MHN Test Dökümanı

MHN(Modern Honey Network) honeypotlari merkezi olarak yönetim ve data izleme aracıdır. Bu dökümanda MHN ve honeypot araçlarının test yöntemleri gösterilmiştir.

1. MHN

MHN kullanım dökumanındaki gibi kurulduktan sonra doğru bir şekilde aşağıdaki sayfalar tarayıcı tarafından açılarak merkezi cihazın hazır olduğu teyit edilir.

Merkezi cihazın IP adresinin 169.254.1.1 olduğunu varsayarsak.

http://169.254.1.1

http://169.254.1.1:3000 (Atak haritası)

İlk adresten ‘Deploy’ sekmesine girilerek honeypot yapılandırmalarında kullanılacak deploy kodu alınır. Bu kod her honeypot container icin aynı olacaktır. MHN cihazı yeniden yuklenirse değişir.

Kurulan her bir honeypot ‘Sensors’ sekmesinden gözükmelidir. Oluşan ataklar ‘Attacks’ sekmesinde görülür.

2. Cowrie Honeypot

Cowrie, ssh ve telnet tuzak aracıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında cowrie container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n cowrie

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#supervisorctl status cowrie

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak icin containera belirlenen porttan ssh veya telnet baglantisi kurulur.

3. Dionaea Honeypot

Dionaea, bir cok protokolden honeypot saglar. Fakat ahtapot projesinde http ve https protocolleri için kullanılmıştır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında dionaea container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n dionaea

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#supervisorctl status dionaea

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak için container IP adresine tarayıcı ile http ve https bağlantı atılır.

4. FTP Honeypot

Bu playbook FTP ve FTPS protokolleri için honeypot yaratır. Honeypot-ftp araci kullanılmıştır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında ftp container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n ftp

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status honeypot-ftp

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak için containera FTP protokolü ile bağlanılır.

5. POP3 Honeypot

Bu playbook POP3 protokolleri için honeypot yaratır. Honeypot-pop3 araci kullanılmıştır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında pop3 container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n pop3

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status honeypot-pop3

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak için containera pop3 istegi atılır.

6. Amun Honeypot

Amun zaafiyet içeren tuzak aracıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında amun container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n amun

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status amun

komutu ile aracın çalıştığı görülür.

7. Elastichoney Honeypot

Bu araç elasticsearch uygulamasının tuzağıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında elastichoney container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n elastichoney

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status elastichoney

komutu ile aracın çalıştığı görülür.

8. Glastopf Honeypot

Glastopf web uygulama tuzak aracıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında glastopf container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n glastopf

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#supervisorctl status glastopf

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak icin honeypot a web istekleri atılır.

9. P0f honeypot

P0f pasif parmak izi tanımlayıcıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında p0f container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n p0f

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#supervisorctl status p0f

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak icin container tcp bağlantı atılması yeterlidir.

10. Shockpot Honeypot

Shockpot shellsock zafiyeti icin tuzak aracıdır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında shockpot container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n   shockpot

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#supervisorctl status   shockpot

komutu ile aracın çalıştığı görülür.

Loglama testi yapmak icin aşağıdaki şekilde bağlantı atılır

#curl -A '() { :; }; /bin/ls' http://169.254.1.2

11. SMTP Honeypot

Bu playbook SMTP protokolü için honeypot yaratır. Honeypot-smtp araci kullanılmıştır. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında smtp container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n smtp

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status honeypot-smtp

komutu ile aracın çalıştığı görülür.

12. Suricata Honeypot

Bu playbook MHN ile entegre adilmiş suricata kurar. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında suricata container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n suricata

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status suricata-rup.service

#systemctl status suricata-rup.timer

komutu ile aracın çalıştığı görülür.

13. Wordpot Honeypot

Wordpot wordpress tuzak sistemidir. Kullanım dökümanındaki gibi kurulum yapıldıktan sonra host cihazında wordpot container ı oluştuğundan emin olunur.

#lxc-ls

komutu varolan containerları listeler.

#lxc-attach -n wordpot

komutu ile containera bağlanılarak ayakta olduğu teyit edilir. Daha sonra

#systemctl status wordpot

komutu ile aracın çalıştığı görülür.