ThinVNC 1.0b1 Directory Traversal Açıklığı ve Sömürme

ThinVNC versiyon 1.0b1 vnc sunucu yazılımının web arayüzünde directory traversal açıklığı duyurulmuştur. Bu açıklığa göre ThinVNC Server web arayüzünde sayfayı isterken gönderilen http paketindeki ilgili sayfayı talep eden dizin yolu yerine üst dizindeki ThinVNC Server konfigurasyon dosyası dizin yolu talep edilmektedir. Bu şekildeki paket gönderimi sonucu ThinVNC Server web arayüzünde dizin gezinme açıklığı var olduğundan dolayı paket gönderimi başarılı olmaktadır ve talep edilen konfigurasyon dosyası içeriği yanıt olarak gelmektedir.

ThinVNC server'a web arayüzünden bağlanırken kimlik doğrulama aşamasında sorduğu geçerli kullanıcı adı ve parola bilgileri açık metin halinde ThinVNC Server konfigurasyon dosyası içeriğinde depolu tutulmaktadır. Dolayısıyla dizin gezinme açıklığı ile konfigurasyon dosyası içeriği yanıt olarak alındığında kimlik doğrulama aşamasında geçerli olan kullanıcı adı ve parola bilgileri de elde edilmiş olmaktadır. Bundan yola çıkarak herhangi yabancı bir kimse web tarayıcıdan ThinVNC web arayüzünde kimlik doğrulama aşamasına geldiğinde dizin gezinme açıklığını kullanarak ThinVNC Server konfigurayon dosyasını okuyabilir, kimlik doğrulama aşamasında istenen geçerli kullanıcı adı ve parola bilgisini elde edebilir ve bu bilgilerle kimlik doğrulama aşamasını geçebilir. Böylece ThinVNC web arayüzündeki kimlik doğrulama aşamasında kullanılan bilgilere sahip olmayan herkes kimlik doğrulama aşamasını atlatabilir, web arayüzünde arka sayfalara / iç sayfalara uzanabilir ve arka sayfalarda / iç sayfalarda masaüstü bağlantısı kurarak hedef vnc sunucu sisteme sızabilir.

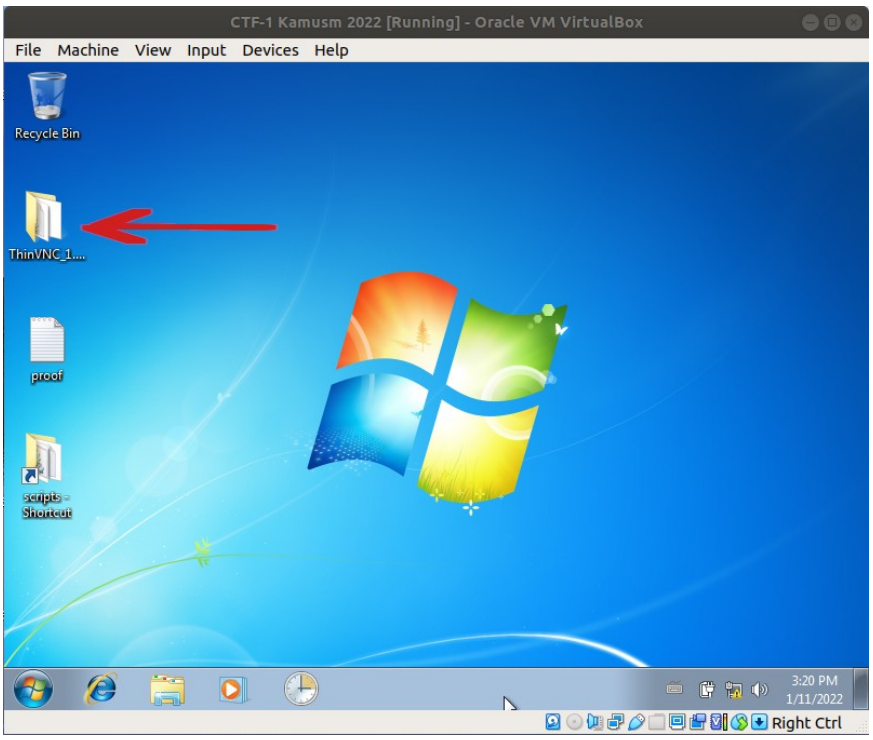
Uygulama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

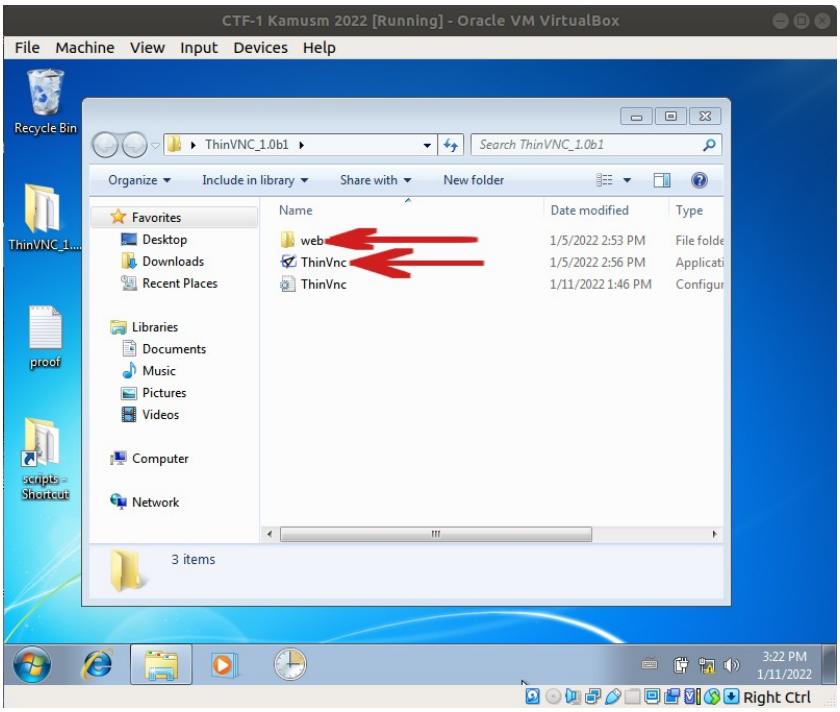
> Gereksinimler
>
> - Firefox Browser - Ubuntu 18.04 LTS Ana Makine // VNC İstemcisi
> - ThinVNC Version 1.0b1 - Windows 7 Home Premium VM // Hedef VNC Web // Sunucusu
>
> (*Not: ThinVNC versiyon 1.0b1 kurulum dosyası ve Windows 7 Home Premium Pro iso'su ~/Downloads/ CTF - 1 - KamuSM 2022 VM Materyaller.zip klasöründe mevcuttur. Hazır ThinVNC Server kurulu Windows 7 Home Premium VM ise CTF-1 KamuSM 2022/ şeklinde mevcuttur.*)

Bu uygulamada thinvnc web arayüzünde var olan directory traversal açıklığı yoluyla thinvnc konfigurasyon dosyasından vnc erişim bilgilerini elde etme ve vnc masaüstü bağlantısı kurarak ThinVNC server kurulu vm makineye sızma gösterilecektir.

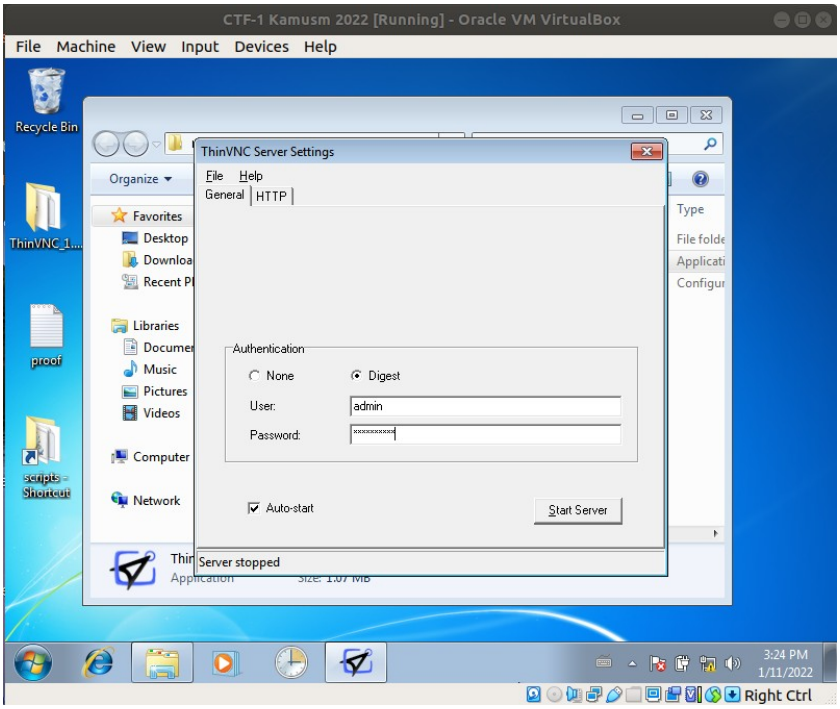
Öncelikle windows 10 pro vm makineye ThinVNC server'ı kuralım. Bunun için zip olarak indirelim ve zip'ten çıkaralım.



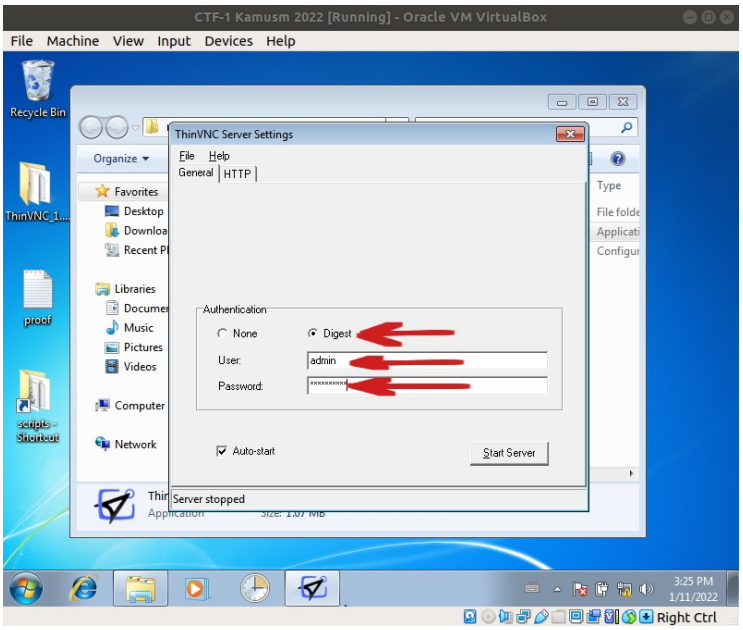
ThinVNC klasöründe bir web/ klasörü vardır ve bir de exe. web/ klasörü vnc sunucusunun web arayüz dosyalarını içerir. Exe dosyası ile de vnc web sunucusu ayağa kaldırılır.



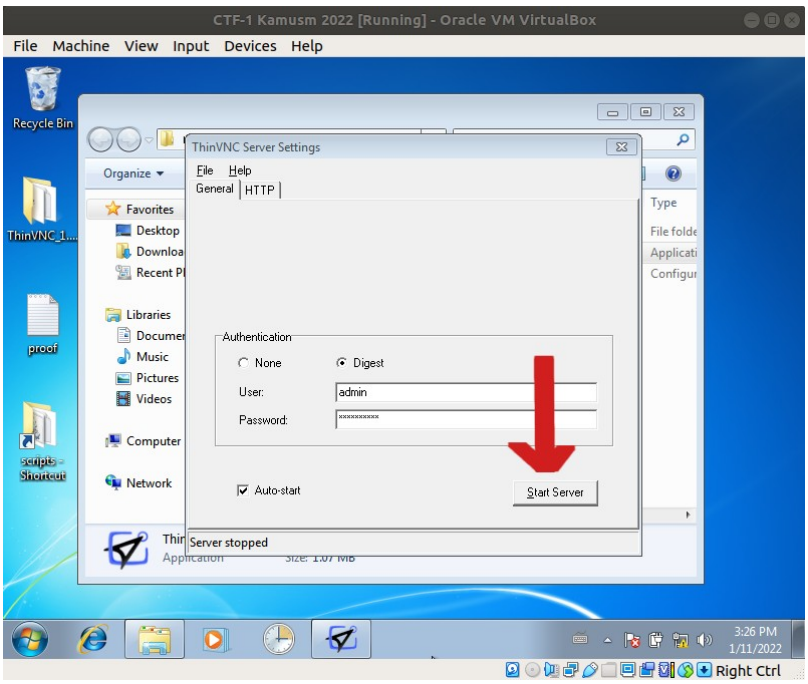
ThinVNC exe dosyası ile vnc yapılandırmasını açalım ve vnc sunucusunu yapılandıralım, ardından vnc web sunucu servisini başlatalım.



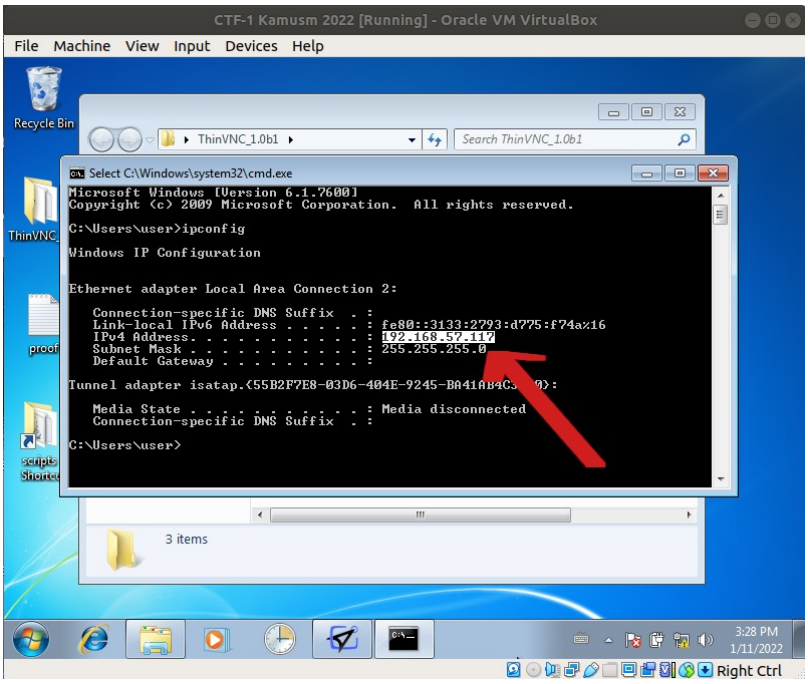
Bu ekranda VNC sunucuya bağlanırken kullanılacak kullanıcı adı ve parola bilgisi ThinVNC Server Digest yetkilendirmesi seçilerek belirlenir.



Belirlenen kullanıcı adı ve parola sonrası ThinVNC server başlatılır.



ThinVNC server başlatıldığında bir http sunucu port 8080'de ayağa kalkar. Artık ThinVNC web sunucunun web arayüzüne web tarayıcıdan erişilebilirdir. Uzaktan bu vnc sunucusunun web arayüzüne erişebilmek için vnc sunucu makinesinin ip'si alınır.



Not:

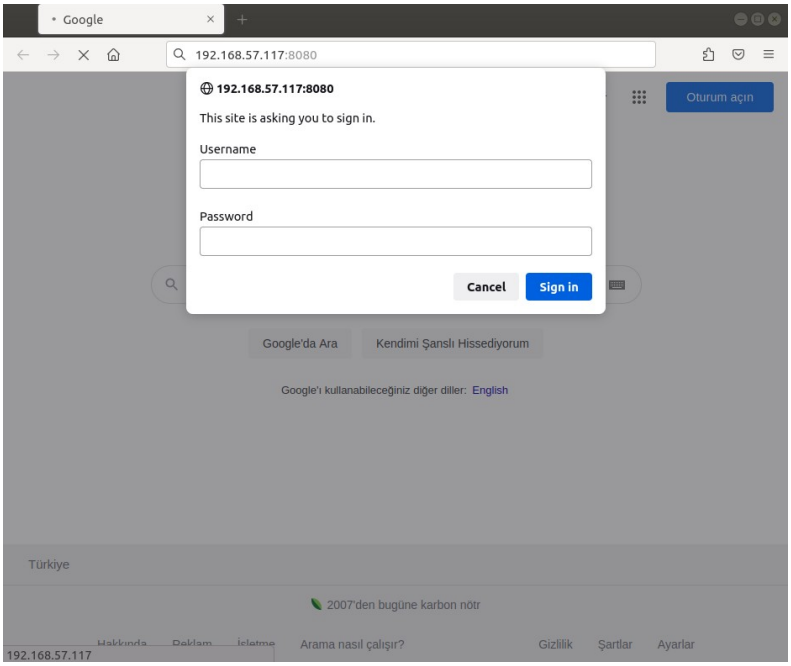
VM içerisinde localhost:8080'den vnc web arayüzüne erişilememekte. Ancak ip:8080 ile vnc sunucuya erişilebilmekte. Dışardan da ip:8080 ile erişimlerde bir sorun olmamakta.

Ardından uzaktan web tarayıcı ile bu vm makinedeki vnc sunucusuna erişilir.

Ubuntu 18.04 LTS Ana Makine:

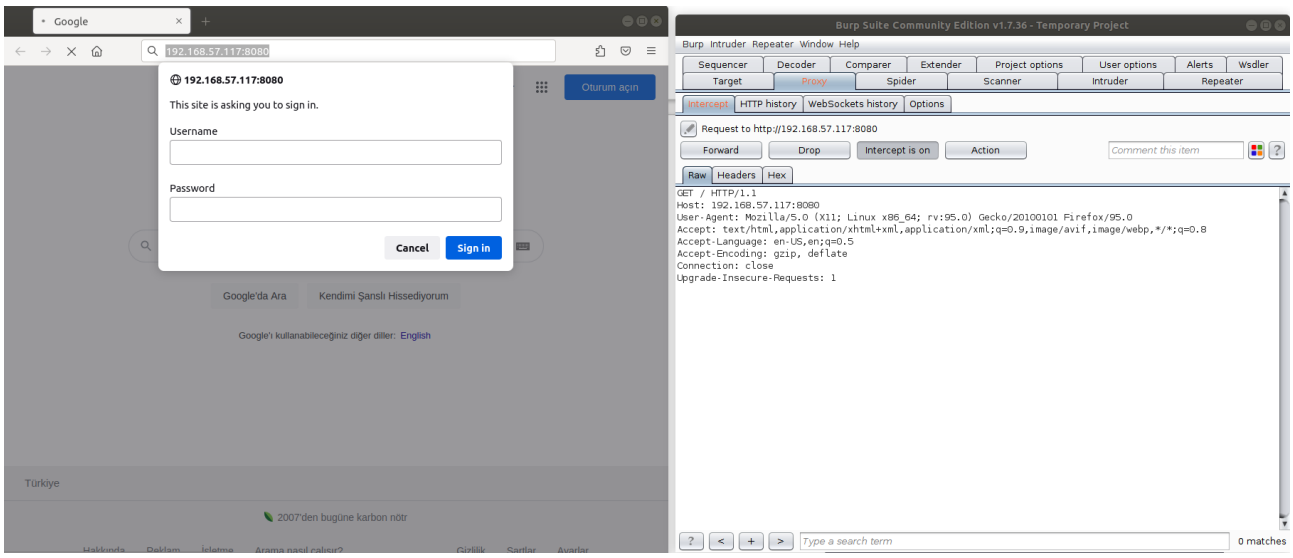
http://192.168.201.173:8080 // http://VMIP:8080

Çıktı:

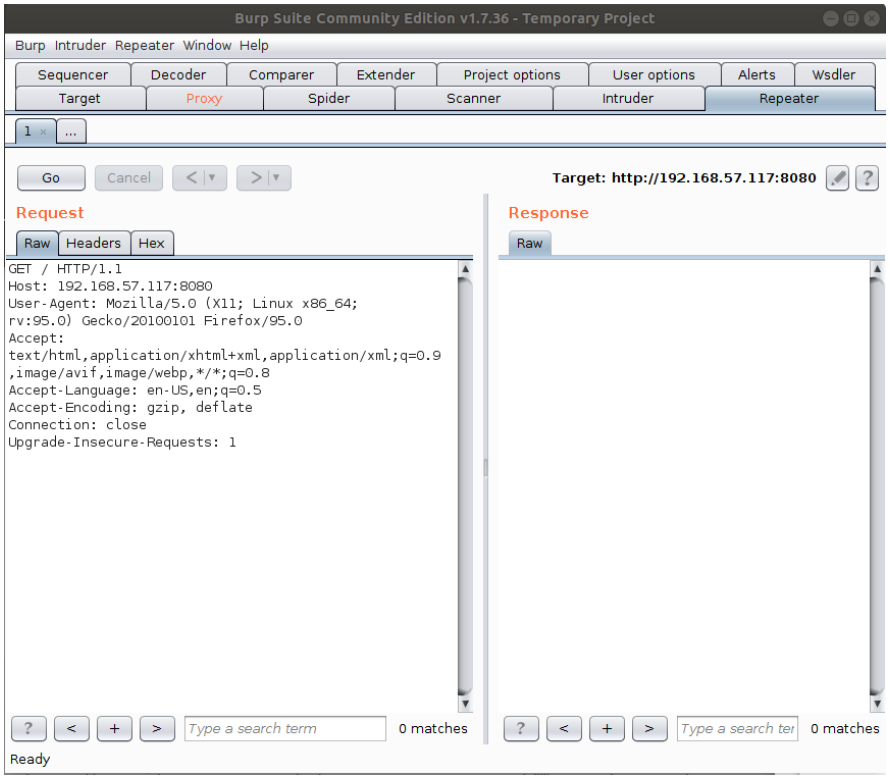


Görüldüğü gibi ana makineden vm makinedeki vnc sunucusu ekranına eriştik. Normal şartlarda yabancı bir kimse bu ekrana geldiğinde kullanıcı adı ve parolayı bilmediğinden vnc sunucu portaline erişemeyecektir. Ancak ThinVNC Server versiyon 1.0b1'lerdeki web arayüzünde var olan Directory Traversal açıklığı nedeniyle ThinVNC Server'ın konfigurasyon dosyası okunabilmekte ve konfigurasyon dosyasında ThinVNC server'ın istediği geçerli kullanıcı adı ve parola bilgileri var olduğundan bu bilgilerle vnc sunucusu portaline erişilebilmektedir.

Şimdi açıklık yoluyla thinvnc konfigurasyon dosyasını okuyabilmek için web tarayıcıda burpsuite ile araya girelim ve thinvnc web sayfasını yeniden talep ederek bir http talebi yakalayalım. Ardından bu http talebini vnc konfigurasyon dosyasını talep edecek şekilde değiştirelim.

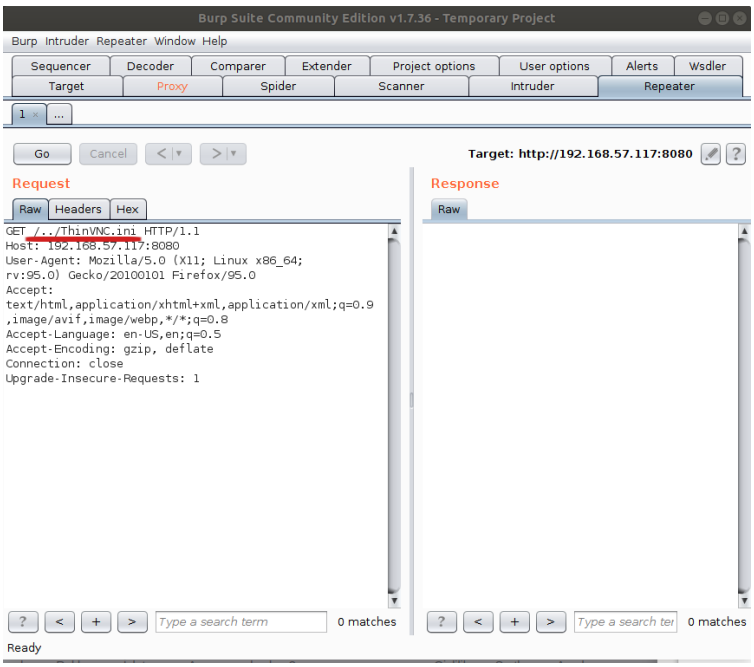


(Sayfa Talep Etme Http Talebi Alınır)

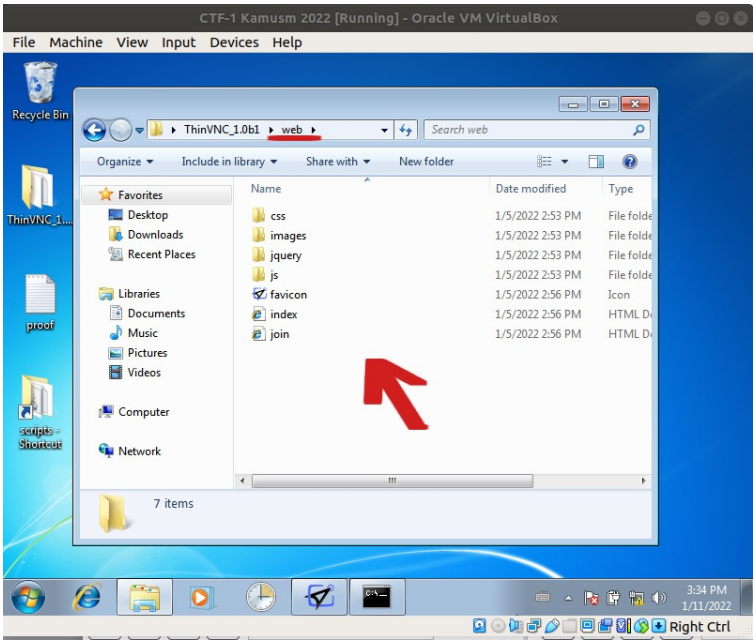


(Sayfa Talep Etme Http Talebi Repeater'a Gönderilir)

Http paketi mevcut bu haldeyken / dizinini, yani kök dizindeki web sayfasını talep etmektedir. Biz bu dizin yolunu ThinVNC server'ın konfigurasyon dosyası şeklinde değiştirelim ve konfigurasyon dosyasını talep edelim.

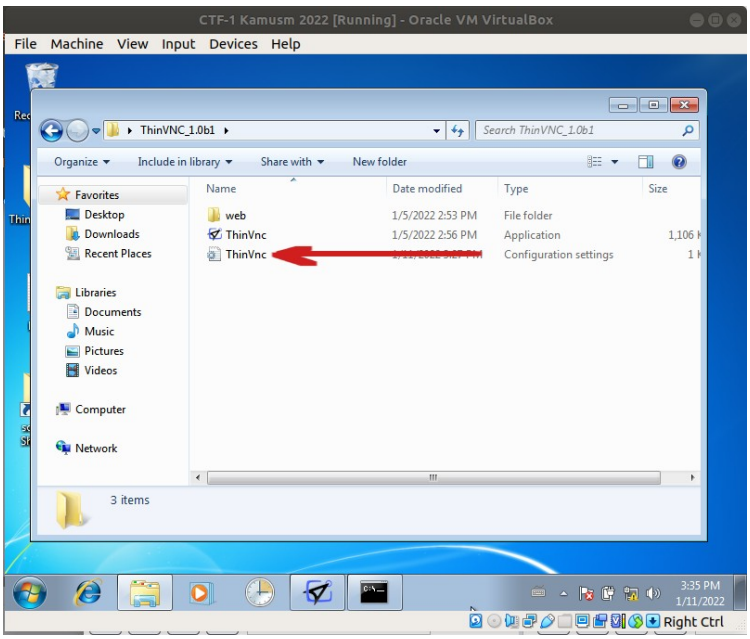


Bu girilen dizin yolunu anlamlandırmak için vm makinedeki VNC kurulum klasörüne bir göz atalım. VNC kurulum klasöründe web uygulama kök dizini web/ klasörü şeklindedir.



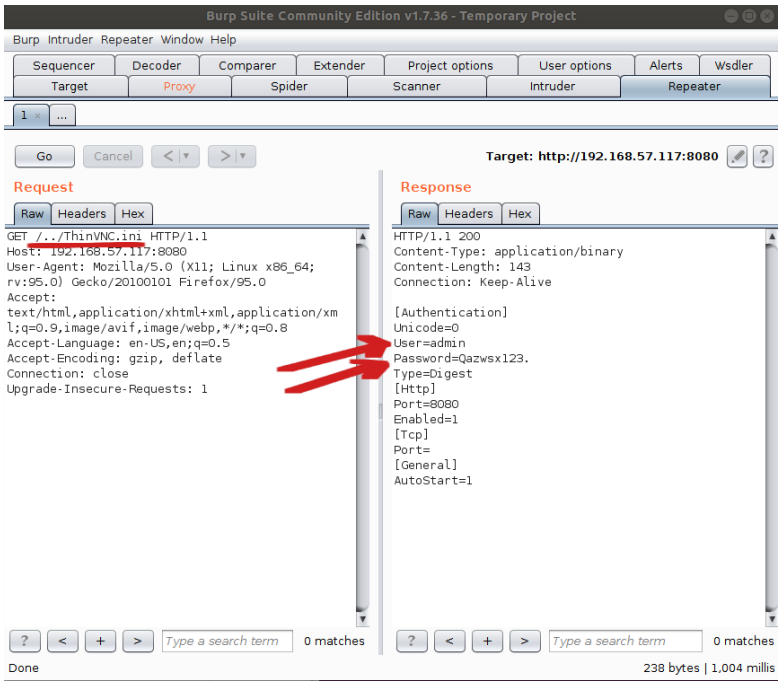
(VNC Web Klasörü)

VNC konfigurasyon dosyası ise web/ klasörünün bir üst dizininde yer alır.

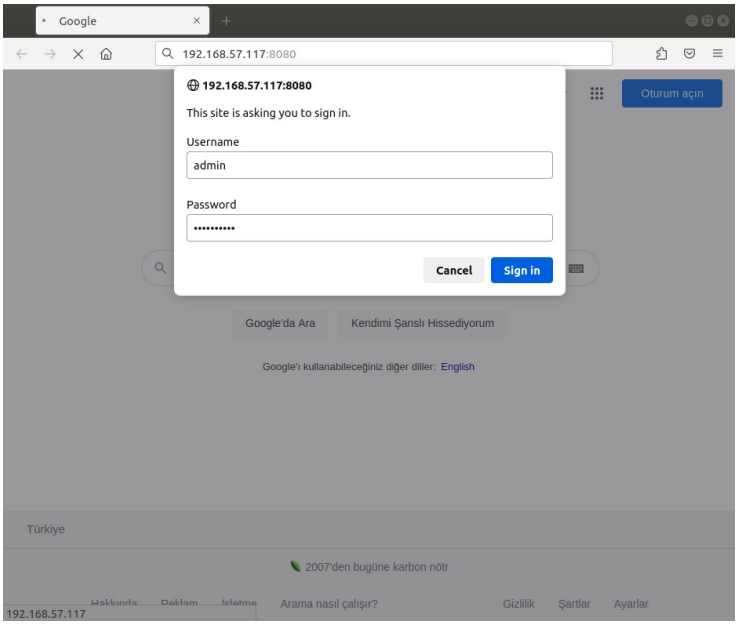


(VNC Konfigurasyon Dosyası)

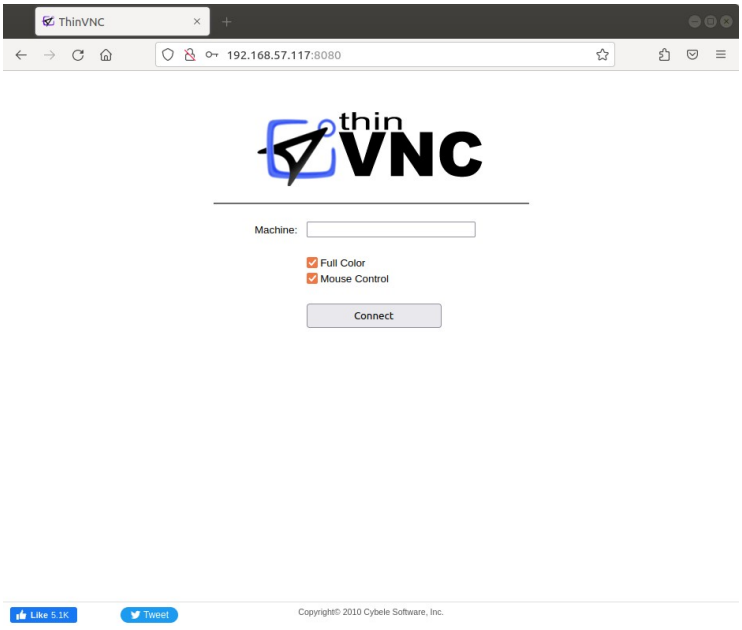
Http paketinde talep edilen dizin yolu ifadesinde / ifadesi VNC kurulum klasöründeki web/ kök dizinin içini ifade eder. ../ ifadesi ile o dizinin bir üzerine (yani web/ kök dizininin yukarısına) çıkılır. Ardından gelinen dizin yolundaki ThinVNC.ini ifadesi ile konfigurasyon dosyası gösterilir ve talep edilir.



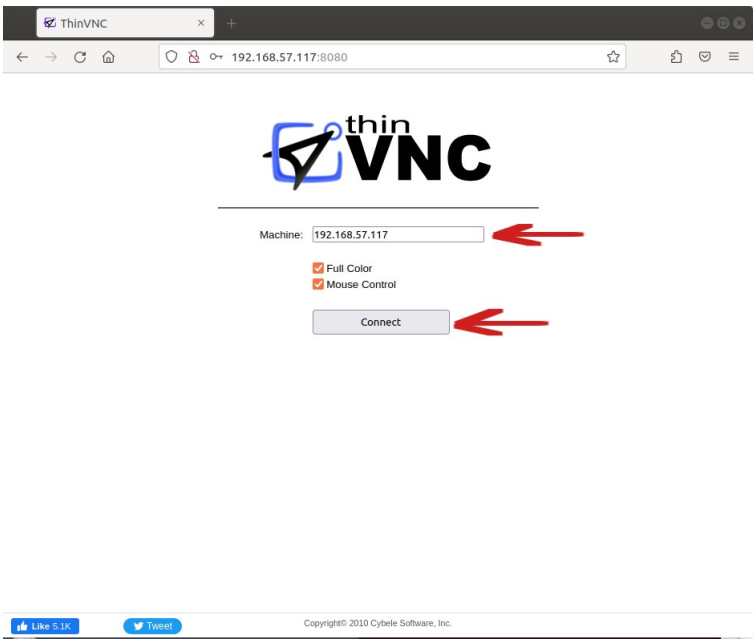
Talep bu şekilde gönderildiğinde konfigurasyon dosyası yanıt olarak gelecektir ve vnc sunucusunun geçerli kullanıcı adı ve parola bilgisi konfigurasyon dosyası okunarak elde edilecektir. Şimdi vnc sunucusuna elde edilen bu bilgilerle erişelim ve vnc sunucusuna masaüstü bağlantısı başlatarak sızalım.



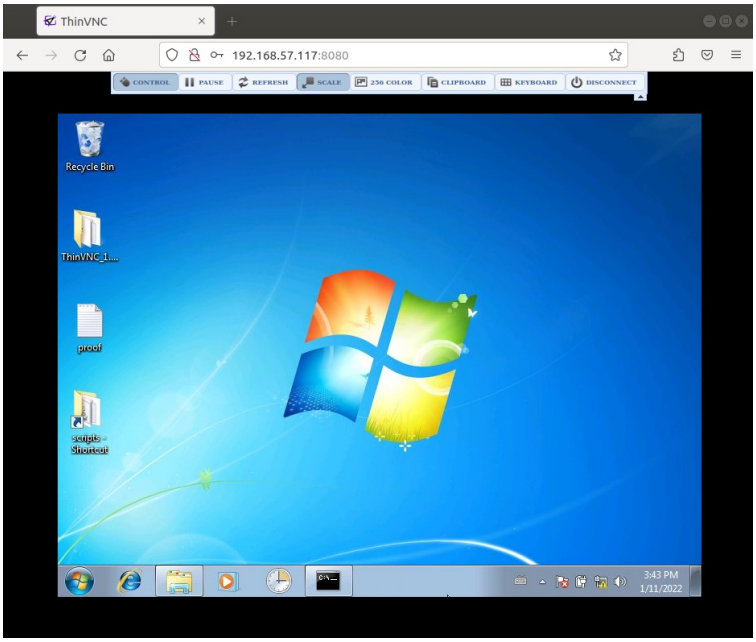
(Elde Edilen Bilgiler Girilir)



(VNC Web Portale Erişilir)



(VNC Web Portale VNC Sunucu IP'si Girilir)



(VNC Masaüstü Bağlantısı Başlar)

Bu şekilde hedef vnc sunucusuna bağlanılır, masaüstü ekrana gelir ve sızma faaliyeti gerçekleşir. Bu uygulamada hedef vnc sunucusunun web uygulamasındaki directory traversal açıklığından faydalanarak vnc sunucusu konfigurasyon dosyası okunmuştur ve geçerli kullanıcı adı ve parola bilgisi elde edilmiştir. Ardından bu bilgilerle vnc sunucusuna web tarayıcıdan bağlanılmıştır ve vnc sunucusuna masaüstü bağlantısı yapılarak sızılmıştır.

Ekstra

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

- Metasploit - Kali Linux 2021.2 VM // VNC İstemcisi
- ThinVNC Version 1.0b1 - Windows 7 Home Premium VM // Hedef VNC Web // Sunucusu

(*Not: ThinVNC versiyon 1.0b1 kurulum dosyası ve Windows 7 Home Premium Pro iso'su ~/ Downloads/ CTF - 1 - KamuSM 2022 VM Materyaller.zip klasöründe mevcuttur. Hazır ThinVNC Server kurulu Windows 7 Home Premium VM ise CTF-1 KamuSM 2022/ şeklinde mevcuttur.*)

Bu uygulamada thinvnc web arayüzünde var olan directory traversal açıklığı yoluyla thinvnc konfigurasyon dosyasından vnc erişim bilgilerini elde etme ve vnc masaüstü bağlantısı kurarak ThinVNC server kurulu vm makineye sızma gösterilecektir. Önceki uygulamaya göre bu uygulamada vnc web arayüzündeki directory traversal açıklığı burpsuite yerine metasploit modülü ile sömürülecektir. Metasploit modülü ile konfigurasyon dosyası, oradan da gerçeli vnc kullanıcı adı ve parolası elde edilerek vnc web arayüzünden masaüstü bağlantısı başlatılacaktır ve sızma faaliyeti gerçekleştirilecektir.

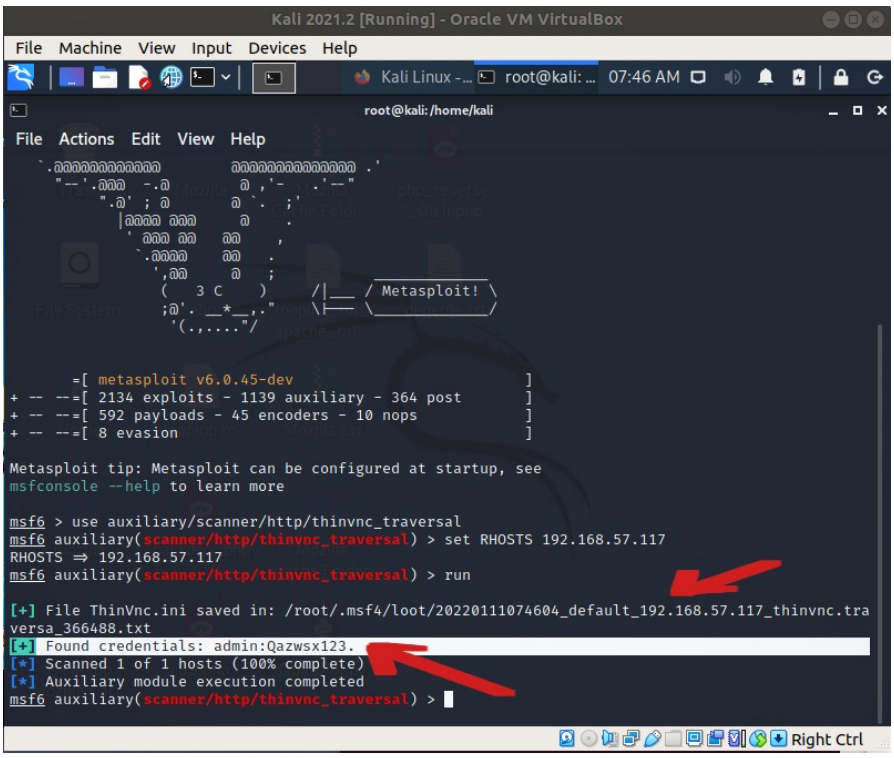
Öncelikle Kali 2021 VM sanal makinesinde metasploit'i başlatalım, ardından ThinVNC'deki directory traversal açıklığını sömüren modülü seçelim, konfigure edelim ve çalıştıralım.

Kali 2021.2 VM:

```
> service postgresql start
> msfconsole
> use auxiliary/scanner/http/thinvnc_traversal
> set RHOSTS 192.168.201.173
> run
```

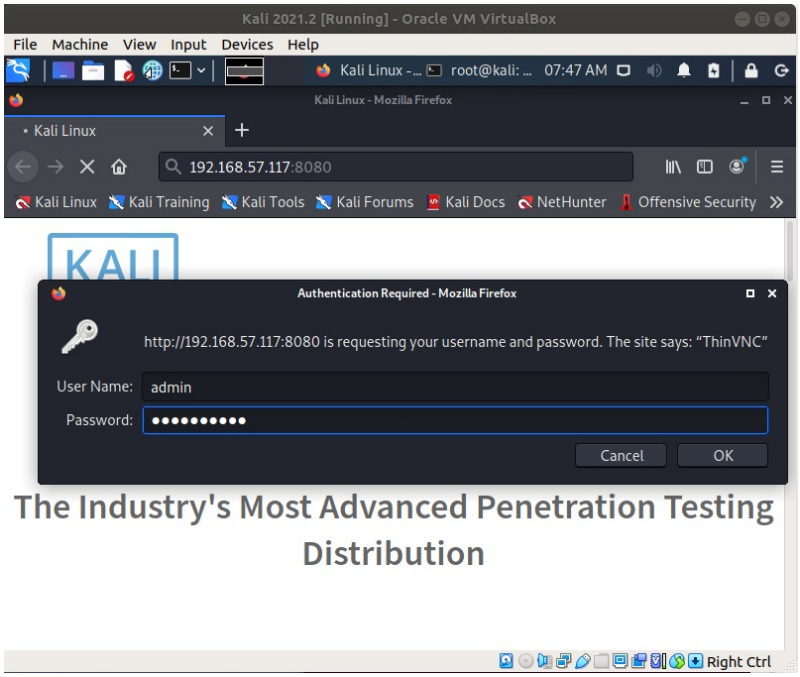
Not: RPORT varsayılan olarak 8080'dir.

Çıktı:

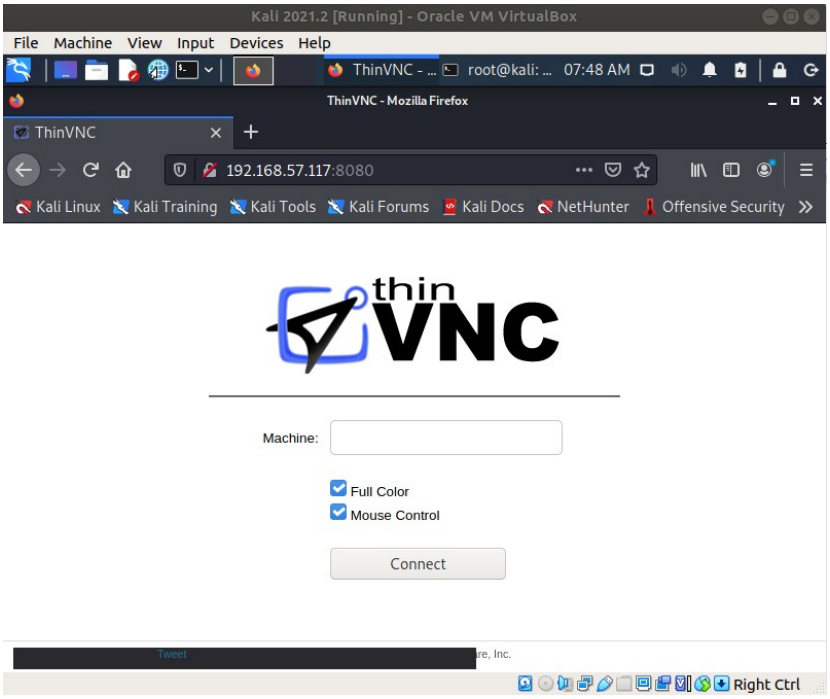


Metasploit modülünün çalışmasıyla vnc sunucudaki ThinVNC.ini konfigurasyon dosyası yanıt olarak tıpkı burpsuite'teki gibi gelecektir. Geçerli kullanıcı adı ve parola bilgisinin yer aldığı konfigurasyon dosyası yanıtı .txt halinde sistem dizini altında kayıt altına alınacaktır. Bu dizin yolu modül çıktısında gösterilmiştir. Ayrıca geçerli kullanıcı adı ve parola bilgisi konfigurasyon dosyası yanıtından cımbızlanarak metasploit modül ekranına çıktı olarak yansıtılacaktır. Bu da ikinci satır olarak modül çıktısında gösterilmiştir.

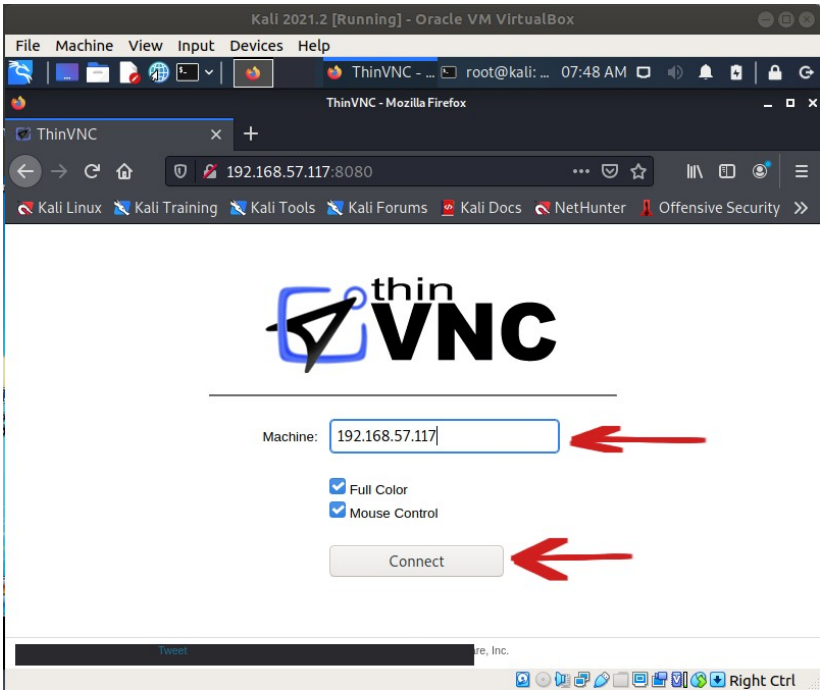
Edinilen geçerli kullanıcı ad ve parola bilgisi sonrası vnc web arayüzünde bilgiler girilerek portale erişilir ve masaüstü bağlantısı yapılarak hedef vnc sunucu makineye sızılır.



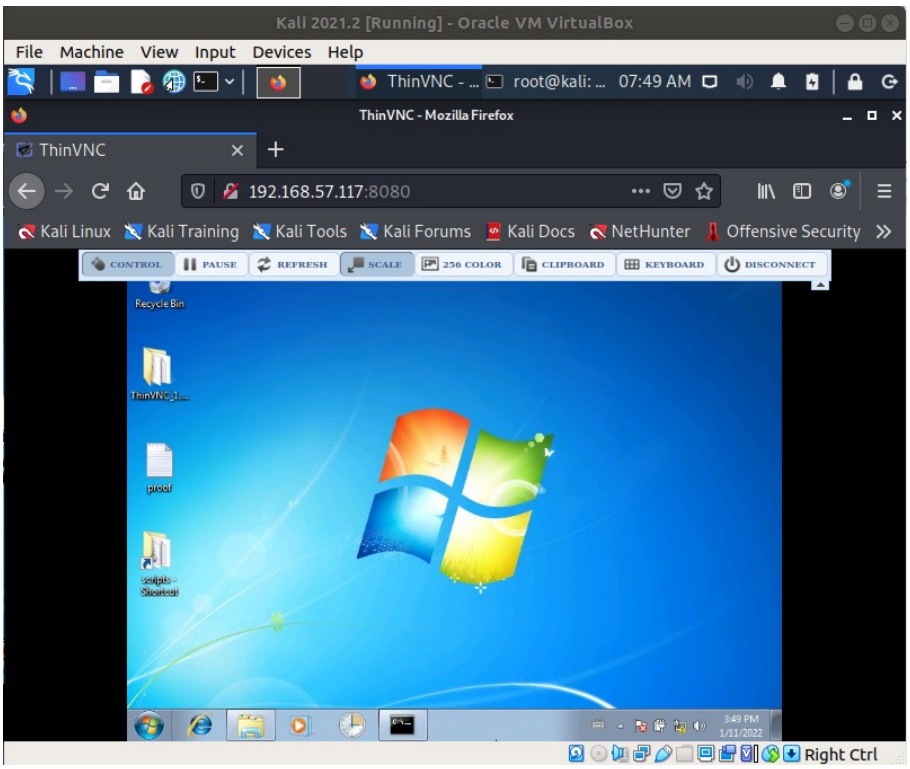
(Elde Edilen Bilgiler Girilir)



(VNC Web Portale Erişilir)



(VNC Web Portale VNC Sunucu IP'si Girilir)



(VNC Masaüstü Bağlantısı Başlar)

Bu şekilde hedef vnc sunucusuna bağlanılır, masaüstü ekrana gelir ve sızma faaliyeti gerçekleşir. Bu uygulamada hedef vnc sunucusunun web arayüzündeki directory traversal açıklığı metasploit modülü ile sömürülerek vnc sunucusu konfigurasyon dosyası alınmıştır ve geçerli kullanıcı adı ve parola bilgisi elde edilmiştir. Ardından bu bilgilerle vnc sunucusuna web tarayıcıdan bağlanılmıştır ve vnc sunucusuna masaüstü bağlantısı başlatılarak sızılmıştır.

Kaynaklar:

https://sourceforge.net/projects/thinvnc/files/ThinVNC_1.0b1/

https://www.webservertalk.com/thinvnc-authentication-bypass-poc/

https://vulmon.com/vulnerabilitydetails?qid=CVE-2019-17662

https://www.rapid7.com/db/modules/auxiliary/scanner/http/thinvnc_traversal/

https://nvd.nist.gov/vuln/detail/CVE-2019-17662