

## IIS Fingerprinting Engelleme Ayarı

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

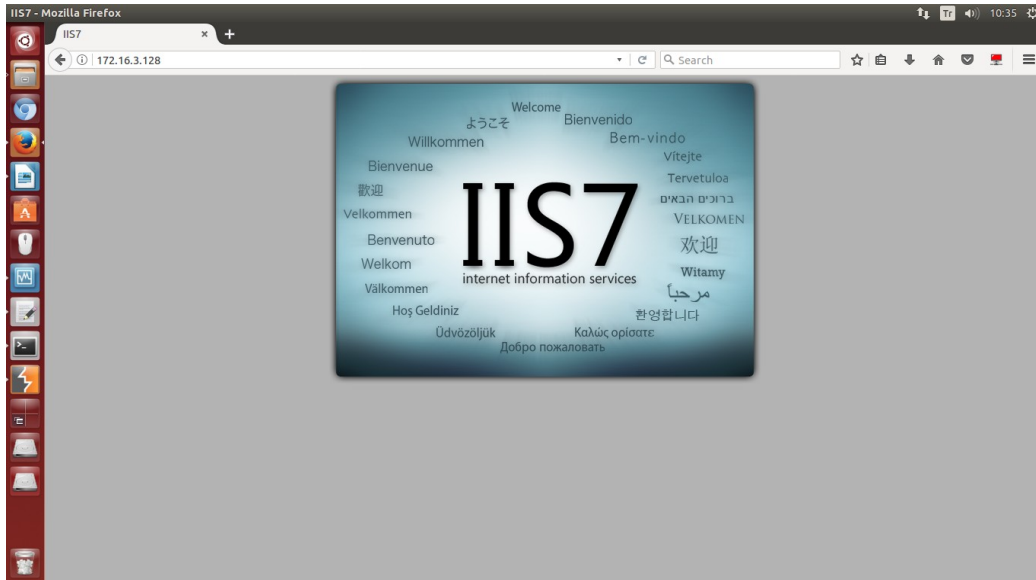
IIS çalışan web sunucuları http yanıt paketlerinde bilgi ifşasında bulunabilmekteler. Bu bilgi ifşalarını durdurabilmek için bazı yapılandırma ayarları gereklidir. Http yanıt paketlerindeki bilgi ifşalarını görüntüleme ve sonra kaldırma işlemini simule etmek için hedef web sunucusu olarak Windows Server 2008 R2 kullanılacaktır.

### Gereksinimler

Ubuntu // Ana Makina  
Windows Server 2008 R2 // Web Sunucusu  
UrlScan (rewrite\_2.0\_rtw\_x64.msi)  
UrlScan (rewrite\_3.1\_rtw\_x64.msi)

Not: Windows Server 2008 R2 işletim sistemine sahip sunucuyu IIS hizmeti sunan bir web sunucusu yapmak için gerekli yapılandırma ayarları için bkz. /home/hefese/Downloads/Windows Server 2008 R2/Windows Server 2008'i Web Sunucusu Yapma.

Windows Server 2008 R2 sanal makinasının sunduğu internet sayfası şu şekildedir:



Ana makinadan web sunucusundaki deneme.html dosyasına erişmeye çalıştığımızda şu http response'u dönmektedir:

http://172.16.3.128/deneme.html // Not: IIS'in varsayılan sayfası http response  
// dönmediği için deneme.html kullanılmıştır.

Http Response:

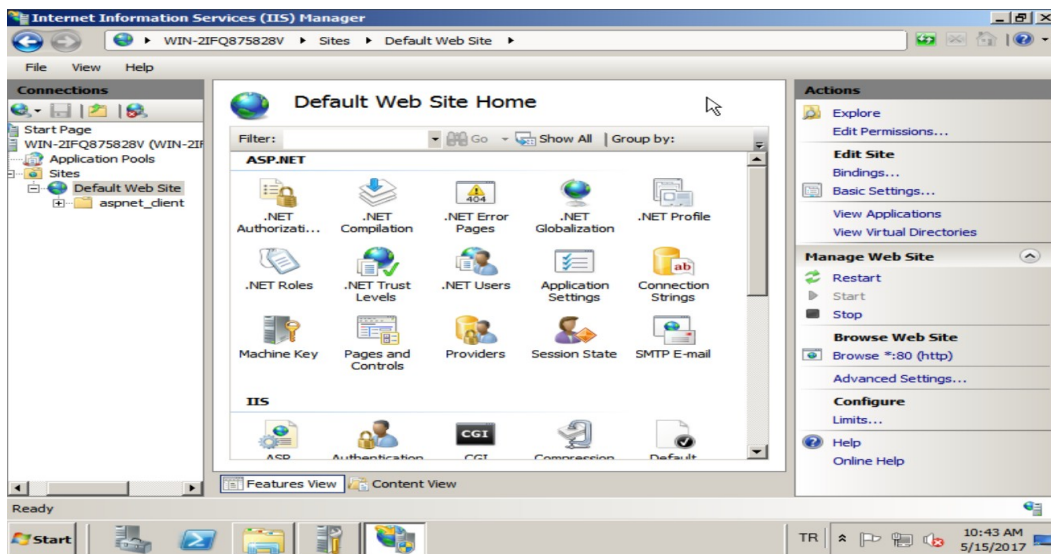
```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 12 May 2017 13:18:56 GMT
Accept-Ranges: bytes
ETag: "c6f6264f22cbd21:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 15 May 2017 07:38:45 GMT
Connection: close
Content-Length: 689
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
...
```

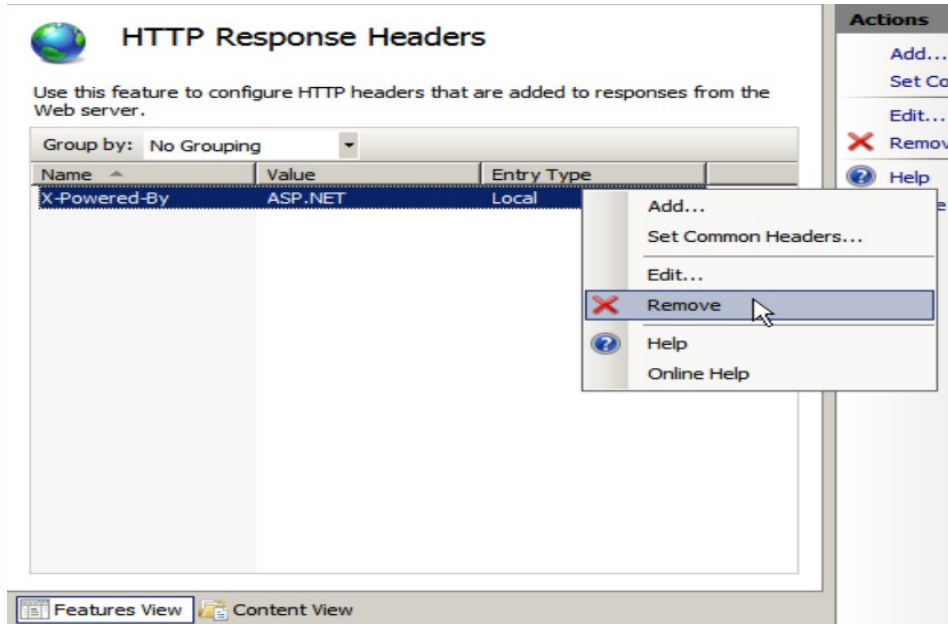
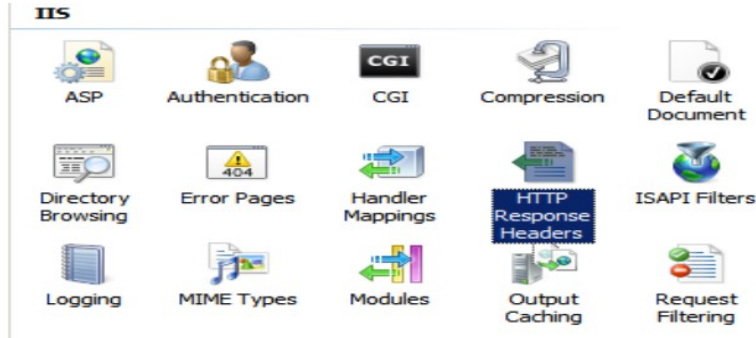
Görüldüğü üzere web sunucusu X-Powered-By header'ı ve Server header'ı ile bilgi ifşasında bulunmuştur. Şimdi bu bilgi ifşalarını sırayla durduralım.

#### a. X-Powered-By Başlığını Kapatma

Web framemwork bilgisinin (X-Powered-By başlığının) kullanıcılara gönderilmesini engellemek için sunucudaki IIS Manager paneli açılır.



Paneldeki Http Response Headers ögesine tıklanılır ve X-Powered-By başlığı silinir.



Ana makinadan tekrar hedef web sunucusuna bağlandığımızda dönen http yanıtının header'ı şöyle olacaktır:

Http Response:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 12 May 2017 13:18:56 GMT
Accept-Ranges: bytes
ETag: "c6f6264f22cbd21:0"
Server: Microsoft-IIS/7.5
```

// X-Powered-By header'ı kalkmıştır.

Date: Mon, 15 May 2017 07:50:20 GMT  
Connection: close  
Content-Length: 689

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />  
<title>IIS7</title>  
  <style type="text/css">  
<!--
```

Görüldüğü üzere X-Powered-By header'ı kalkmıştır. Bu header'ı silmek yerine yanıltıcı bir değer ile de doldurabilirdik. Bu tercihe kalmıştır.

## b. Server Header'ını Kapatma

Web sunucu yazılımı bilgisinin (Server başlığının) kullanıcılara gönderilmesini engellemek için sunucuya urlscan tool'u indirilmelidir.

```
# Microsoft URL Rewrite Module 2.0 for IIS 7 (x64)  
https://www.microsoft.com/en-us/download/details.aspx?id=7435 // Ubuntu 18.04 LTS  
// ~/Downloads/  
// Windows Server  
// 2008 R2.rar  
// içerisinde bu exe var.
```

```
# Microsoft URL Rewrite Module 3.1 for IIS 7 (x64)  
https://download.cnet.com/UrlScan-for-IIS-64-bit/3000-10248_4-75451809.html  
// Ubuntu 18.04 LTS  
// ~/Downloads/  
// Windows Server  
// 2008 R2.rar  
// içerisinde bu exe var.
```

Uyarı: Bu makale yazıldıktan epey sonra makale tekrar tatbik edildiğinde UrlScan 2.0 ile UrlScan.ini dosyası ilgili dizinde oluşmamıştır ve bu nedenle server header'ının tamamen gönderilmemesi yapılamamıştır. Bu nedenle UrlScan 3.1 kurulmuştur ve UrlScan.ini dosyası üzerinden server header'ının tamamen gönderilmemesi uygulanabilmiştir. Fakat UrlScan 3.1'de rewrite kural syntax'ı farklı olduğundan server header 'ını farklı bir değerle doldurma kuralı syntax hatası vermiştir. Bu nedenle UrlScan 3.1 ile eski UrlScan 2.0 beraber kurulmuştur. Böylece makalede belirtilen kural syntax'ında server header değerini değiştirme uygulanabilmiştir.

Not: Sanal makinedeki Internet Explorer 8 hiçbir siteden exe dosyası indiremediği için www.includekarabuk.com sitesine firefox.exe atılmıştır. Ardından Internet Explorer ile www.includekarabuk.com sitesine gidilmiştir. Tarayıcıdan Tools->Internet Options-

>Security sekmelerine geçip Trusted Site ikonuna tıklanılmıştır. Ardından Sites butonuna tıklayıp Add butonu ile www.includekarabuk.com güvenilir site olarak eklenmiştir. Ok butonuna basıp www.includekarabuk.com/firefox.exe linkinden firefox indirilmiştir.

Firefox ile URLScan tool'u indirildikten sonra urlscan kurulumuna geçmeden önce bir feature yüklemesinde bulunmamız gerekmektedir. Feature'un adı IIS 6 Metabase Compatibility şeklindedir. Bu feature'u IIS servisimize yüklemek için

- Başlat çubuğuna basılır
- Arama kutucuğuna Administrative Tools yazılır ve Administrative Tools'a tıklanılır
- Ekranaya gelen penceredeki Server Manager öğesine tıklanılır
- Soldaki Roles -> Web Server (IIS) hiyerarşisinden Web Server (IIS)'e sağ tıklanılır ve Add Role Services denir.
- Ekranaya gelen checkbox'lardan Web Server (IIS) -> Management Tools 'daki IIS 6 Management Compatibility'ye ve IIS Management Console'a tick atılır.
- Son olarak Next ve Install denir.

IIS 6 Metabase Compatibility özelliği IIS'e eklendikten sonra urlscan.exe dosyası ile kurulumu geçilir. Kurulum sonrası ;

i) Normal Http Talepleri + Anormal Http Talepleri için Server Header'ını Yollamama

Sistem tamamen kapatılır ve yeniden açılır. Ardından C:\inetpub\wwwroot\ dizini altında web.config dosyası oluşturulmalıdır ve dosya içeriği aşağıdaki gibi olmalıdır:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <outboundRules>
        <rule name="Remove_RESPONSE_Server">
          <match serverVariable="RESPONSE_Server" pattern=".+"/>
          <action type="Rewrite" value="Yuppii"/>
        </rule>
      </outboundRules>
    </rewrite>
  </system.webServer>
</configuration>
```

Eğer C:\inetpub\wwwroot\ dizini altında zaten web.config konfigürasyon dosyanız varsa bu durumda mevcut web.config dosyanız içerisindeki <configuration> etiketleri arasına <system.webServer> ... </system.webServer> etiketlerini yerleştirip arasına yukarıda belirtilen satırları girebilirsiniz.

Yukarıdaki web.config üzerinde yapılan kodlama işlemleri sonrası dosyanızı kaydedin ve IIS Manager üzerinden IIS servisinizi yeniden başlatın. Böylece normal http paketlerinde Server

başlığını göndermediğiniz gibi anormal http başlıklarında da Server başlığını göndermemiş olacaksınız.

>> Durum I:

Http Request:

GET / HTTP/1.0  
Host: 172.16.3.128  
...

Http Response:

200 OK  
Content-Type: text/html  
Last-Modified: Mon, 15 May 2017 11:32:08 GMT  
Accept-Ranges: bytes  
ETag: "1ef0afe26ecdd21:0"  
Date: Mon, 15 May 2017 12:35:34 GMT  
Connection: close  
Content-Length: 689

**// Server header'ı kalkmıştır.**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <title>IIS7</title>
<style type="text/css">
```

>> Durum II:

Http Request (Anormal and/or Erroneous) :

QQQQQQQQQ / HTTP/1.0  
Host: 172.16.3.128  
...

Http Response:

405 Method Not Allowed  
Content-Type: text/html  
Last-Modified: Mon, 15 May 2017 11:32:08 GMT  
Accept-Ranges: bytes  
ETag: "1ef0afe26ecdd21:0"

**// Server header'ı kalkmıştır.**

Date: Mon, 15 May 2017 12:35:34 GMT  
Connection: close  
Content-Length: 689

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />  
  <title>IIS7</title>  
<style type="text/css">
```

Görüldüğü üzere bilgi ifşası yapan Server header'ı normal http paketlerine karşılık gönderilen http yanıtlarında ve aynı zamanda - hataya sebebiyet verecek - anormal http paketlerine karşılık gönderilen http yanıtlarında da kalkmıştır. Böylece IIS sistemlerde, kullanılan teknolojiye dair bilgi ifşalarının önüne geçilebilir.

ii) Sadece Normal Http Talepleri için Server Http Header'ını Yollamama

Kurulum sonrası URLScan.ini dosyası metin editörü ile açılır. Bu dosya genellikle %WINDIR%\System32\Inetsrv\URLscan dizininde yer alır.

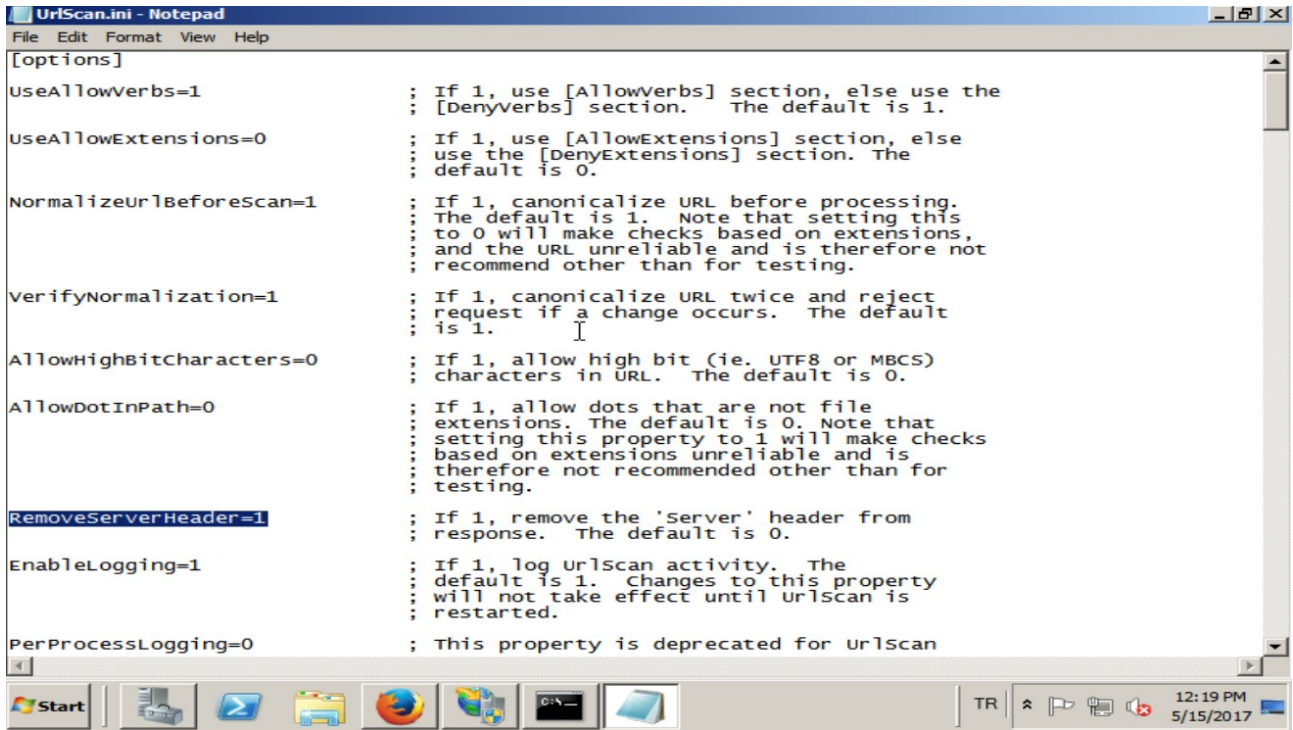
// Konsolu Run As Administrator ile başlatmalısın.

Windows Server 2008 R2 Console:

```
C:\Users\hasan > cd ..  
C:\Users > cd ..  
C:\ > cd Windows  
C:\Windows > cd System32  
C:\Windows\System32 > cd inetsrv  
C:\Windows\System32\inetsrv > cd urlscan  
C:\Windows\System32\inetsrv\urlscan > notepad UrlScan.ini
```

Not: Başlat menüsünden CMD'ye sağ tık yapıp Run As Administrator diyerek konsol başlatılmalıdır. Diğer türlü notepad güncelleme yapamıyor ve Access Denied hatası veriyor.

URLScan.ini dosyası yukarıdaki kodlamalar ile açıldıktan sonra RemoveServerHeader satırı 1 yapılır.



```
[options]
UseAllowVerbs=1           ; If 1, use [AllowVerbs] section, else use the
                          ; [DenyVerbs] section. The default is 1.
UseAllowExtensions=0      ; If 1, use [AllowExtensions] section, else
                          ; use the [DenyExtensions] section. The
                          ; default is 0.
NormalizeUrlBeforeScan=1  ; If 1, canonicalize URL before processing.
                          ; The default is 1. Note that setting this
                          ; to 0 will make checks based on extensions,
                          ; and the URL unreliable and is therefore not
                          ; recommend other than for testing.
VerifyNormalization=1    ; If 1, canonicalize URL twice and reject
                          ; request if a change occurs. The default
                          ; is 1.
AllowHighBitCharacters=0  ; If 1, allow high bit (ie. UTF8 or MBCS)
                          ; characters in URL. The default is 0.
AllowDotInPath=0         ; If 1, allow dots that are not file
                          ; extensions. The default is 0. Note that
                          ; setting this property to 1 will make checks
                          ; based on extensions unreliable and is
                          ; therefore not recommended other than for
                          ; testing.
RemoveServerHeader=1     ; If 1, remove the 'Server' header from
                          ; response. The default is 0.
EnableLogging=1          ; If 1, log urlscan activity. The
                          ; default is 1. Changes to this property
                          ; will not take effect until urlscan is
                          ; restarted.
PerProcessLogging=0      ; This property is deprecated for urlscan
```

Ardından dosya kaydedilir ve sistem restartlanır. Ana makinedan tekrar hedef web sayfasına (deneme.html'e) bağlanmaya çalıştığımızda ise http response şu şekli alacaktır:

>> Durum I:

Http Request:

```
GET / HTTP/1.0
Host: 172.16.3.107
...
```

Http Response:

```
200 OK
Content-Type: text/html
Last-Modified: Mon, 15 May 2017 11:32:08 GMT
Accept-Ranges: bytes
ETag: "1ef0afe26ecdd21:0"
Date: Mon, 15 May 2017 12:35:34 GMT
Connection: close
Content-Length: 689
```

**// Server header'ı kalkmıştır.**

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <title>IIS7</title>
<style type="text/css">
```



>> Durum II:

Http Request (Anormal and/or Erroneous) :

QQQQQQQQQQ / HTTP/1.0  
Host: 172.16.3.107  
...

Http Response:

405 Method Not Allowed  
Content-Type: text/html  
Last-Modified: Mon, 15 May 2017 11:32:08 GMT  
Accept-Ranges: bytes  
ETag: "1ef0afe26ecdd21:0"  
Server: IIS/7.5 // **Maalesef server header'ı halen geliyor.**  
Date: Mon, 15 May 2017 12:35:34 GMT  
Connection: close  
Content-Length: 689

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
```

Görüldüğü üzere bilgi ifşası yapan Server header'ı normal http paketlerine karşılık gönderilen http yanıtlarında kalkmıştır. Böylece IIS sistemlerde, kullanılan teknolojiye dair bilgi ifşalarının önüne geçilebilir.

## Ekstra

(+) Bu başlık birebir denenmiştir ve başarıyla uygulanmıştır.

Bahsedilen IIS sunucu bilgi ifşalarını önlemenin bir de otomatize çözümü vardır. Bu çözüm bir IIS Managed (yani üçüncü taraf olmayan, Microsoft'un resmi diye kabul ettiği) **IIS Remove Server Headers** (by Pingfu) modülüdür.

Gereksinimler

Ubuntu // Ana Makina  
Windows Server 2012 R2 // Web Sunucusu  
RemoveServerHeaderModule-1.0.1-x86.msi.zip

Not: IIS Remove Server Headers (by Pingfu) exe'leri (x64 ve x86)

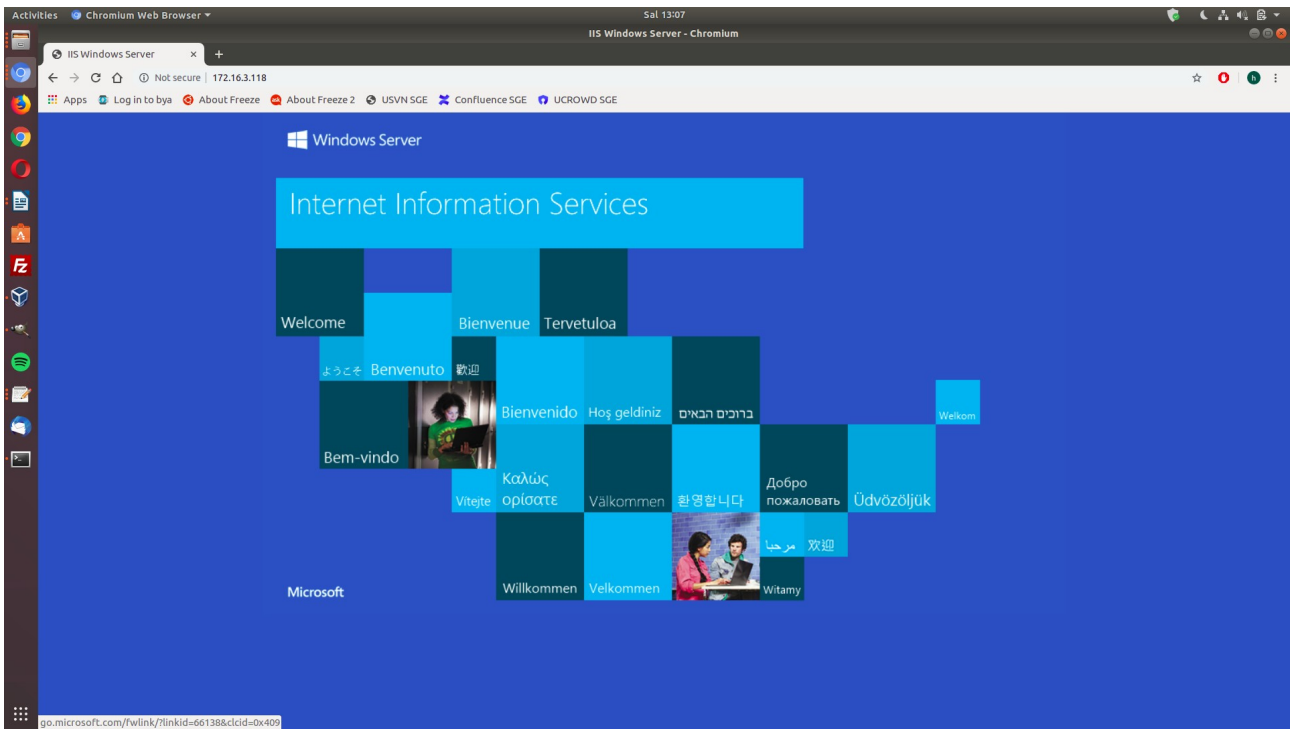
Downloads/Windows Server 2008 R2.zip klasöründe mevcuttur. Ayrıca <https://github.com/pingfu/iis-remove-server-headers#download> adresinden indirilebilir.

Bu managed IIS modülü sunucuya yüklendiğinde ve IIS yönetim panelinde yapılacak ufak bir konfigürasyon ayarı ile modül IIS'te aktif hale gelecektir. IIS sunucu restart'landığında ise web sunucudan dışarıya

Server  
X-Powered-By  
X-AspNet-Version  
X-AspNetMvc-Version

başlıklarının çıkışı artık engellenmiş olacaktır. Şimdi bu aracı Windows Server 2012 R2'ye kuralım ve sunucu bilgi ifşalarının önüne geçişini gözlemleyelim.

Windows Server 2012 R2 sanal makinasının sunduğu internet sayfası şu şekildedir:



Ana makinadan web sunucusundaki deneme.html dosyasına erişmeye çalıştığımızda şu http response'u dönmektedir:

Ubuntu 18.04 LTS Terminal:

```
> telnet 172.16.3.118 80
GET / HTTP/1.0
Host: 172.16.3.113
```

```
Output:
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 12 May 2017 13:18:56 GMT
```

Accept-Ranges: bytes  
ETag: "c6f6264f22cbd21:0"  
Server: Microsoft-IIS/8.5  
X-Powered-By: ASP.NET  
Date: Mon, 15 May 2017 07:38:45 GMT  
Connection: close  
Content-Length: 689

oylesine bir icerik :::::

Connection closed by foreign host.

Görüldüğü üzere web sunucusu Server header'ı ve X-Powered-By header'ı ile bilgi ifşasında bulunmuştur. Şimdi bu bilgi ifşalarını otomatize aracı kurarak durduralım.

IIS Managed Remove Server Headers Modülünün Uyumluluğu Hk.

-----  
(\* ) Windows Server 2012 ve sonraki sürümlere hitap etmektedir.

IIS Remove Server Headers modülü .NET 2.0 ile çalıştığından .NET 2.0'ı içeren .NET 3.5 feature'unun Windows Server 2012 ve sonrasında IIS'e feature olarak eklenmesi gerekmektedir. Çünkü Windows Server 2012 ve sonrasında hazır kurulu gelen .NET framework versiyonu .NET 4.5 tir ve .NET 3.5 seçime bağlı olarak sonradan eklenebilir halde hazır kurulu gelmemektedir. Ayrıca Windows Server 2012 ve sonrasında IIS Remove Server Headers modülünün ihtiyaç duyduğu ISAPI Filters ve ISAPI Extensions feature'ları Windows Server 2008 ve öncesinde default kuruluken sonrasında kurulu olarak gelmediğinden ilave feature olarak eklenmeleri gerekmektedir.

Server Manager

Roles and Features

Web Server (IIS) -> Web Server -> Application Development	
+ .NET 3.5 Extensibility	(* ) Gerekli
+ .NET 4.0 Extensibility	(* ) Seçime Bağlı (optional)
+ ASP	(* ) Gerekli
+ ASP.NET 3.5	(* ) Gerekli
+ ASP.NET 4.5	(* ) Seçime Bağlı (optional)
+ ISAPI Extentions	(* ) Gerekli
+ ISAPI Filters	(* ) Gerekli

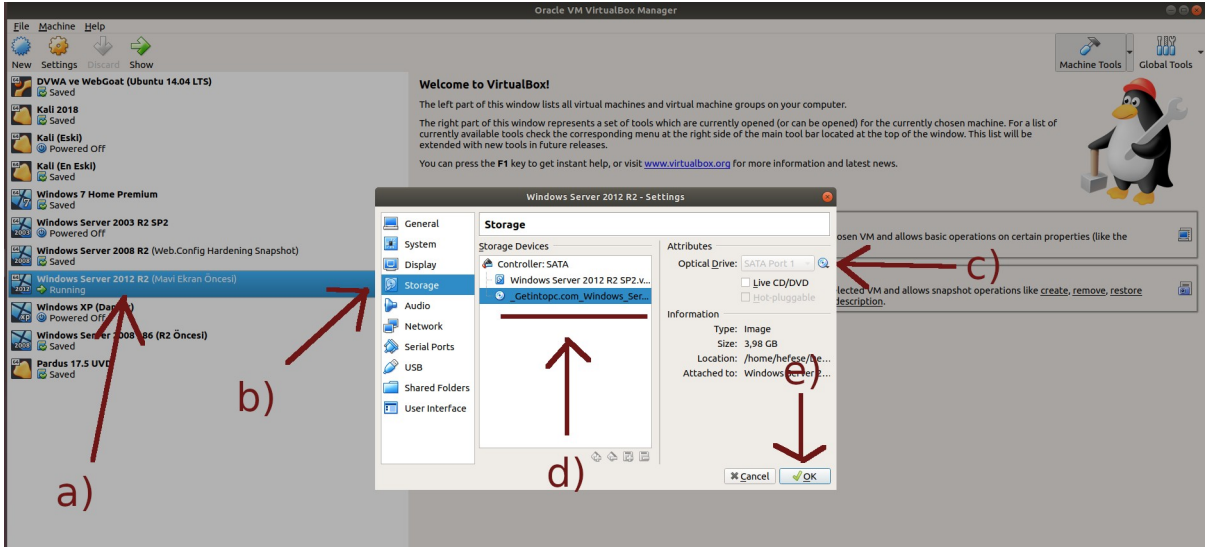
[!] Uyarı:

Bu yüklemeler için Windows Server Kurulum DVD'si takılmalıdır ve IIS feature eklemeleri sırasında kurulum kaynak dosyası yolu için DVD'nin takılı olduğu sürücü ve akabinde \sources\sxs\ dizin yolu gösterilmelidir. Ancak bu sayede, kurulum başarıyla tamamlanabilecektir.

Kurulum sonrası IIS Remove Headers modülünü IIS panele ekleme işlemi sorunsuzca gerçekleşip modül, bilgi ifşası sunan sunucu başlıklarının gönderimini engelleyebilecektir.

-----  
Adım I: RemoveServerHeader modülünün ihtiyaç duyduğu .net framework sürümü (ihtiyaç

duyulan 2.0 sürümünü içerdğinden 3.5 sürümü) ve ISAPI Filters feature'larını IIS'e yüklemek için Windows Server kurulum DVD'si takılır.



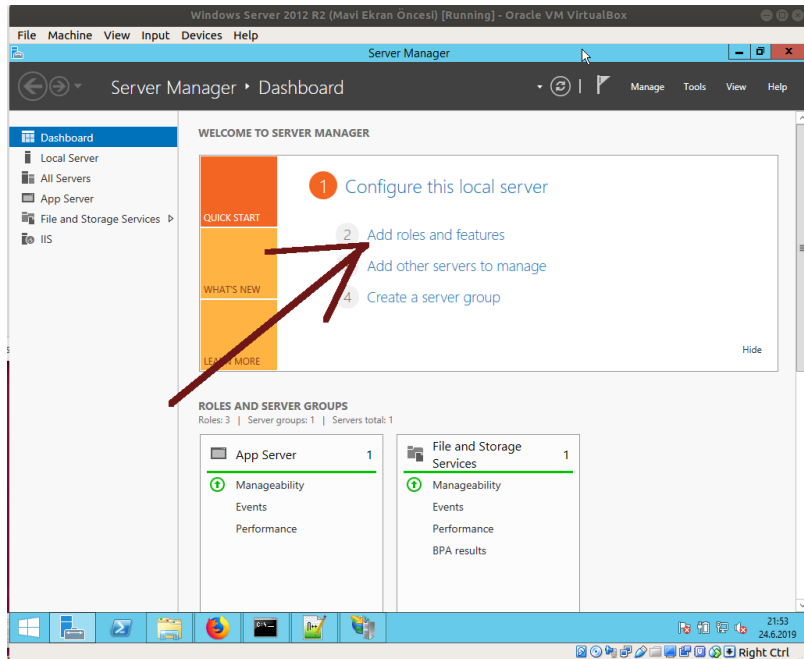
Ardından Server Manager açılır. “Add Roles And Features”dan Server Roles penceresine gelindiğinde

Web Server (IIS) -> Web Server -> Application Development

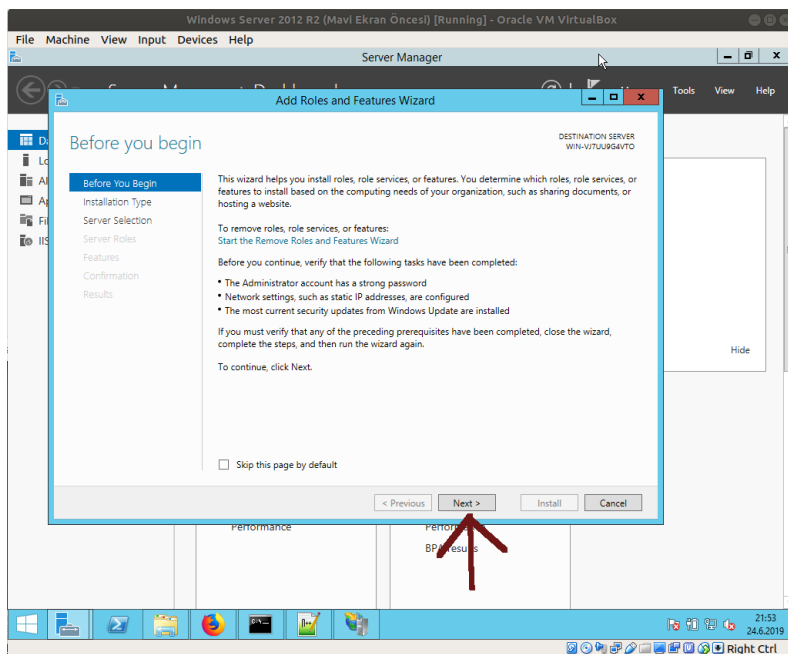
seçeneklerine gidilir ve

- |                        |                             |
|------------------------|-----------------------------|
| .NET 3.5 Extensibility | (*) Gerekli                 |
| .NET 4.0 Extensibility | (*) Seçime Bağlı (optional) |
| ASP                    | (*) Gerekli                 |
| ASP.NET 3.5            | (*) Gerekli                 |
| ASP.NET 4.5            | (*) Seçime Bağlı (optional) |
| ISAPI Extentions       | (*) Gerekli                 |
| ISAPI Filters          | (*) Gerekli                 |

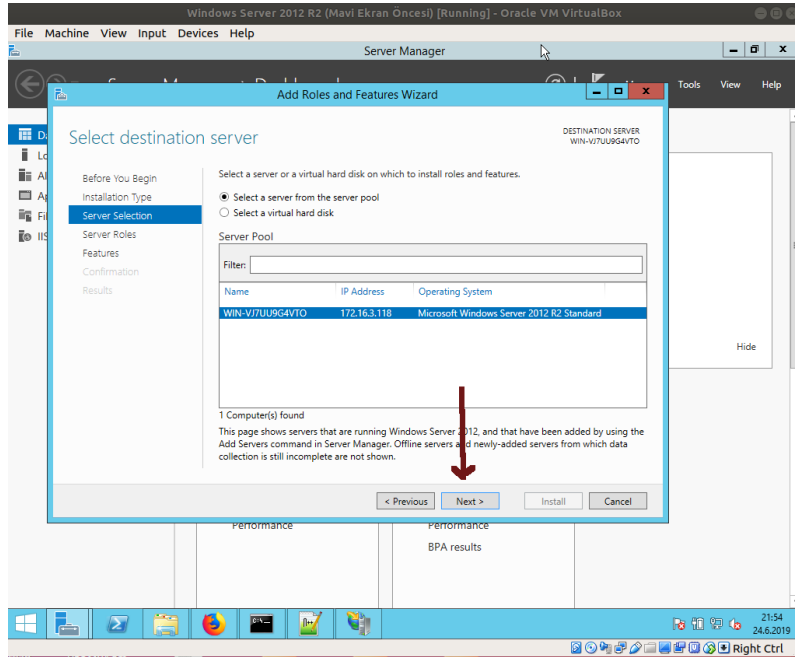
seçenekleri işaretlenir.



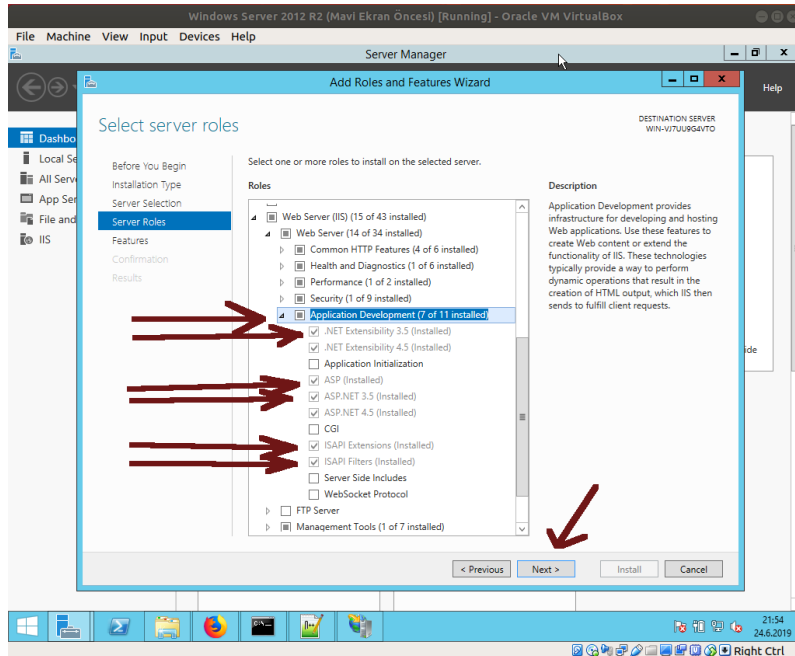
( Add Roles and Features )



( Next )

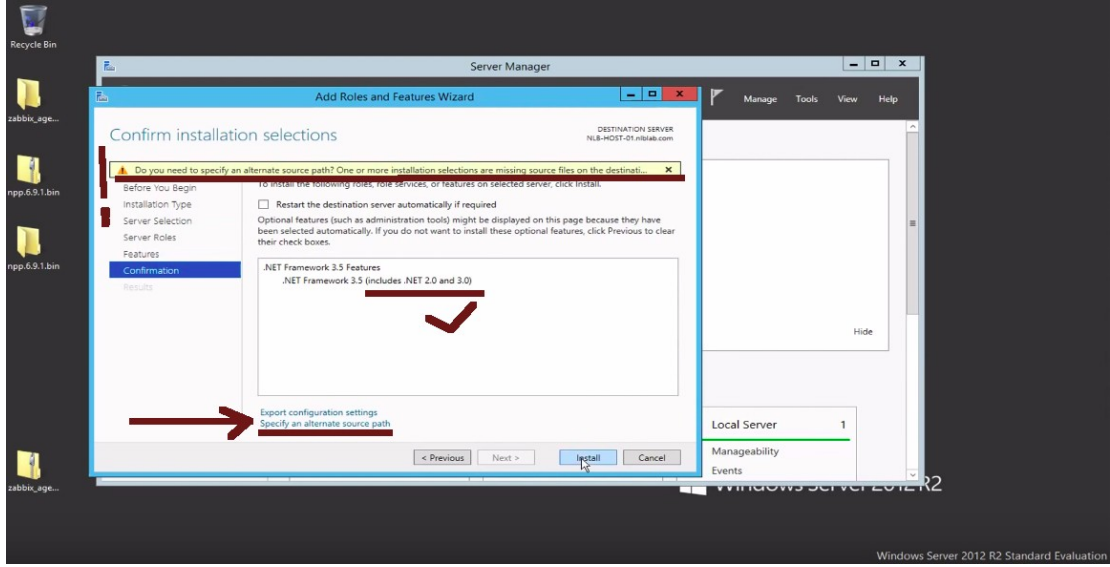


( Next )



( Yüklenen Feature'lar İşaretlemesi )

Ardından yüklenenler listesi ekrana gelir. Bu ekranda bir uyarı görünecektir: "... One or more installation selections are missing source files on the destination...".



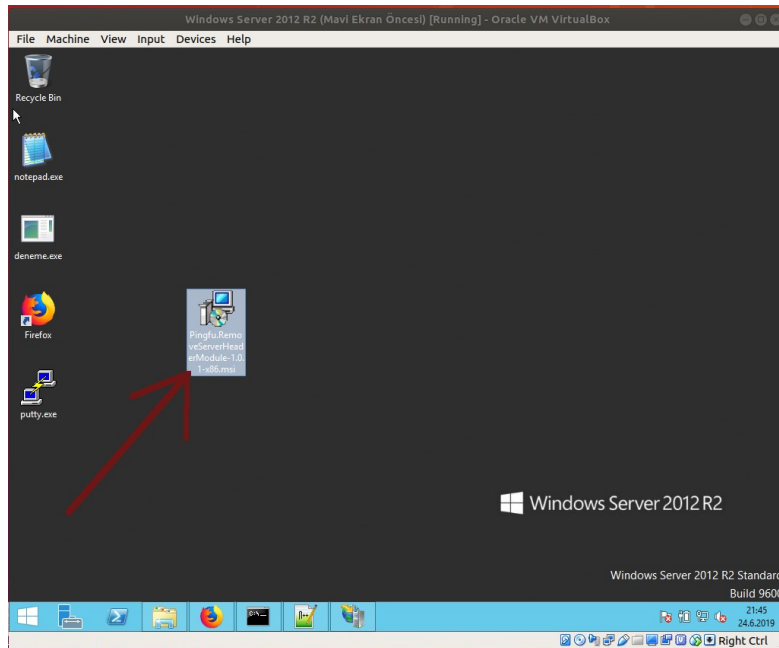
Bu ekrandaki uyarıda söylenmek istenen şey yüklenecekler listesindeki bazı bileşenlerin (örn; .NET Framework 3.5'in) Windows Server kurulum DVD'sinin sources\sxs\ dizininde yer alan kurulum dosyalarına ihtiyaç duymasındır. Dolayısıyla ekrandaki "Specify an alternate source path" linkine tıklayıp gelen ekrandaki source path textbox'ına Windows Server kurulum DVD'si ve sources\sxs\ dizin yolu girilmelidir ve sonra kurulum başlanmalıdır. Böylece yükleme sorunsuz gerçekleşecektir.

Kurulum Dosyaları Path'i (örn):

D:\sources\sxs\

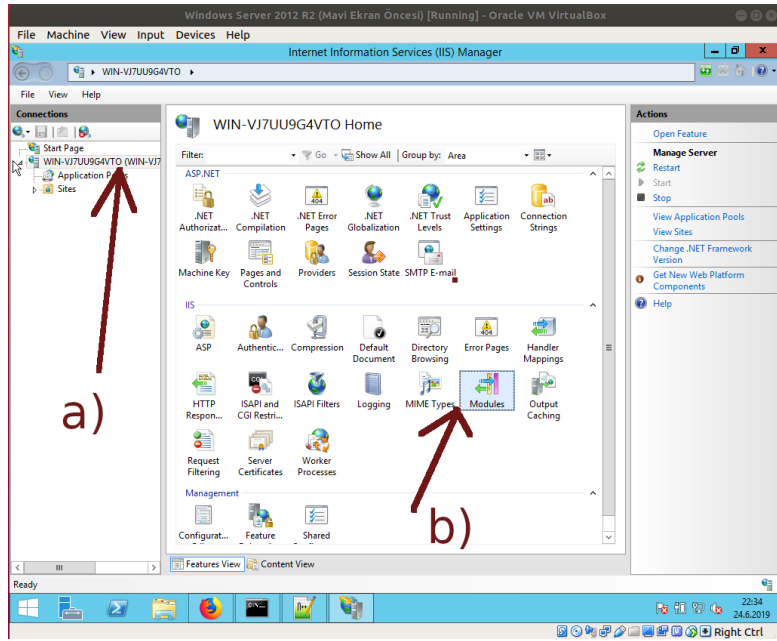
// D sürücüsü DVD'nin Olduğu Sürücü

Adım II: RemoveServerHeader Modülü kurulum ve sonra sistem restart'lanır.

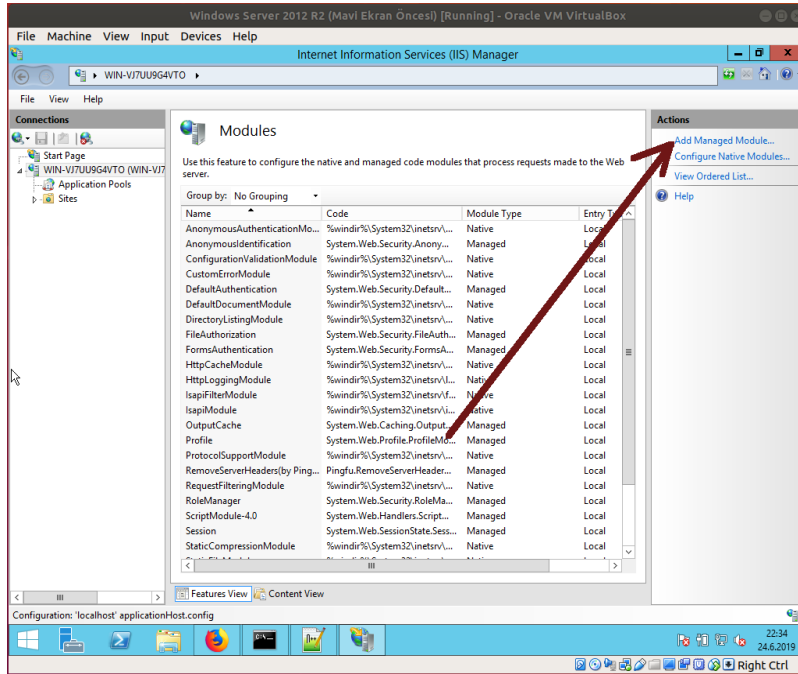


Adım III: Ardından IIS Manager açılır ve Server level'da olan (yani application level'da olan değil,

Server level’da olan) Modules’e girilir.

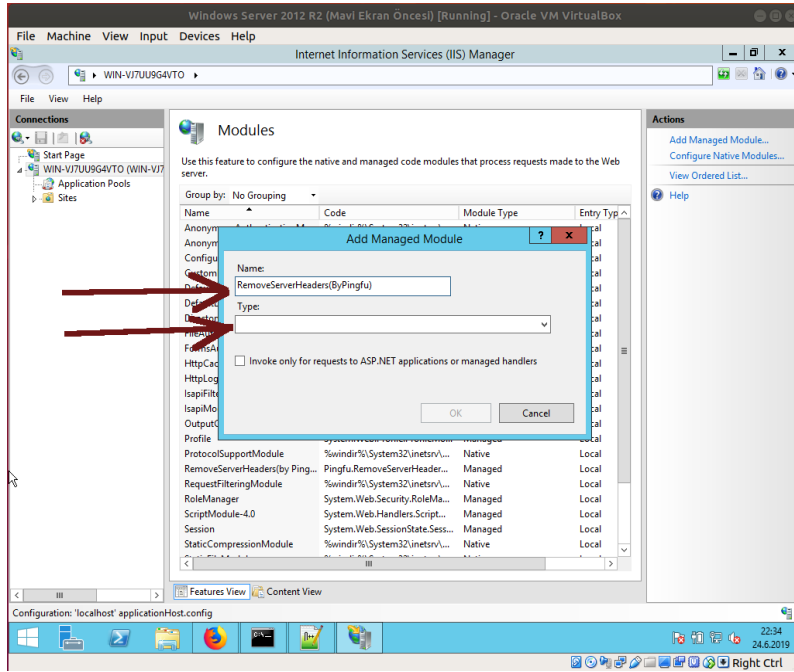


Adım IV: Add Managed Module.. seçeneğine tıklanır.

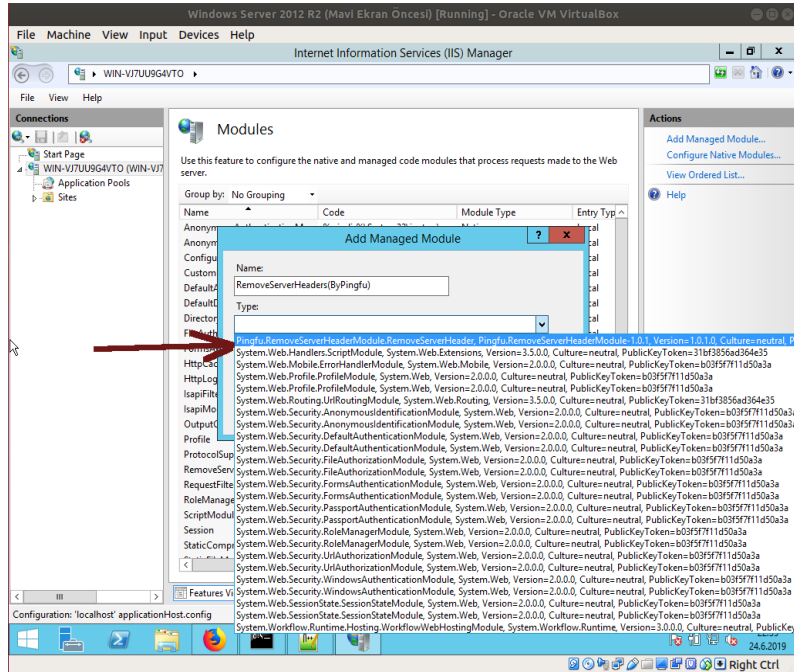


Adım V: Modül ismi olarak keyfi bir (tanımlayıcı) ifade girilir. Modül türü olarak da Windows Server 2012 R2’ye exe’siyle kurduğumuz modül seçilerek konur.

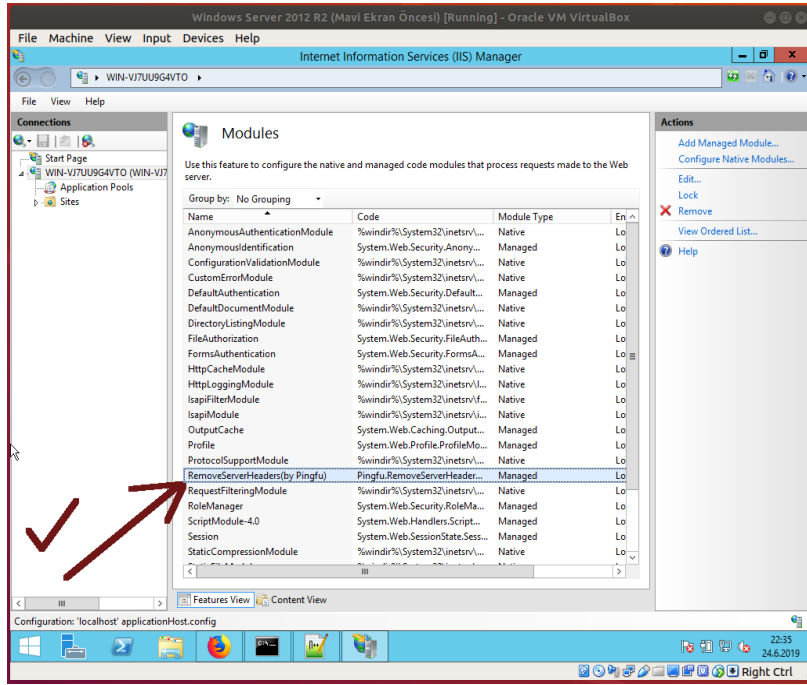




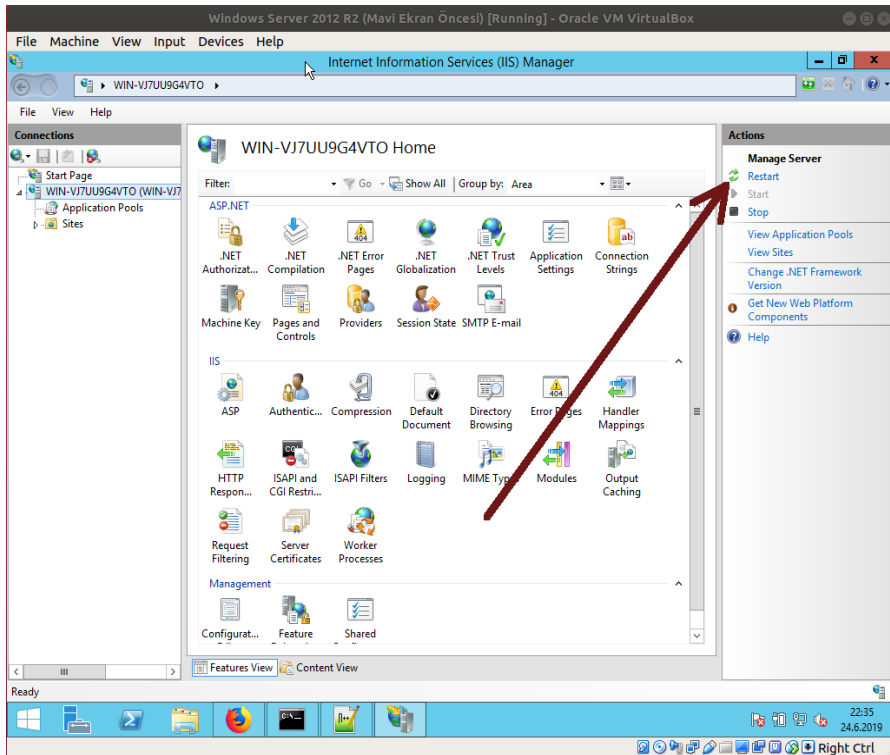
(Keyfi / Tanımlayıcı Modül İsmi Girilir )



( Windows Server 2012 R2'ye exe'siyle yüklenen modül seçilir )



( Windows Server 2008'e Kurulan Modül IIS Manager'dan IIS'e Eklenir)



( IIS sunucu restart'lanır ve eklenen modül böylece etkin hale gelir )

Bu adımlar ile IIS sunucunun döndüğü yanıtlardaki bilgi ifşalarının önüne geçilmiş olacaktır:

Ubuntu 18.04 LTS Terminal ( **MODÜL ÖNCESİ** ):

```
> telnet 172.16.3.113 80  
HEAD / HTTP/1.0
```

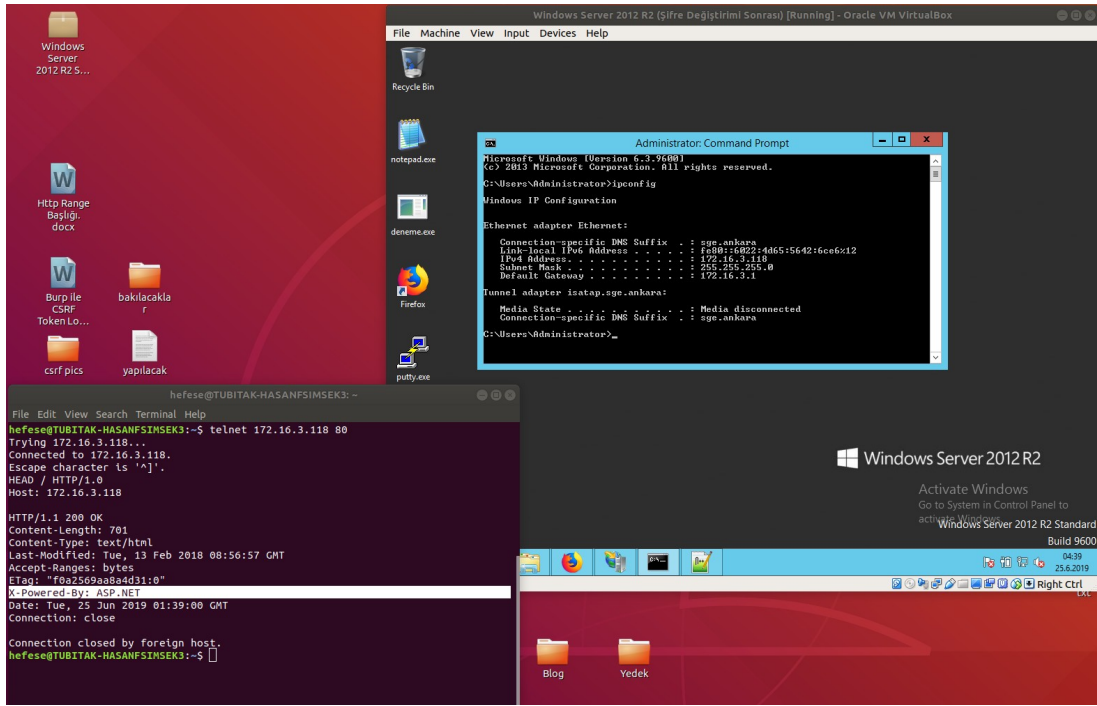
```
Çıktı:  
HTTP/1.1 200 OK  
Content-Length: 689  
Content-Type: text/html  
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT  
Accept-Ranges: bytes  
Etag: "43acgjr0874933dafwq"  
Server: IIS/8.5  
X-Powered-By: ASP.NET  
Date: Mon, 17 Jun 2019, 21:22:36 GMT  
Connection: close  
Connection closed by foreign host.
```

Ubuntu 18.04 LTS Terminal ( **MODÜL SONRASI** ):

```
> telnet 172.16.3.113 80  
HEAD / HTTP/1.0
```

```
Çıktı:  
HTTP/1.1 200 OK  
Content-Length: 689  
Content-Type: text/html  
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT  
Accept-Ranges: bytes  
Etag: "43acgjr0874933dafwq"  
X-Powered-By: ASP.NET  
Date: Mon, 17 Jun 2019, 21:22:36 GMT  
Connection: close  
Connection closed by foreign host.
```

// (-) Halen geliyor.



( Bilgi ifşa eden başlıklardan sadece X-Powered-By kalmış )

NOT 1:

Eğer halen X-Powered-By gelirse ufak bir elle müdahale yapmak ve web.config içerisinde şunu ilave etmek yeterlidir:

web.config

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Böylece şu başlıkların tamamının dışarıyı çıkışı engellenmiş olacaktır.

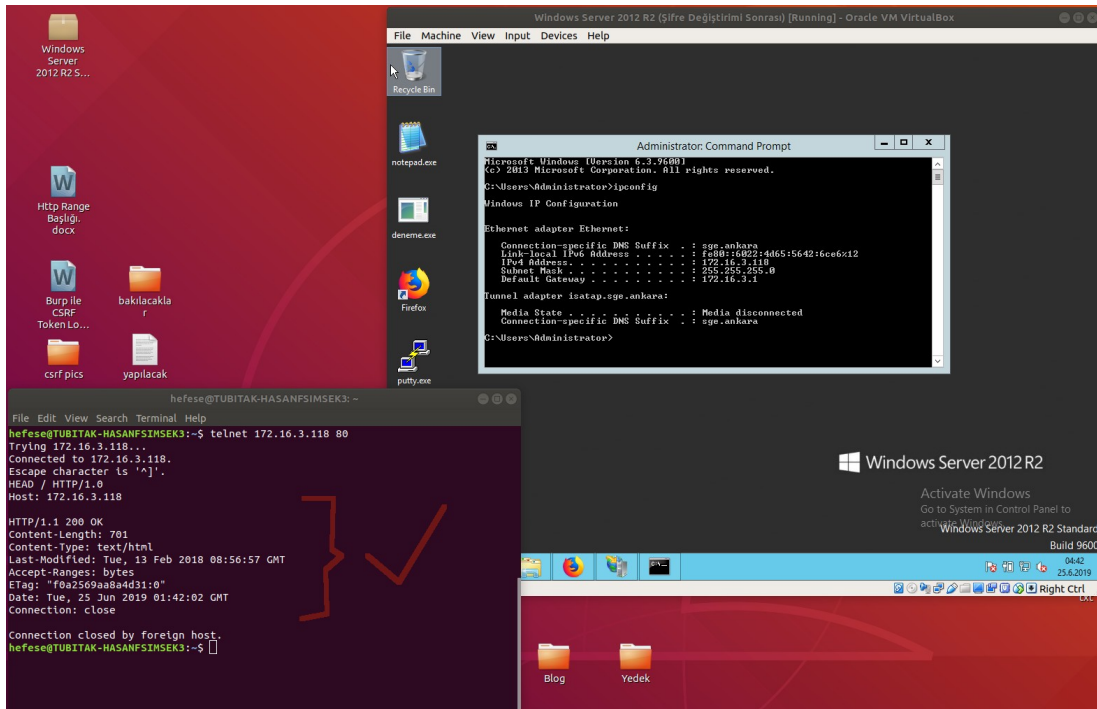
Server  
X-Powered-By  
X-AspNet-Version  
X-AspNetMvc-Version

## Ubuntu 18.04 LTS Terminal ( MODÜL SONRASI ve Web.Config SONRASI ):

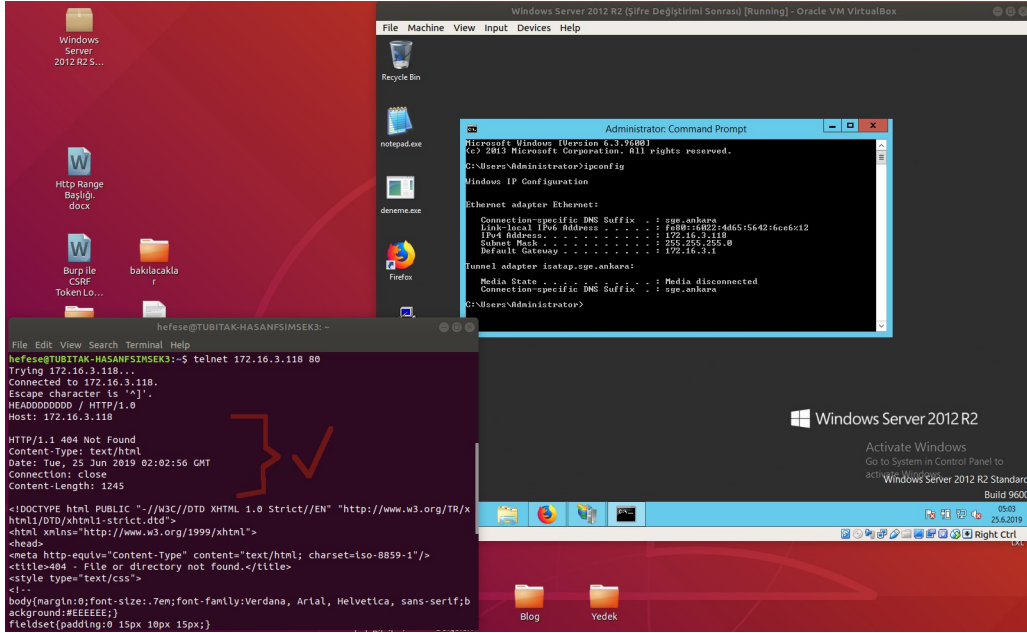
```
> telnet 172.16.3.113 80  
HEAD / HTTP/1.0
```

Çıktı:

```
HTTP/1.1 200 OK  
Content-Length: 689  
Content-Type: text/html  
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT  
Accept-Ranges: bytes  
Etag: "43acgjr0874933dafwq"  
Date: Mon, 17 Jun 2019, 21:22:36 GMT  
Connection: close  
Connection closed by foreign host.
```



( Tüm bilgi ifşa eden başlıklar engellenmiş vaziyette )



( Anormal / Eksik / Hatalı Paket Gönderiminde Dahi Bilgi İfşa Eden Başlıklar Engellenmiş Vaziyette )

## Ekstra 2

(+) Bu başlık birebir denenmiştir ve başarıyla uygulanmıştır.

Bahsedilen IIS sunucu bilgi ifşalarını önlemenin bir de otomatize çözümü vardır. Bu çözüm bir IIS Managed (yani üçüncü taraf olmayan, Microsoft'un resmi diye kabul ettiği) **IIS Remove Server Headers** (by Pingfu) modülüdür.

### Gereksinimler

Ubuntu

Windows Server 2008 R2

RemoveServerHeaderModule-1.0.1-x86.msi.zip

// Ana Makina

// Web Sunucusu

Not: IIS Remove Server Headers (by Pingfu) exe'leri (x64 ve x86) Downloads/Windows Server 2008 R2.zip klasöründe mevcuttur. Ayrıca <https://github.com/pingfu/iis-remove-server-headers#download> adresinden indirilebilir.

Not: Windows Server 2008 R2 işletim sistemine sahip sunucuyu IIS hizmeti sunan bir web sunucusu yapmak için gerekli yapılandırma ayarları için bkz. /home/hefese/Downloads/Windows Server 2008 R2/Windows Server 2008'i Web Sunucusu Yapma.

(!) Uyarı: Windows Server 2008 R2'de web.config'te daha önceden koyduğunuz sıkılaştırma ayarları mevcut olabilir. Bu ayarlar çakışma yapmamaktadır. Fakat eğer <system.web><deployment retail="true"/></system.web> ayarı web.config'deyse (ki yeri web.config değildir, ancak machine.config'te (yani application level'da değil, server level'da) olabilir) bu sıkılaştırma ayarı machine.config'e taşınmalıdır. Diğer tüm web.config'teki sıkılaştırmalar sorunsuzca IIS Remove Server Header Modülü

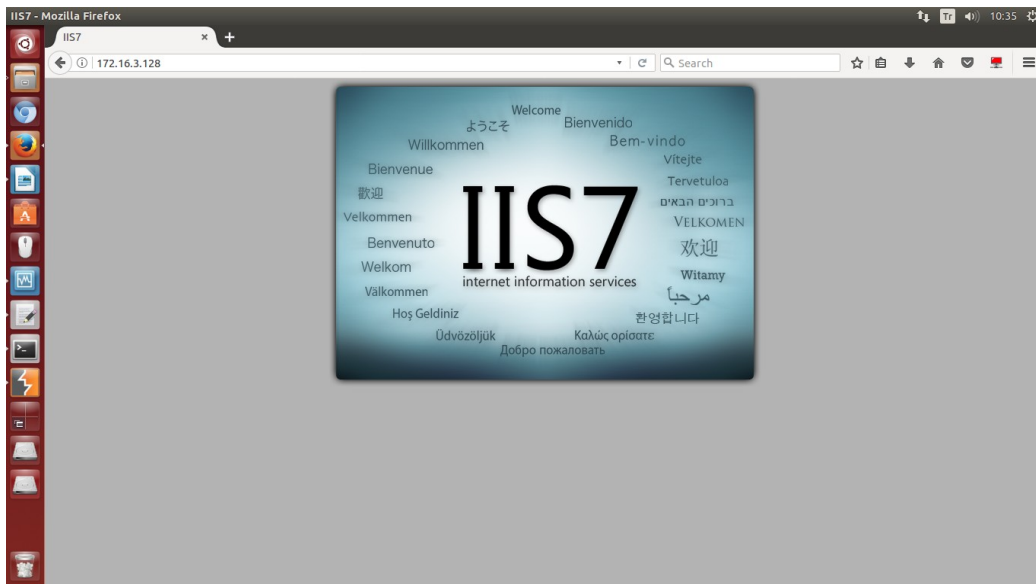
ile beraber çalışabilmektedir.

Bu managed IIS modülü sunucuya yüklendiğinde ve IIS yönetim panelinde yapılacak ufak bir konfigürasyon ayarı ile modül IIS'te aktif hale gelecektir. IIS sunucu restart'landığında ise web sunucudan dışarıya

Server  
X-Powered-By  
X-AspNet-Version  
X-AspNetMvc-Version

başlıklarının çıkışı artık engellenmiş olacaktır. Şimdi bu aracı Windows Server 2008 R2'ye kuralım ve sunucu bilgi ifşalarının önüne geçişini gözlemleyelim.

Windows Server 2008 R2 sanal makinasının sunduğu internet sayfası şu şekildedir:



Ana makinadan web sunucusundaki deneme.html dosyasına erişmeye çalıştığımızda şu http response'u dönmektedir:

Ubuntu 18.04 LTS Terminal:

```
> telnet 172.16.3.113 80  
GET / HTTP/1.0  
Host: 172.16.3.113
```

Output:

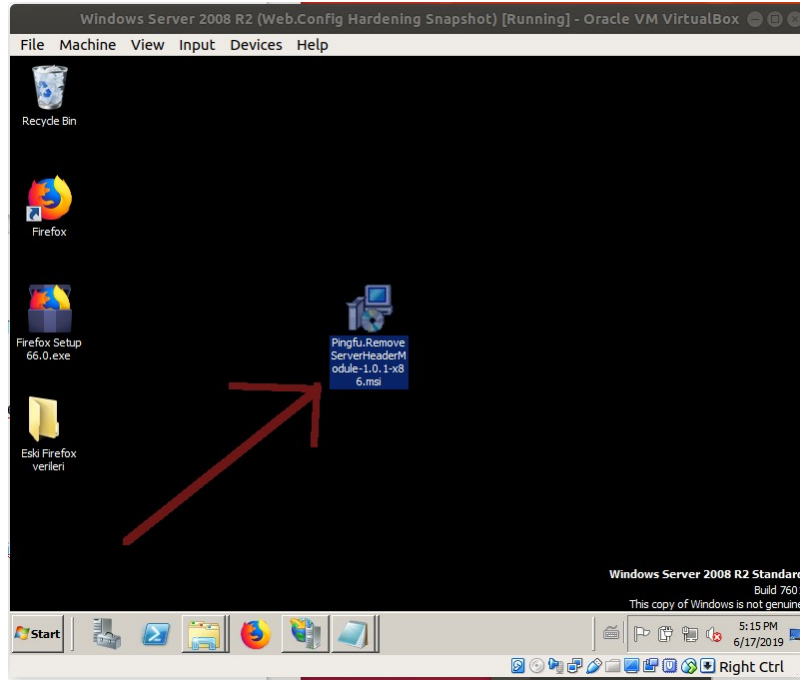
```
HTTP/1.1 200 OK  
Content-Type: text/html  
Last-Modified: Fri, 12 May 2017 13:18:56 GMT  
Accept-Ranges: bytes  
ETag: "c6f6264f22cbd21:0"  
Server: Microsoft-IIS/7.5  
X-Powered-By: ASP.NET  
Date: Mon, 15 May 2017 07:38:45 GMT
```

Connection: close  
Content-Length: 689

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
...
```

Görüldüğü üzere web sunucusu X-Powered-By header'ı ve Server header'ı ile bilgi ifşasında bulunmuştur. Şimdi bu bilgi ifşalarını otomatize aracı kurarak durduralım.

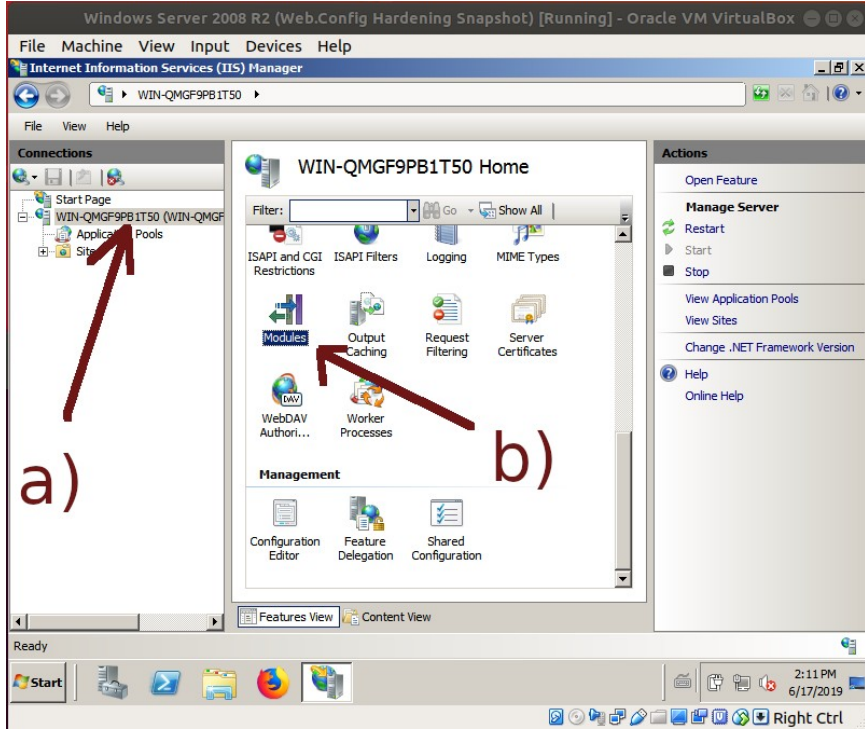
Adım I: RemoveServerHeader Modülü kurulur.



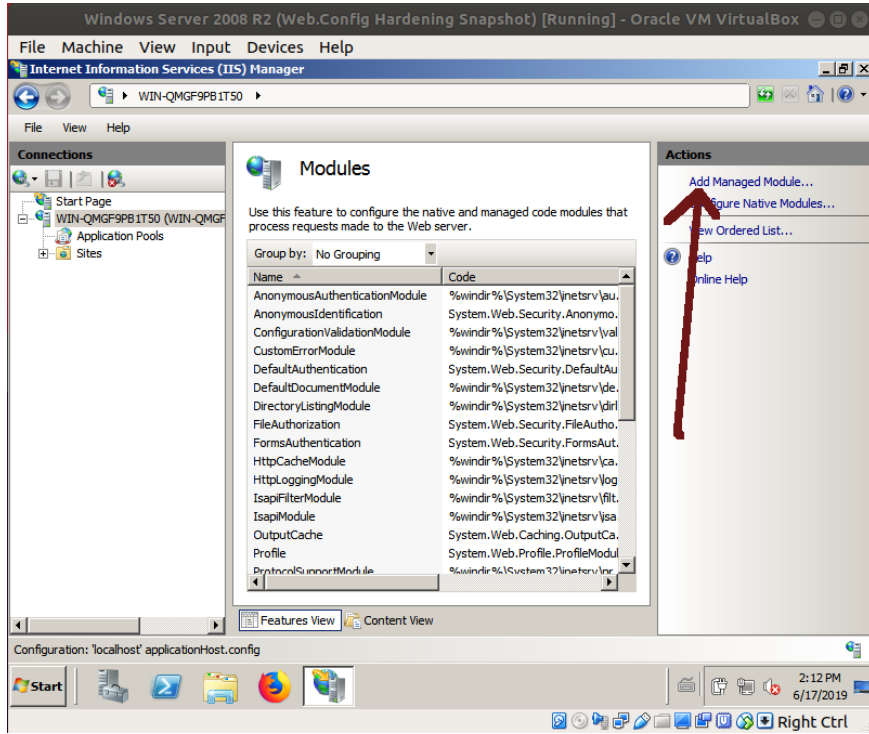
Sonra sistem yeniden başlatılır.

Adım II: Ardından IIS Manager açılır ve Server level'da olan (yani application level'da olan değil, Server level'da olan) Modules'e girilir.

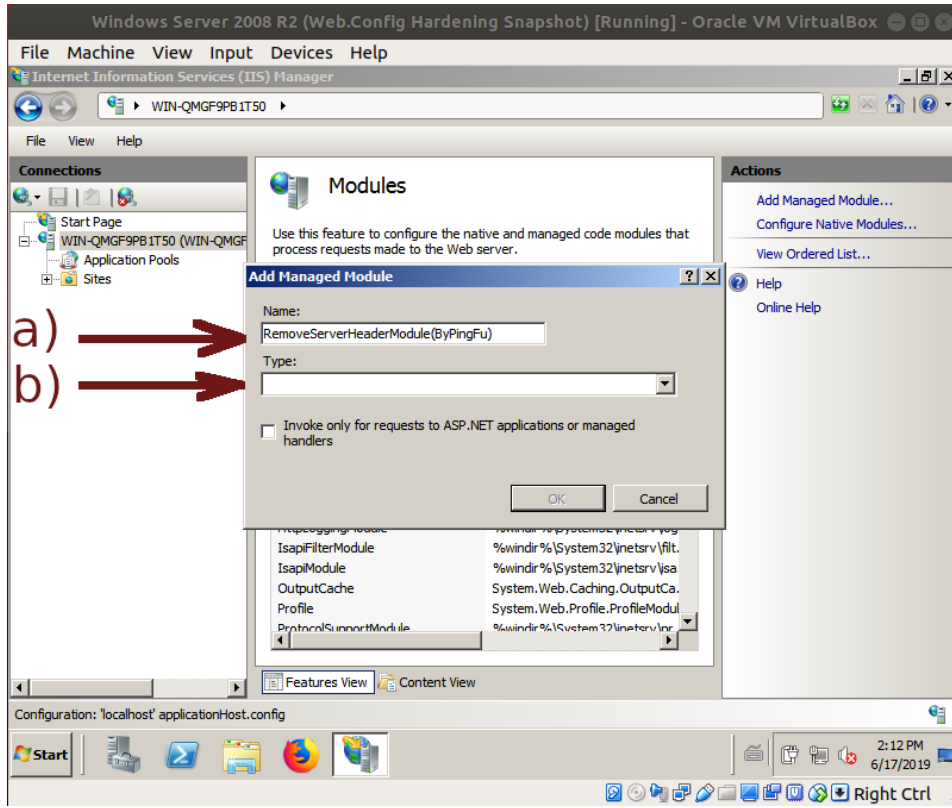




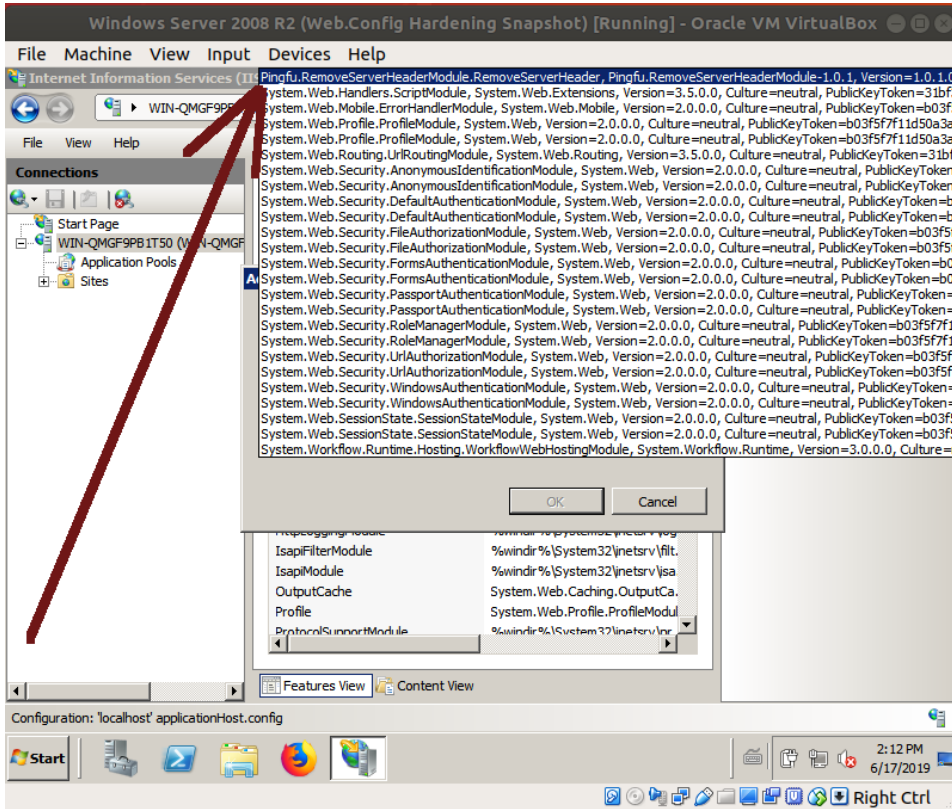
Adım III: Add Managed Module.. seçeneğine tıklanır.



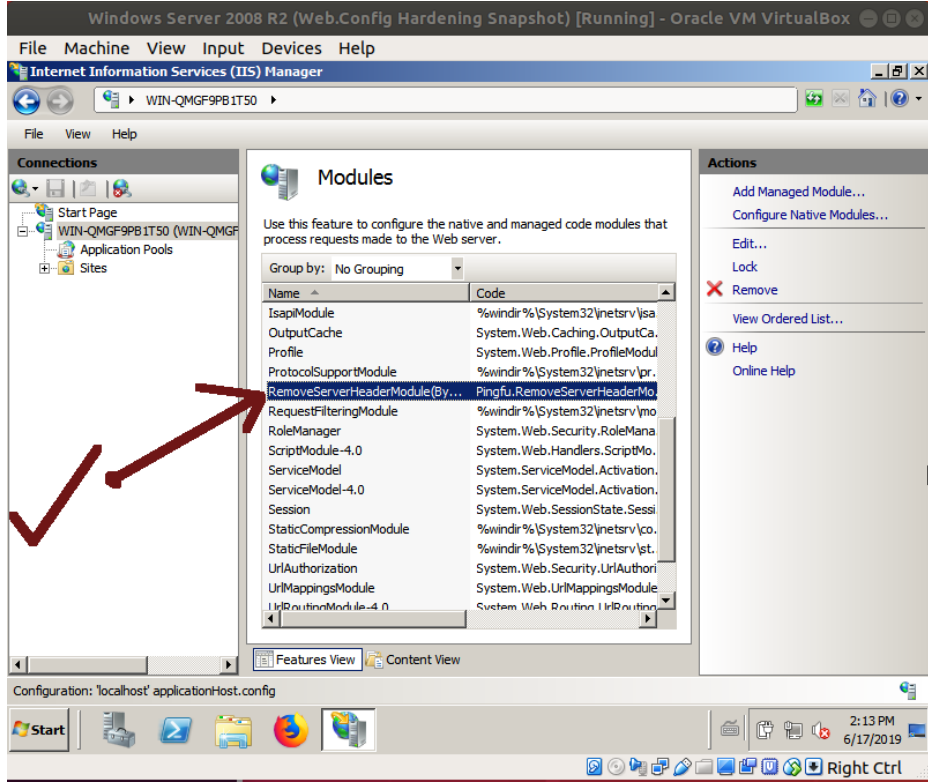
Adım IV: Modül ismi olarak keyfi bir (tanımlayıcı) ifade girilir. Modül türü olarak da Windows Server 2008 R2'ye exe'siyle kurduğumuz modül seçilerek konur.



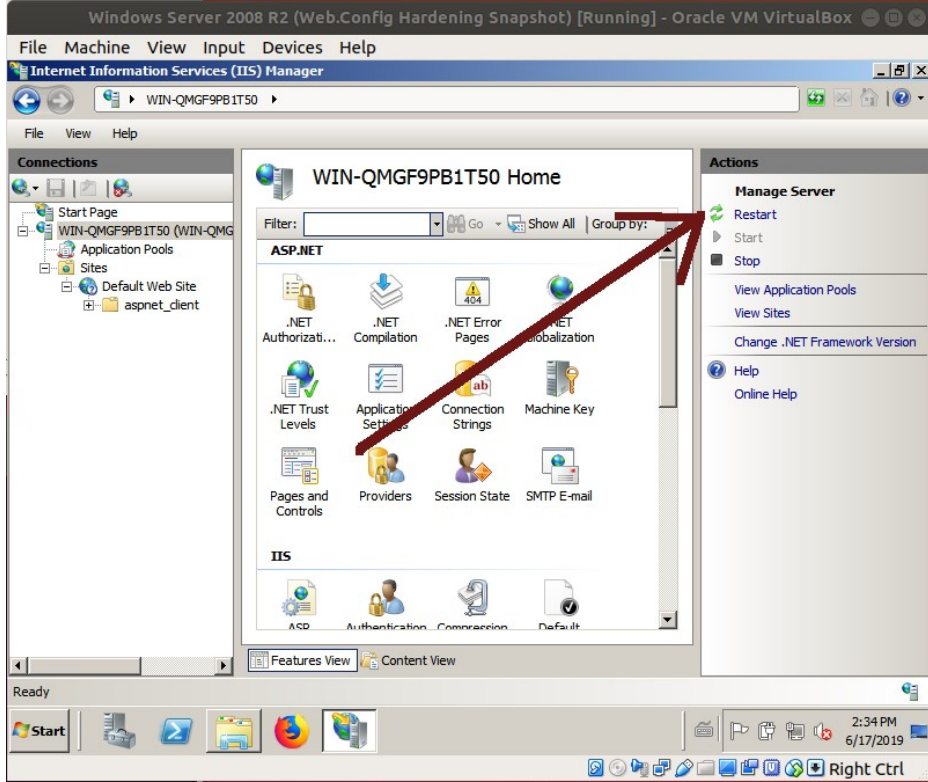
(Keyfi / Tanımlayıcı Modül İsmi Girilir )



( Windows Server 2008 R2'ye exe'siyle yüklenen modül seçilir )



( Windows Server 2008'e Kurulan Modül IIS Manager'dan IIS'e Eklenir )



( IIS sunucu restart'lanır ve eklenen modül böylece etkin hale gelir )

Bu adımlar ile IIS sunucunun döndüğü yanıtlardaki bilgi ifşalarının önüne geçilmiş olacaktır:

## Ubuntu 18.04 LTS Terminal ( MODÜL ÖNCESİ ):

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

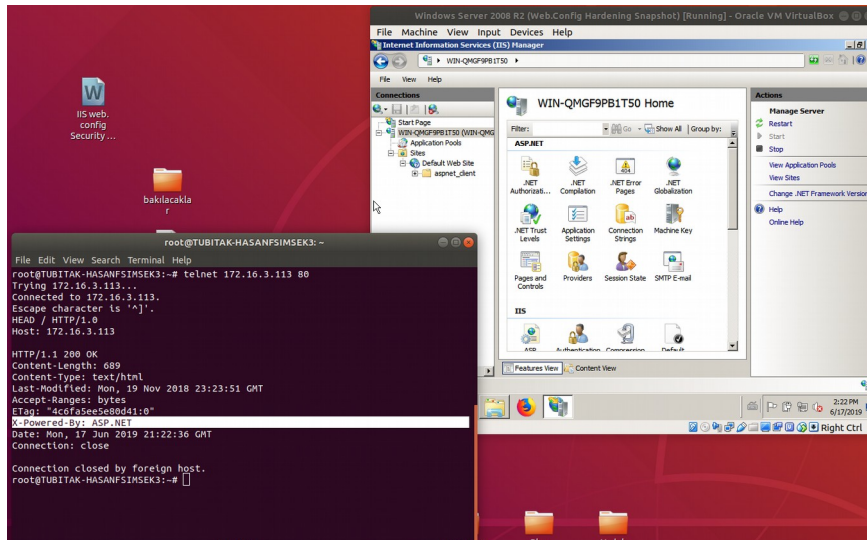
```
Çıktı:
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT
Accept-Ranges: bytes
Etag: "43acgjr0874933dafwq"
Server: IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 17 Jun 2019, 21:22:36 GMT
Connection: close
Connection closed by foreign host.
```

## Ubuntu 18.04 LTS Terminal ( MODÜL SONRASI ):

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

```
Çıktı:
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT
Accept-Ranges: bytes
Etag: "43acgjr0874933dafwq"
X-Powered-By: ASP.NET
Date: Mon, 17 Jun 2019, 21:22:36 GMT
Connection: close
Connection closed by foreign host.
```

// (-) Halen geliyor.



( Bilgi ifşa eden başlıklardan sadece X-Powered-By kalmış )

NOT 1:

Eğer halen X-Powered-By gelirse ufak bir elle müdahale yapmak ve web.config içerisine şunu ilave etmek yeterlidir:

web.config

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Böylece şu başlıkların tamamının dışarıyı çıkışı engellenmiş olacaktır.

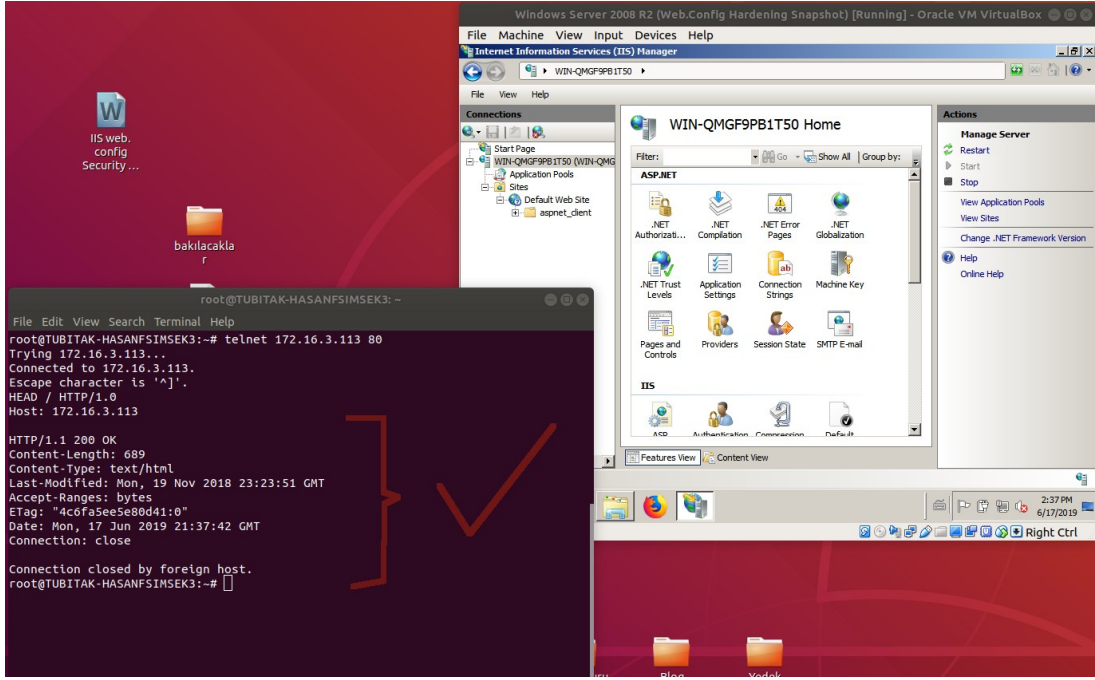
Server  
X-Powered-By  
X-AspNet-Version  
X-AspNetMvc-Version

Ubuntu 18.04 LTS Terminal ( **MODÜL SONRASI ve Web.Config SONRASI** ):

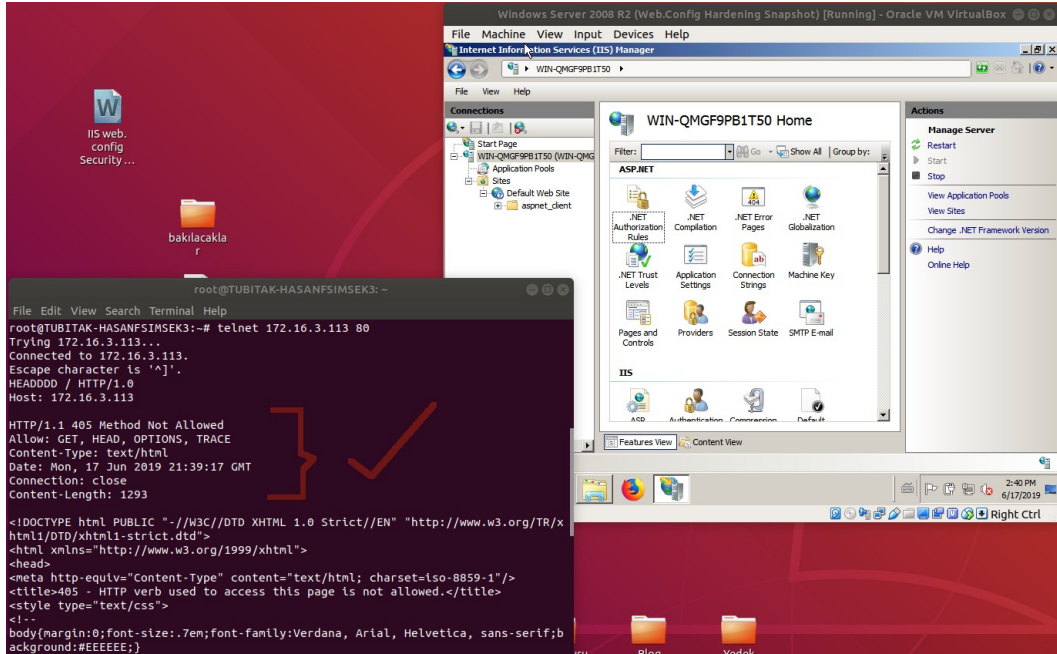
```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

```
Çıktı:
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT
Accept-Ranges: bytes
Etag: "43acgjr0874933dafwq"
Date: Mon, 17 Jun 2019, 21:22:36 GMT
Connection: close
Connection closed by foreign host.
```





( Tüm bilgi ifşa eden başlıklar engellenmiş vaziyette )



( Anormal / Eksik / Hatalı Paket Gönderiminde Dahı Bilgi İfşa Eden Başlıklar Engellenmiş Vaziyette )

NOT 2:

IIS Managed Remove Server Headers Modülünün Uyumluluğu Hk.

IIS Remove Server Headers modülü .NET 2.0 ile çalıştığından .NET 2.0'ı içeren .NET 3.5 feature'unun Windows Server 2012 ve sonrasında IIS'e feature olarak eklenmesi gerekmektedir. Çünkü Windows Server 2012 ve sonrasında hazır kurulu gelen .NET framework versiyonu artık .NET 4.5 sürüm framework'tür. Ayrıca Windows Server 2012 ve

sonrasında IIS Remove Server Headers modülünün ihtiyaç duyduğu ISAPI Filters ve ISAPI Extensions feature'ları Windows Server 2008 ve öncesinde default kuruluken sonrasında kurulu olarak gelmediğinden ilave feature olarak eklenmeleri gerekmektedir.

## Server Manager

### Roles and Features

#### Web Server (IIS)

##### Application Development

.NET 3.5 Extensibility	(*) Gerekli
.NET 4.0 Extensibility	(*) <i>Seçime Bağlı (optional)</i>
ASP	(*) Gerekli
ASP.NET 3.5	(*) Gerekli
ASP.NET 4.5	(*) <i>Seçime Bağlı (optional)</i>
ISAPI Extentions	(*) Gerekli
ISAPI Filters	(*) Gerekli

## [!] Uyarı:

Bu yüklemeler için Windows Server Kurulum DVD'si takılmalıdır ve IIS feature eklemeleri sırasında kurulum kaynak dosyası yolu için DVD'nin takılı olduğu sürücü ve akabinde \sources\sxs\ dizin yolu gösterilmelidir. Ancak bu sayede, kurulum başarıyla tamamlanabilecektir.

Kurulum sonrası IIS Remove Headers modülünü IIS panele ekleme işlemi sorunsuzca gerçekleşip modül, bilgi ifşası sunan sunucu başlıklarının gönderimini engelleyebilecektir.

## Kaynaklar

<https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/>

<https://www.activexperts.com/support/network-monitor/online/ii6metabase/>

<https://scotthelme.co.uk/hardening-your-http-response-headers/>

<https://www.microsoft.com/en-us/download/confirmation.aspx?id=7435>

<https://stackoverflow.com/questions/1178831/remove-server-response-header-iis7>

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/modules/add>

<https://docs.microsoft.com/tr-tr/dotnet/api/system.web.configuration.deploymentsection.retail?view=netframework-4.8>

<https://www.devcurry.com/2010/11/using-deployment-retailtrue-attribute.html>

<https://gist.github.com/marcbarry/47644b4a43fbfb63ef54>

<https://www.youtube.com/watch?v=yRNZ3zWOyNI>