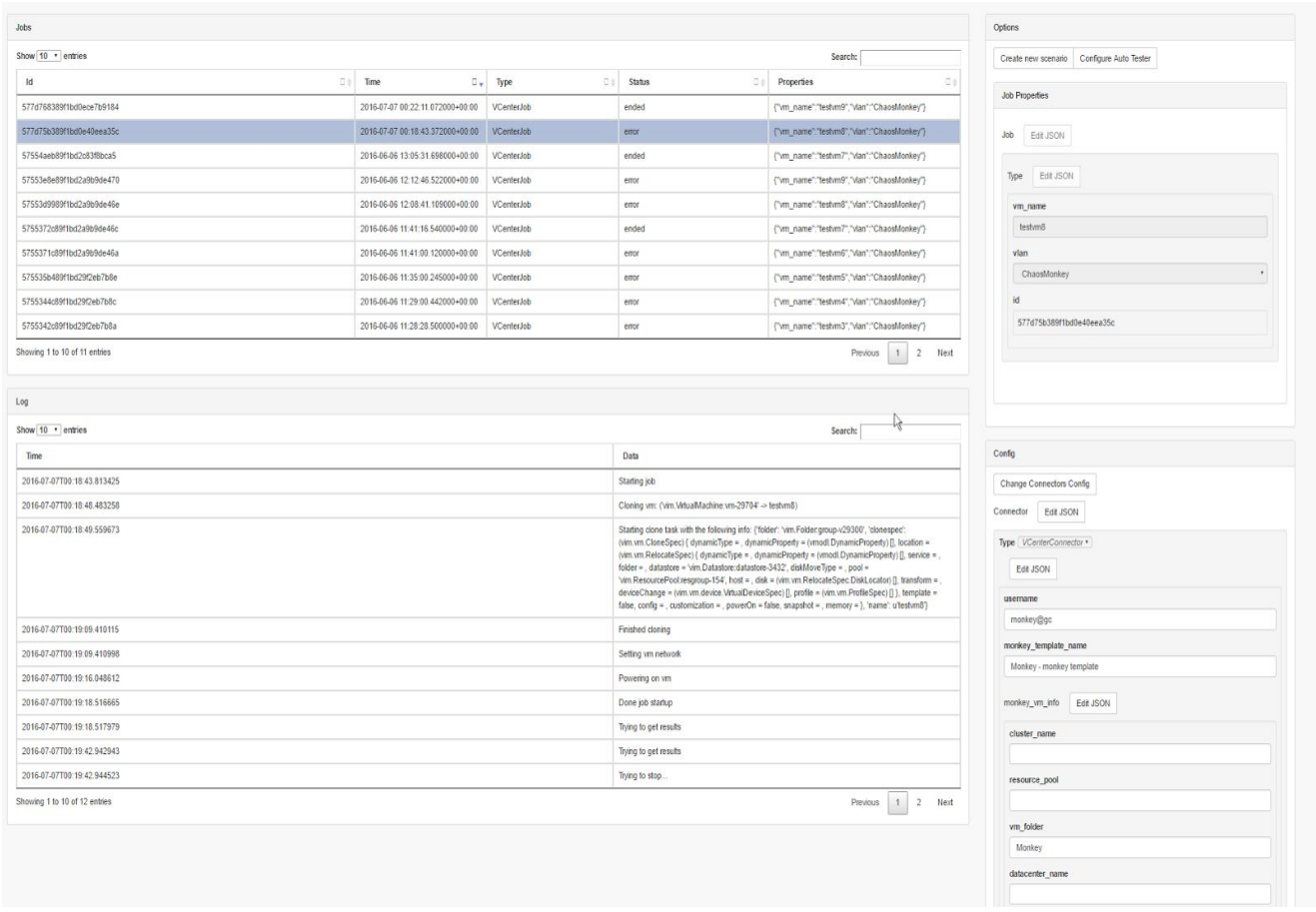
Time	Type	Data
2016-07-21 13:34:26.645000+00:00	exploit	{"machine": {"ip_addr":"10.0.1.51","default_server":"10.0.1.169:5000","monkey_exe":"monkeyfs://monkey-linux-64","os":{"machine":"x86_64","type":"linux"},"default_tunnel":"10.0.1.77:52525","services": {"tcp-22":{"banner":"SSH-2.0-OpenSSH_6.2p2\r\n","name":"ssh"}},"cred": {"root":"1234"}},"exploiter":"SSHExploiter"}
2016-07-21 13:34:26.809000+00:00	scan	{"machine":{"ip_addr":"10.0.1.90","default_server":null,"monkey_exe":null,"os": {"version":"Ubuntu-2ubuntu2","type":"linux"},"default_tunnel":null,"services":{"tcp-22": {"banner":"SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2\r\n","name":"ssh"}},"cred": {}},"scanner":"TcpScanner"}

Telemetry feed

Monkey Business

Monkey Business is a web interface that automatically generates Monkey Islands and randomly infects the network in several places, letting users easily run tests.

Using an easy to extend API, Monkey Business can communicate with network orchestration tools such as vSphere, making it easy to spin up a Monkey Island VM, connect it to a random network and watch it infect hosts.



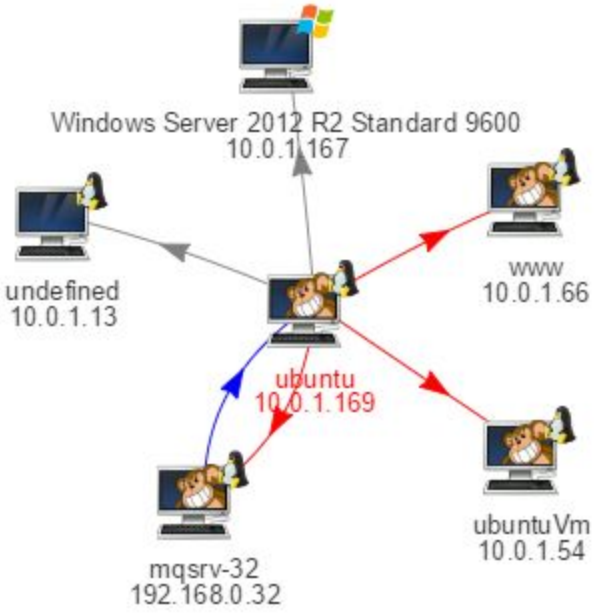
Monkey Business lets you easily plan and execute infections in the network

Real world usage

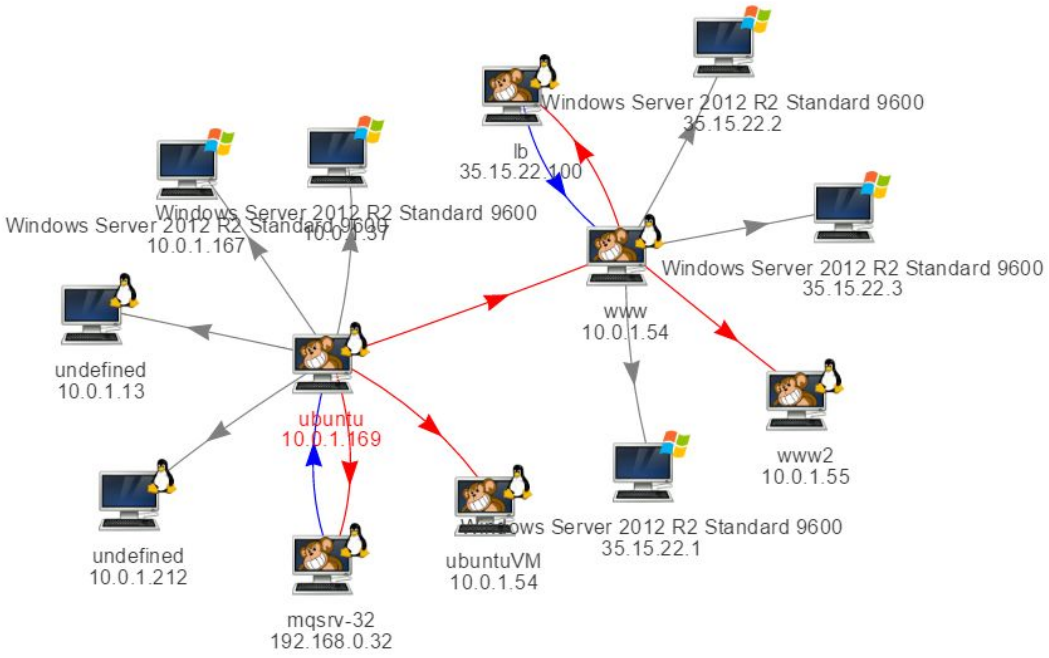
One of the best use cases of Infection Monkey is verifying that security policies are actually followed. In this case, we ran Infection Monkey in a network that recently moved away from using common hardcoded passwords to development servers.

By configuring Infection Monkey to know about these passwords ahead of time and allowing it to spread around the network, the security team can easily see how well the rest of the company complies with the new policies and what work remains to be done.

We started by running the Monkey in a generated VM inside the network and let it start scanning.

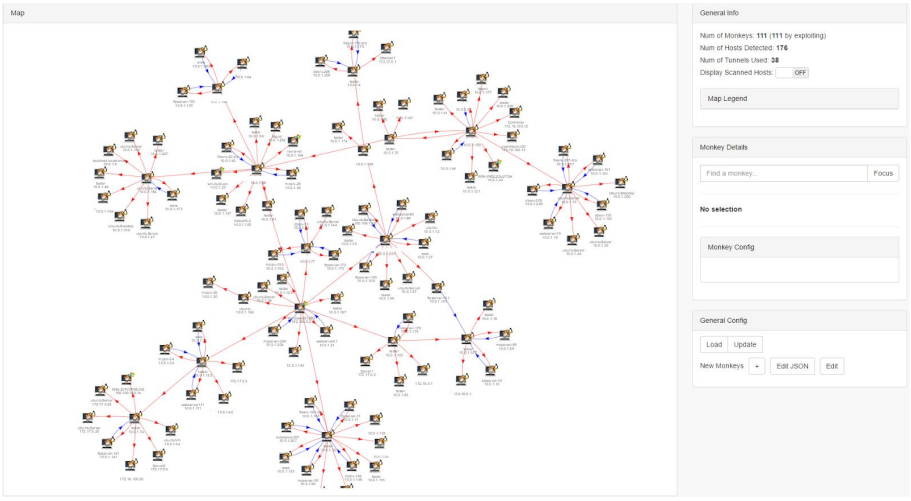


After a short period of time, the Monkey managed to reach 3 victims. We left it running and discovered one of the servers ended up reaching a few more machines.



“There’s always a way in…”

Eventually we managed to reach 111 out of 176 machines visible on the network, using more than 30 tunnels to connect the different network segments!



With this information at hand, the security team was able to modify policies in the organisation and verify overall compliance (and even tracked down machines with no owners marked!).

Summary

With our Infection Monkey we're kicking off a new standard for security resiliency testing. Use the Infection Monkey to make your network resilient to real-life attacks. The Monkey is designed for security professionals, with the vast majority of its code written in Python. Feel free to contribute code and share techniques and ideas at https://github.com/guardicore/monkey.