WHAT IS CLAIMED IS:

1. A method for operating a honeypot network, the method comprising:

after creating honeypot containers respectively corresponding to service machines based on service addresses of the service machines, sending, at intervals of a preset duration, heartbeat information to N to-be-monitored probes, wherein the heartbeat information is sent to each of the to-be-monitored probes at intervals of the preset duration, wherein the to-be-monitored probes refer to probes connected to a honeypot host, the N to-be-monitored probes are located at N service machines respectively, N is an integer greater than or equal to 1, and each probe is used to acquire and forward a service address of a corresponding service machine;

acquiring feedback information returned by M to-be-monitored probes, determining that the M to-be-monitored probes are active probes, wherein the active probes are properly functioning probes, and M is an integer greater than or equal to 1 and less than or equal to N;

determining at least one newly added probe in the M active probes, wherein the newly added probe is a probe corresponding to a newly added service machine for which a corresponding honeypot container has not been created;

acquiring each newly added service address transmitted by each newly added probe respectively; and

creating a honeypot container corresponding to the each newly added service machine respectively, based on the each newly added service address;

acquiring attack traffic for a service machine;

forwarding the attack traffic to a honeypot container corresponding to the service machine, wherein a container address of the honeypot container is the same as a service address of the service machine, the service address is a network address of the service machine, and the container address is a network address of the honeypot container; and

returning virtual data generated by the honeypot container, wherein the virtual data is data requested by the attack traffic, and the virtual data comprises the container address.

2. The method for operating a honeypot network according to claim 1, wherein, before the acquiring attack traffic for a service machine, the method further comprises:

acquiring the service address of the service machine; and

creating the honeypot container corresponding to the service machine based on the service address.

3. The method for operating a honeypot network according to claim 2, wherein, the acquiring the service address of the service machine, comprises:

acquiring the service address transmitted by a probe, wherein the probe is located at the service machine, and the probe is used to acquire and forward the service address of the service machine;

the acquiring attack traffic for a service machine, comprises:

acquiring the attack traffic transmitted by the probe, wherein the probe is also used to forward the attack traffic accessing the service machine.

4. The method for operating a honeypot network according to claim 2, wherein, before the acquiring the service address for the service machine, the method further comprises:

acquiring a service network segment of a service subnet, wherein the service network segment comprises at least one network address occupied by the service subnet; and

setting up an application container engine based on the service network segment, wherein the application container engine is used to create, based on the network address in the service network segment, the honeypot container corresponding to the network address;

the creating the honeypot container corresponding to the service machine based

on the service address, comprises:

invoking, after determining that the service address belongs to the service network segment, the application container engine to create the honeypot container corresponding to the service machine.

5. The method for operating a honeypot network according to claim 2, wherein, before the creating the honeypot container corresponding to the service machine based on the service address, the method comprises:

acquiring a honeypot custom directive for creating the honeypot container corresponding to the service machine, wherein the honeypot custom directive comprises an execution manner and a service type of the honeypot container;

the creating the honeypot container corresponding to the service machine based on the service address, comprises:

creating, based on the service address, the honeypot container corresponding to the service machine, in the execution manner and the service type in the honeypot custom directive, wherein a honeypot service comprises a virtual service established in the service type;

after the forwarding the attack traffic to a honeypot container corresponding to the service machine, the method further comprises:

executing the virtual service in the execution manner based on the attack traffic.

6. The method for operating a honeypot network according to claim 3, wherein, the acquiring the service address transmitted by a probe, comprises:

acquiring at least one service address transmitted by at least one probe respectively, wherein the at least one probe is located on at least one service machine respectively;

the creating the honeypot container corresponding to the service machine based on the service address, comprises:

creating a honeypot container respectively corresponding to the at least one

service machine based on the at least one service address;

the acquiring the attack traffic transmitted by the probe, comprises:

acquiring the attack traffic transmitted by the at least one probe, respectively targeting at the at least one service machine;

the forwarding the attack traffic to a honeypot container corresponding to the service machine, comprises:

forwarding the attack traffic respectively targeting at the at least one service machine, to the honeypot container respectively corresponding to the at least one service machine, respectively.

7. An apparatus for operating a honeypot network, the apparatus comprising:

a real-time processing module, configured to: after creating honeypot containers respectively corresponding to service machines based on service addresses of the service machines, send, at intervals of a preset duration, heartbeat information to N to-be-monitored probes, wherein the heartbeat information is sent to each of the to-be-monitored probes at intervals of the preset duration, wherein the to-be-monitored probes refer to probes connected to a honeypot host, the N to-be-monitored probes are located at N service machines respectively, N is an integer greater than or equal to 1, and each probe is used to acquire and forward a service address of a corresponding service machine; acquire feedback information returned by M to-be-monitored probes, determining that the M to-be-monitored probes are active probes, wherein the active probes are properly functioning probes, and M is an integer greater than or equal to 1 and less than or equal to N; determine at least one newly added probe in the M active probes, wherein the newly added probe is a probe corresponding to a newly added service machine for which a corresponding honeypot container has not been created; acquire each newly added service address transmitted by each newly added probe respectively; and create a honeypot container corresponding to the each newly added service machine respectively, based on the each newly added service address;

an acquisition module, configured to acquire attack traffic for a service

machine;

a forwarding module, configured to forward the attack traffic to a honeypot container corresponding to the service machine, wherein a container address of the honeypot container is the same as a service address of the service machine, the service address is a network address of the service machine, and the container address is a network address of the honeypot container; and

a returning module, configured to return virtual data generated by the honeypot container, wherein the virtual data is data requested by the attack traffic, and the virtual data comprises the container address.

8. An electronic device, comprising:

a processor; and

a memory, storing a computer program executable on the processor, wherein, the program, when executed by the processor, performs the method for operating a honeypot network according to any one of claims 1-6.

9. A non-transitory computer readable storage medium, storing a computer program thereon, wherein, the computer program, when executed by a processor, performs the method for operating a honeypot network according to any one of claims 1-6.