IIS Sunucularda Server Header'ını Farklı Bir Değerle Doldurma

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

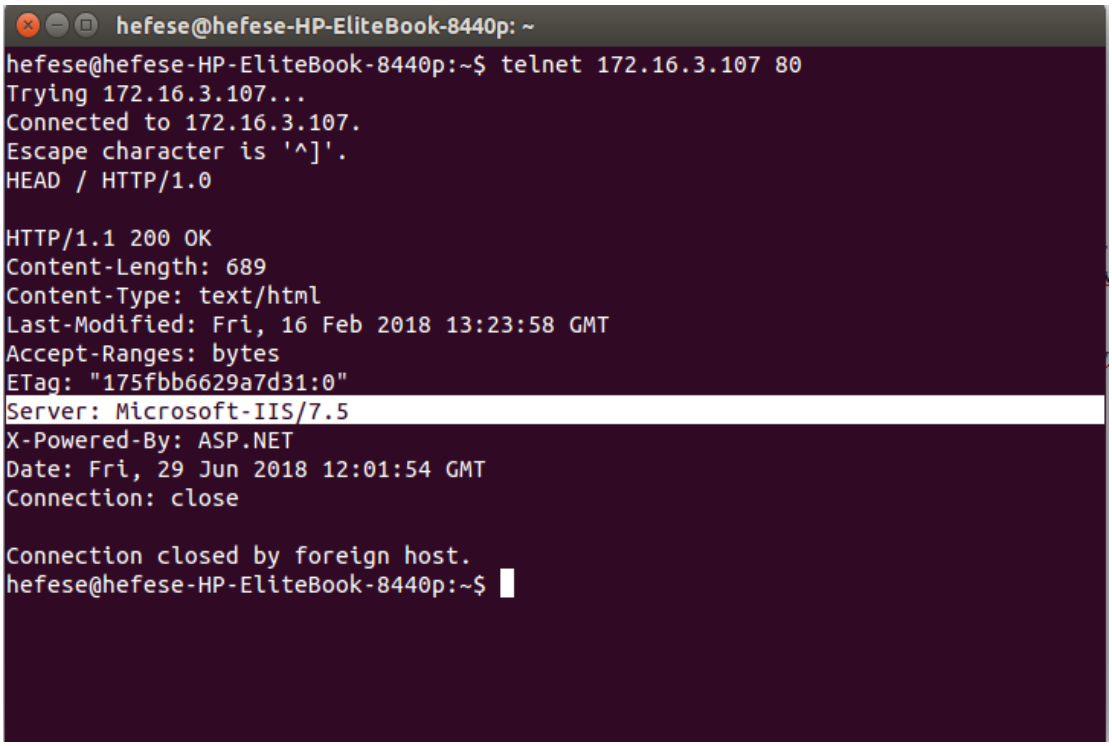
Gereksinimler

Windows Server 2008 R2 Sanal Makinası
URLRewrite

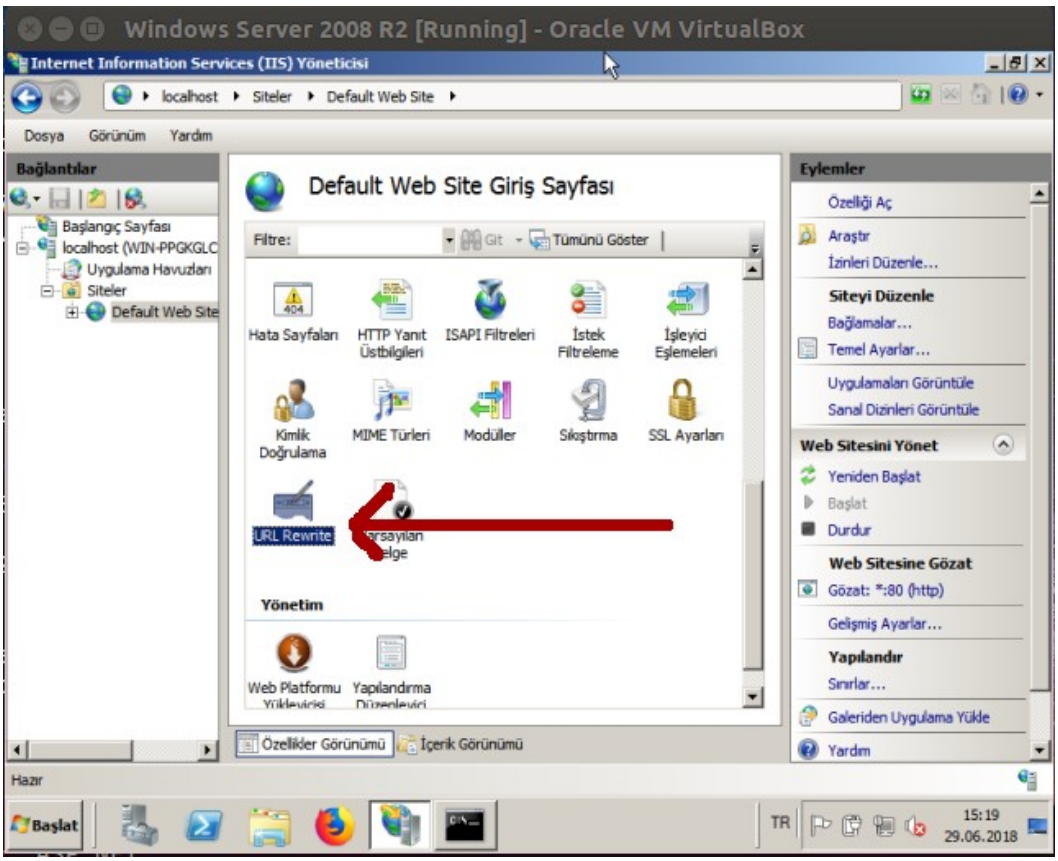
Bu yazıda IIS sunucularda Server header'ını modifiye etme ve bu yolla saldırganlar için hedef şaşırtmanın nasıl yapılabileceği gösterilecektir. Bu işlem için IIS sunuculara UrlRewrite tool'unun yüklenmesi ve sistemin restart'lanması gerekmektedir.

Öncelikle hedef IIS sunucuya bir Http HEAD talebi yapalım ve sunucudan dönen yanıttaki Server başlığına bir bakalım.

> telnet 172.16.3.92 80 // Windows Server 2008 R2 IP'si

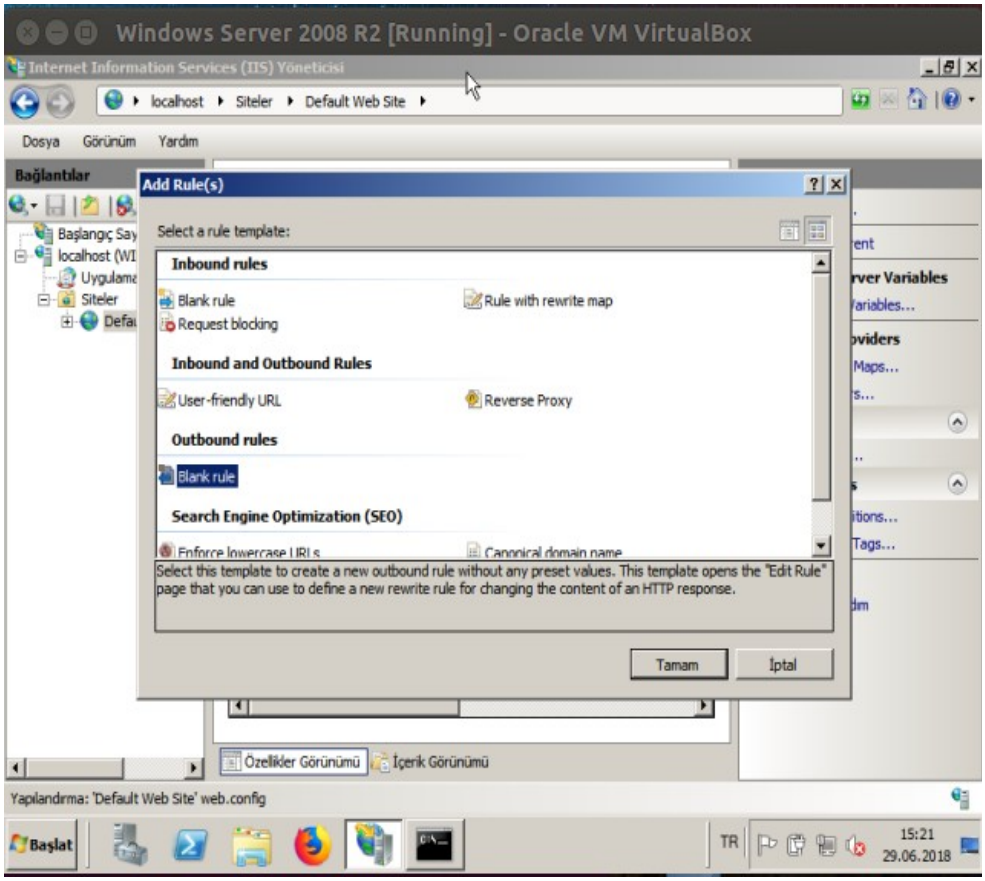


Görüldüğü üzere hedef sistem IIS/7.5 web sunucu yazılımını kullanıyormuş. Bu bilgiyi manipule edelim ve saldırganlar için hedef şaşırtmaca yapalım. Bu işlem için IIS paneli açılır ve URLRewrite öğesine tıklanır.

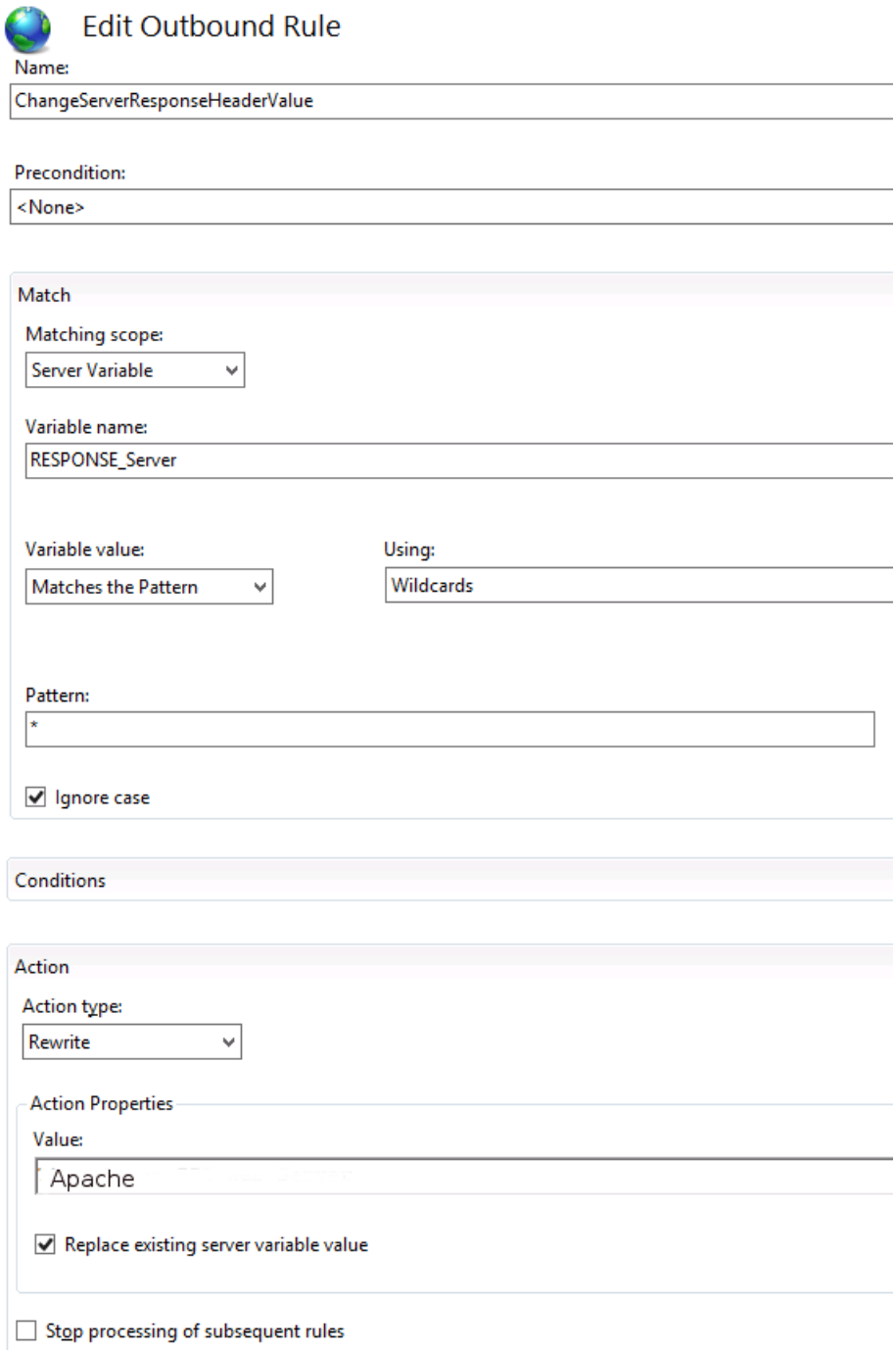


Ardından Add Rules linkine tıklanır.

Daha sonra Outbands Rule -> Blank rule seçeneği seçilir ve Tamam denir.

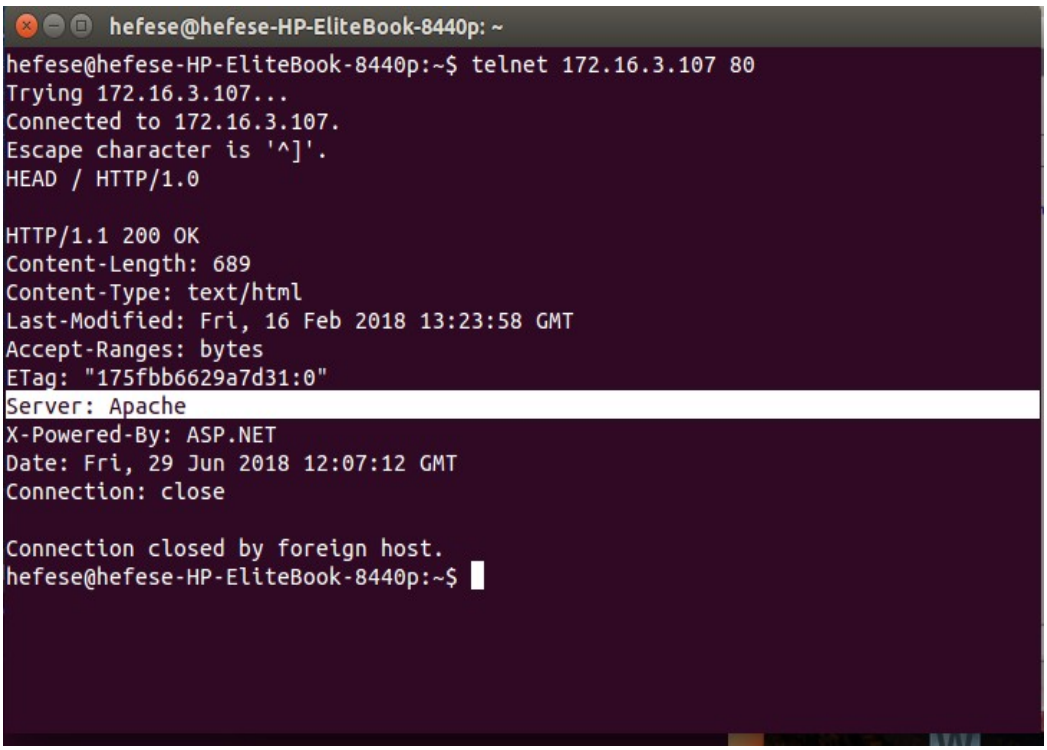


Son olarak gelen sayfaya aşağıdaki değerler girilir.



ve Uygula denir. Böylece Server header'ı belirlediğimiz değeri gösterir duruma gelecektir.

> telnet 172.16.3.92 80



Görüldüğü üzere bir IIS sunucuyu Apache sunucusu gibi gösterdik. Bunun yerine örneğin farklı bir IIS sunucusu bilgisi de girebilirdik veya herhangi alakasız bir string de girebilirdik. Bu tercihe kalan bir şeydir.

Not: URLRewrite tool'u IIS 7 ve sonrasında sorunsuz çalışabilmektedir: IIS 7.0, 7.5, IIS 8, IIS 8.5, IIS 10 (bkz. https://www.iis.net/downloads/microsoft/url-rewrite)

Kaynak

https://blogs.msdn.microsoft.com/benjaminperkins/2012/11/02/change-or-modify-a-response-header-value-using-url-rewrite/

https://www.iis.net/downloads/microsoft/url-rewrite

https://en.wikipedia.org/wiki/Internet_Information_Services