TEHDİT SİMÜLASYONU VE AÇIK KAYNAK KODLU YAZILIMLAR

Yazar: Samet SAZAK
Baskı: 2018

İÇİNDEKİLER

Kırmızı, Mavi, Mor Takım Kavramları Nelerdir?

Kırmızı Takım (Red Team)

Temel olarak, kırmızı takım bir saldırı planlamak ve yürütmek için herhangi bir muhtemel yolu araştırmak için kendi uzmanlık alanlarını kullanır; bu yüzden bakış açılarını potansiyel saldırganların tutumunu benimseyerek oluştururlar. Kırmızı takım çalışmaları; bir kurum ağının, uygulamalarının, çalışanlarının ve fiziksel güvenlik kontrollerinin gerçek hayattaki bir saldırgandan gelebilecek iyi bir saldırıya dayanıp dayanamayacağını ölçmek için tasarlanmış tam kapsamlı, çok katmanlı bir saldırı simülasyonudur.

Mavi Takım (Blue Team)

Mavi takım hem gerçek saldırganlara hem de Kırmızı Takımlara karşı savunma yapan iç güvenlik ekibidir. Güvenliği sağlamak, güvenlik açıklarını belirlemek, her bir güvenlik önleminin etkinliğini doğrulamak ve uygulamadan sonra tüm güvenlik önlemlerinin etkili olmaya devam etmesini sağlamak için bilgi sistemleri analiz çalışmalarını yapmaktadır. Mavi Takımlar çoğu organizasyonda standart güvenlik ekiplerinden ayrılmalıdır; çünkü çoğu güvenlik operasyon ekibi, gerçek bir Mavi Takımın misyonu ve perspektifi olan saldırıya karşı sürekli bir öngörü zihniyetine sahip değildir.

Mor Takım (Purple Team)

Mor takım, Kırmızı Takım ve Mavi Takımın birlikte çalışması, iş birliğidir. Kırmızı Takım ve Mavi Takımın birbirleriyle simbiyotik bir ilişkisi vardır; birlikte çalıştıklarında, her ikisinin de becerileri ve süreçleri geliştirilir. Kırmızı takımlar güvenlik politikalarını atlamayı denerken, Mavi takımlar kırmızı takımın simüle ettiği saldırıları tespit etmeye, engellemeye ve azaltmaya çalışır. Her takım bir kurumun güvenliğini olgunlaştırmak için sınırları zorlamaya çalışır.

Mor Takımlar, her takımdan birer birer metotları bir araya getirmek olarak açıklanabilir. Tek bir birim (ya da mor takım) olarak birlikte çalışan siber güvenlik uzmanlarının saldırı ve savunma ekipleri, uygun iş birliği, iletişim ve genel güvenlik hijyenini sağlamada çok etkili olduklarını kanıtlamıştır. Renk teorisinde olduğu gibi, hem “Kırmızı” hem de “Mavi”nin karışımı Mor takımı oluşturur.

Tehdit Simulasyonu Nedir?

Tehdit Simülasyonu (Adversary Simulation) için henüz standart bir tanım oluşturulmamıştır. Aynı kavram için çeşitli kaynaklarda tehdit emülasyonu, mor takım çalışması ve saldırı simülasyonunu gibi ifadelere de rastlanmaktadır. Tehdit simülasyonun amacı, kurumların karşılaşabilecekleri hedef odaklı saldırılara yönelik olarak ağ savunması hazırlamaktır.

Temel olarak Tehdit Simülasyonu aşağıdaki sorulara cevap olmaktadır.

- Ağınızda hedefe yönelik bir saldırı nasıl ortaya çıkıyor?
- Hedefli bir saldırgan ağınıza erişim ile ne yapabilir?
- Mevcut güvenlik durumunuz, hedefli odaklı bir saldırıyı önleme, tespit etme ve bunlara yanıt verme konusunda ne kadar etkilidir?

Genellikle kuruluşlar zamanlarını, kaynaklarını ve bütçelerini kurum ağlarını sıkılaştırma ve dışarıdan gelen saldırılara karşı hızlı bir şekilde cevap verebilmek üzerine odaklamaktadır. Ancak mevcut saldırıların çoğu, basit bir e-posta yoluyla pahalı güvenlik duvarlarını ve çevre korumalarını atlatmaktadır. Dahili ağa erişim elde edildiğinde, yetki yükseltme ve hatta domain yöneticisi gibi yetkileri elde etmek en kolay iş olabilmektedir. Güvenliği dahili olarak geliştirmek ve dahili ağınızdaki riskleri azaltmak için bir sızma testi, güvenlik ekibinizin saldırı imzaları ve taktikleri konusunda eğitmek için gerçek zamanlı olarak iç saldırıları "simüle etmeye" odaklanmaktadır. **İğnenin neye benzediğini bilmek, samanlıkta onu bulmanın ilk adımıdır.**

ATT&CK Nedir?

ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Framework, yaklaşık olarak beş yıldan beridir MITRE tarafından geliştirilmektedir.

MITRE'nin ATT&CK framework'ü, saldırganların yaşam döngüsünün çeşitli aşamalarını ve hedefledikleri platformları yansıtan ve davranışları için küratörlü bir bilgi tabanı ve modelidir. ATT&CK, kuruluşların siber tehditleri hızlıcaa tespit etmesine, saldırgan davranışlarını tanımlamasına ve kategorize etmesine yardımcı olmaktadır.

Tehdit Simülasyonu İçin Kullanılan Açık Kaynak Yazılımlar

MITRE Caldera

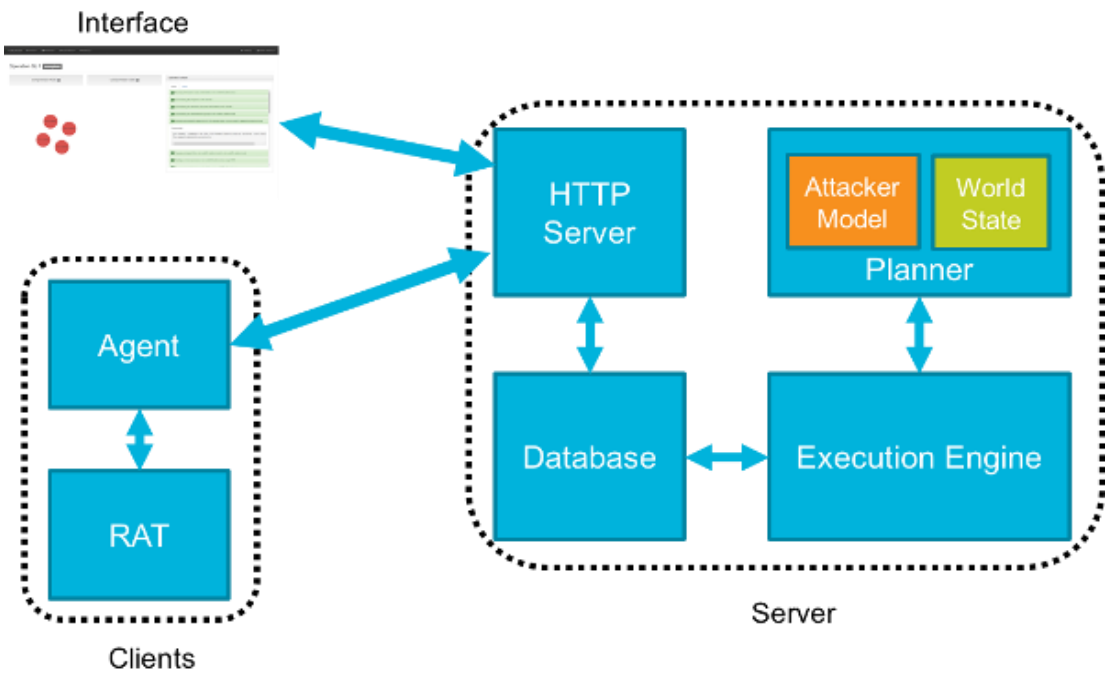
Caldera, volkanik patlama sonucu toprağın çökmesiyle oluşmuş volkanik yer şeklidir. Bazen volkanik kraterlerle karıştırılmaktadır. Kelime, İspanyolcada ‘caldera’ ve Latincede ‘calderia’ denilen ‘pişirilmiş çömlek' anlamına gelmektedir.

Caldera, Windows Enterprise ürünleri kullanan ağların içerisinde bir saldırgan gibi davranışlar sergileyen otomatik tehdit simülasyon sistemidir. Temeli bir ATT&CK ™ projesine dayanan Caldera; bir saldırganın teknik, taktik ve saldırı modellerini kullanarak operasyon sırasında planlar üretir. Bu özellikler, Caldera'nın değişken davranışları kullanarak bir dizi sistem üzerinde çalışmasına izin verir. Bu da saldırganların işlemleri nasıl gerçekleştirdiğini daha önceden "tanımlanmış bir dizi olayları takip eden sistemlerden" daha iyi temsil eder.

Caldera, bir saldırganın tipik olarak ağlarında nasıl davranacağını gösteren ve gerçek veriler üretmek isteyen mavi takım üyeleri için kullanışlı olmaktadır.

Caldera, bir ağ hakkındaki bütün verileri çalışma sırasında toplar. Bu verileri kendi teknikleriyle kullanarak hedefe ulaşmak için kullanmaktadır. Mavi takım için ağ güvenliğinin bir saldırganın başarılı olmasına nasıl "izin verdiğine" dair fikir edinebilmelerini sağlamaktadır. Caldera, yeni veri kaynaklarını tanımlamak, davranışa dayalı saldırı tespit analitiklerini oluşturmak ve iyileştirmek, savunma ve güvenlik yapılandırmalarını test etmek ve eğitim deneyimi yaratmak için kullanışlıdır.

Mimari



Caldera aşağıdaki ekipmanlardan oluşmaktadır.

Server:

- Planlayıcı (Planner): Caldera'nın eylemleri seçmesini sağlayan ana engine(motor)
- Saldırgan Modeli (Attacker Model): ATT & CK dayalı mevcut eylemler
- Dünya Modeli (World Model): Çevrenin Modeli
- Execution Engine (Çalıştırma Motoru): Tekniklerin uygulanması ve veritabanının güncellenmesini sağlar.
- Veritabanı (Database): Çevreyi öğrendikçe verileri buraya kaydeder.
- HTTP Sunucusu

Uç noktalar (Client):

- Agent (Ajan): İletişim için kullanılan uç nokta sistemlerinde istemci
- RAT: Operasyon sırasında saldırgan davranışlarını taklit etmek için kullanılan uzaktan erişim aracı

Caldera'nın planlama sistemi, çevreyle ilgili edindiği mevcut bilgiye ve belirli bir zamanda yapılan eylemlerden elde ettiği bilgiye dayanarak yapılacak en iyi eylemin "karar vermesini" sağlamaktadır. Caldera'nın saldırgan modeli, önceden yapılandırılmış ATT&CK tabanlı tekniklerle temsil edilir.

Proje Sayfası: https://github.com/mitre/caldera

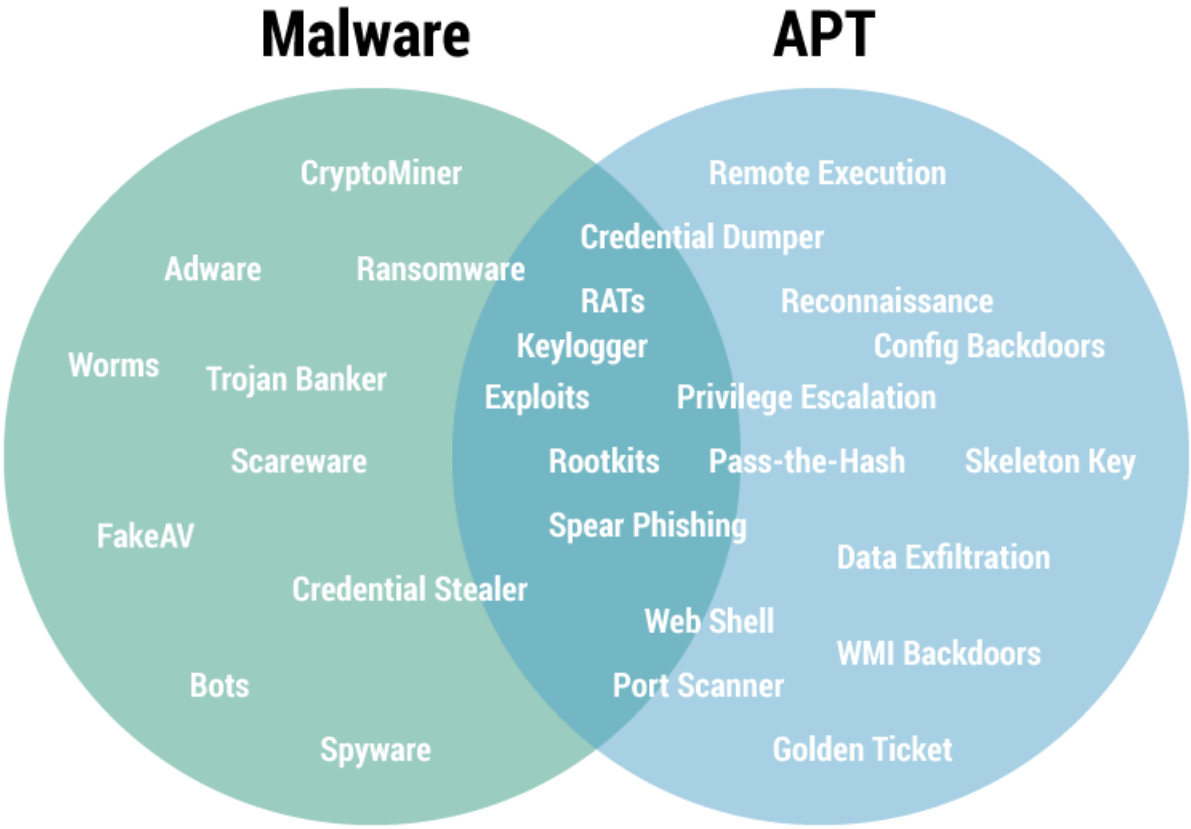
APTSimulator

APT Simulator, bir sistemini "ele geçirmiş gibi görünmesini sağlamak" için bir dizi araç ve çıktı (output) dosyası kullanan bir Windows Batch betiğidir.

APTSimulator'u oluşturan "NextronSystems" durumu şöyle anlatıyor:

"Müşteriler bir POC sırasında tarayıcılarımızın (scanner) test sistemlerine yükledikleri programları rapor etmedikleri konusunda bir şikâyette bulundular. Bir Nmap kurmuşlar, İndirilenler klasörüne bir "PsExec.exe" indirmişler ve kullanıcının Masaüstü'nde "EICAR" test virüsüne yerleştirmişlerdi. Gerçek bir tehdidi daha uygun bir şekilde simüle eden bir araç oluşturmaya karar verdiğimiz an buydu."

Bu aracın odağı zararlı yazılım oluşturmak değil, bir saldırganın oluşturduğu aktiviteyi simüle etmektir.



Kullanım Senaryoları:

- POC'ler: Endpointlerin ve tespit ve monitoring araçlarının algılama yeteneklerini test etmenizi sağlar.
- EICAR veya port taraması olmayan bir tehdit üzerinde SOC müdahalesini test etmenizi sağlar.
- Adli bilişim sınıfı için bir çevre hazırlamanıza yardımcı olur.

Tespit

Aşağıdaki tabloda farklı test durumları ve beklenen algılama sonuçları gösterilmektedir.

- AV = Antivirus
- NIDS = Network Intrusion Detection System
- EDR = Endpoint Detection and Response
- SM = Security Monitoring
- CA = Compromise Assessment

Test Case	AV	NIDS	EDR	SM	CA
Collect Local Files					X
C2 Connects	(X)	X	X	X	
DNS Cache 1 (Cache Injection)	(X)	X		X	X
Malicious User Agents (Malware, RATs)		X	X	X	
Ncat Back Connect (Drop & Exec)	X		X	X	X
WMI Backdoor C2			X	X	X
LSASS Dump (with Procdump)			X	X	X
Mimikatz 1 (Drop & Exec)	X		X	X	X
WCE 1 (Eventlog entries)			X	X	X
Active Guest Account Admin			X	X	X
Fake System File (Drop & Exec)			X	X	X
Hosts File (AV/Win Update blocks)	(X)		X		X
Obfuscated JS Dropper	(X)	X	X	X	X
Obfuscation (RAR with JPG ext)					(X)
Nbtscan Discovery (Scan & Output)		X	X	(X)	X
Recon Activity (Typical Commands)			X	X	X
PsExec (Drop & Exec)			X	X	X
Remote Execution Tool (Drop)	(X)				X

At Job			X	X	X
RUN Key Entry Creation			X	X	X
Scheduled Task Creation			X	X	X
StickyKey Backdoor			X		X
UserInitMprLogonScript Persistence			(X)	X	X
Web Shells	X		(X)		X
WMI Backdoor			X		X

Github: https://github.com/NextronSystems/APTSimulator

Atomic Red Team

"Güvenlik çözümlerinin ayarlandığını ve gerçek rakiplerle yüzleşmeye hazır olduğunu nereden biliyorsunuz? Tespitlerinizi güvence altına almak için yeni veya mevcut ürünleri test ediyor musunuz? Birçok takım gibi belirli bir rakip taktiği veya tekniği simüle etmek için dahili kaynak veya uzmanlıktan yoksun olabilirsiniz. Bu yüzden kısa bir süre önce açık kaynak kodlu bir test framework'ü olan Atomic Red Team'i oluşturduk ve bu sayede tespitlerinizi test edebilecek yetenekler sunuyoruz." - (https://redcanary.com/blog/atomic-red-team-testing/)

Atomic Red Team, Mitre ATT&CK Framework'e uygun olarak geliştirilmiş saldırı testleri yapmanıza olanak sağlayan, açık kaynak geliştirilen bir yazılımdır.

Her bir test, belirli bir taktiği uygulamak için tasarlanmıştır. Atomic Red Team bu sayede mavi takım üyelerinin savunmalarını, geniş bir yelpazeye yayılan saldırılara karşı derhal test etmeye başlaması için oldukça uygun bir ortam sağlamaktadır.

Tavsiye edilen başlangıç kuralları:

- Test yapmadan önce izin ve gerekli onay aldığınızdan emin olun. Yetkisiz testler kötü bir karardır.
- Ortamınızdaki yapıya benzeyen bir test makinesi kurun. "Collection/EDR" çözümünüzün yerinde olduğundan ve uç noktanın (endpoint) etkin olduğundan emin olun.
- Bir test planı veya senaryo geliştirmek için biraz zaman harcayın.

Atomic Red Team'in nasıl kullanılacağına dair hazırlanmış olan videoyu izlemek için: https://www.youtube.com/watch?v=iNl_rltYmoo

Proje: https://redcanary.com/atomic-red-team/
Github : https://github.com/redcanaryco/atomic-red-team

Network Flight Simulator

FlightSim, zararlı ağ trafiği oluşturmak ve mavi takım için network güvenlik kontrollerini ve ağ görünürlüğünü değerlendirmelerine yardımcı olmak için kullanılan hafif bir yardımcı yazılımdır.

Araç, DNS tünelleme, DGA (Domain Generating Algorithm) trafiği, bilinen etkin C2 (komuta&kontrol) hedeflerine gönderilen istekler gibi şüpheli trafik oluşturur ve simüle etmek için testler gerçekleştirir.

FlightSim, Go programlama dili ile yazılmıştır. Dolayısıyla sisteminizde Go kurulu ise aşağıdaki komutu çalıştırarak sisteminize FlightSim kurabilirsiniz.

```
$ go get -u github.com/alphasoc/flightsim/...
```

Daha sonra, örneğin DGA trafiği oluşturmak istiyorsanız:

```
$ flightsim run dga

AlphaSOC Network Flight Simulator™ (https://github.com/alphasoc/flightsim)
The IP address of the network interface is 172.31.84.103
The current time is 10-Jan-18 09:30:28

Time      Module   Description
------------------------------------------------------------------------------
09:30:28  dga      Starting
09:30:28  dga      Generating list of DGA domains
09:30:30  dga      Resolving rdumomx.xyz
09:30:31  dga      Resolving rdumomx.biz
09:30:31  dga      Resolving rdumomx.top
09:30:32  dga      Resolving qtovmrn.xyz
09:30:32  dga      Resolving qtovmrn.biz
09:30:33  dga      Resolving qtovmrn.top
09:30:33  dga      Resolving pbuzkkk.xyz
09:30:34  dga      Resolving pbuzkkk.biz
09:30:34  dga      Resolving pbuzkkk.top
09:30:35  dga      Resolving wfoheoz.xyz
09:30:35  dga      Resolving wfoheoz.biz
09:30:36  dga      Resolving wfoheoz.top
09:30:36  dga      Resolving lhecftf.xyz
09:30:37  dga      Resolving lhecftf.biz
09:30:37  dga      Resolving lhecftf.top
09:30:38  dga      Finished

All done! Check your SIEM for alerts using the timestamps and details above.
```

Github sayfası: https://github.com/alphasoc/flightsim

Metta

Metta bir hazırlık aracıdır. Redis / Celery, Python ve Vagrant kullanarak simülasyonlar oluşturur. Bu, ana (host) makine tabanlı cihazlarınızı test etmenize olanak sağlar; ancak aynı zamanda vagrant'ı nasıl kurduğunuza bağlı olarak ağ tabanlı tespit ve kontrolleri test etmenize de yardımcı olabilmektedir.

Proje yaml dosyalarını parse eder ve bu eylemleri sıraya koymak için Celery kullanır. Sonrasında da tek tek çalıştırır.

Örnek senaryo:

scenario_example.yml 498 Bytes

```yaml
enabled: true
meta:
  author: cg
  created: 2017-10-10
  decorations:
  - Purple Team
  description: Scenario Examples
  link: http://carnal0wnage.attackresearch.com
  mitre_attack_phase: null
  mitre_attack_technique: null
  mitre_link: null
  scenario: True
  scenario_actions:
    1: MITRE/Discovery/discovery_account.yaml
    2: MITRE/Credential_Access/credaccess_win_creddump.yml
    3: MITRE/Execution/execution_regsvr32.yaml
name: Scenario examples
uuid: 7da758ce-7c80-4169-a6ed-27abf3e5978f
```

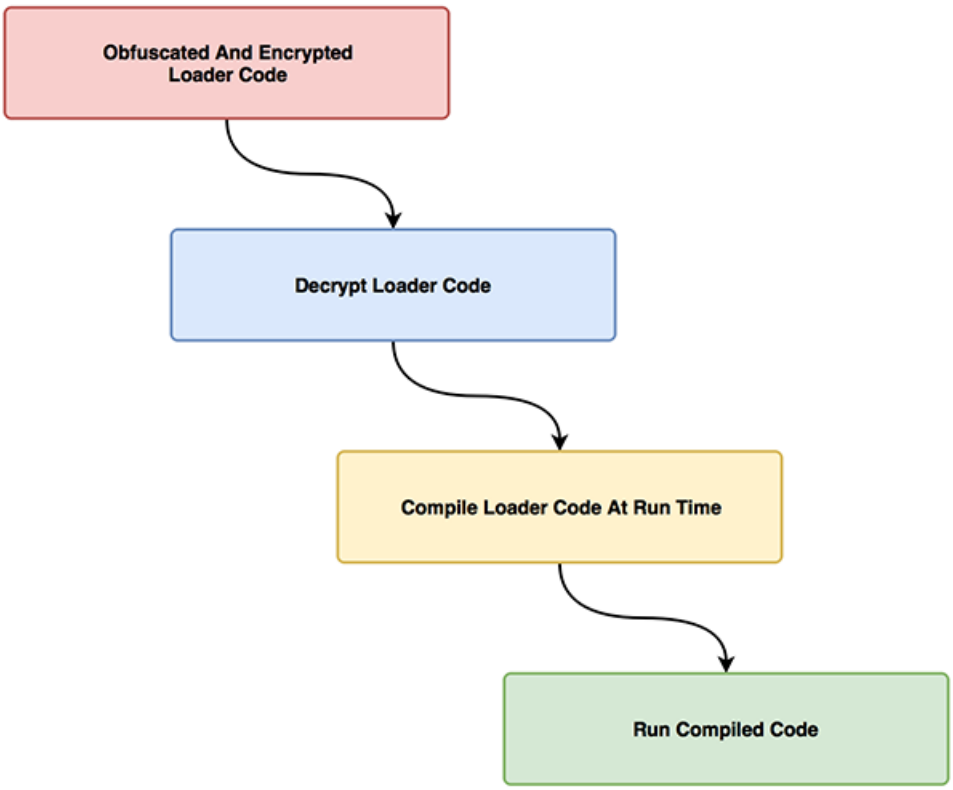
Github sayfası: https://github.com/uber-common/metta

Red Team Automation

RTA, mavi takımların MITRE ATT&CK modellerine göre oluşturulan saldırılara karşı algılama yeteneklerini test etmelerine izin veren bir betik framework'üdür. RTA, 50'den fazla farklı ATT&CK taktiğinin yanı sıra timestopping, process enjeksiyonları ve beacon simülasyonu gibi etkinlikleri gerçekleştiren python betiklerinden oluşur.

SpookFlare

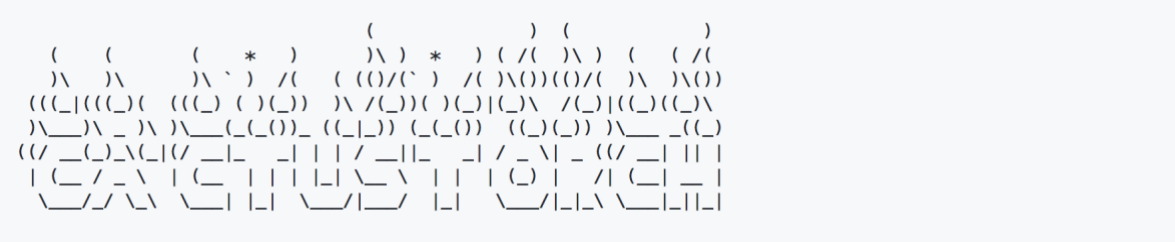
SpookFlare, güvenlik önlemlerini atlamak için farklı bir bakış açısına sahiptir ve size hem client tarafında hem de ağ tabanlı uç nokta önlemlerini atlatma fırsatı sağlamaktadır. SpookFlare, Meterpreter reverse HTTP ve HTTPS aşamaları için bir loader üreticisidir. SpookFlare, "string obfuscation" ve "run-time" kod derleme özelliklerine sahip özel bir encrypterdır. SpookFlare payload tekniğini ve davranışını öğrenene kadar hedef sistemlerin karşı önlemlerini atlatabilirsiniz. Aşağıdaki resimde SpookFlare payload çalışma adımlarını bulabilirsiniz.



SpookFlare kullanımı videolarını aşağıdaki linkten bulabilirsiniz:

SpookFlare HTA Loader for Koadic: https://youtu.be/6OyZuyIbRLU
SpookFlare PowerShell/VBA Loaders for Meterpreter: https://youtu.be/xFBRZz78U_M
v1.0 Usage Video: https://www.youtube.com/watch?v=p_eKKVoEl0o
Github: https://github.com/hlldz/SpookFlare

CactusTORCH



Cactustorch, bir javascript ve vbscript shellcode launcher(başlatıcısıdır.) 32-bit binaryler içerisine shellcode enjekte eder.

Nasıl Kullanılır?

Enjekte etmek istediğiniz bir binary seçin, varsayılan "rundll32.exe", örneğin notepad.exe, calc.exe kullanabilirsiniz. İstediğiniz framework içerisinde 32 bit shellcode oluşturun. (Kobalt Strike, Metasploit ile test edildi.)

Çalıştırın: “cat payload.bin | base64 -w 0”
JavaScript için: Oluşturduğunuz base64 payload'ı aşağıdaki kod değişkenine kopyalayın.

var code = "<base64 encoded 32 bit raw shellcode>";
vbScript için: Oluşturduğunuz base64 payload'ı aşağıdaki kod değişkenine kopyalayın.
Dim code: code = "<base64 encoded 32 bit raw shellcode>"

Komut satırından wscript.exe CACTUSTORCH.js veya wscript.exe CACTUSTORCH.vbs şeklinde çalıştırın.

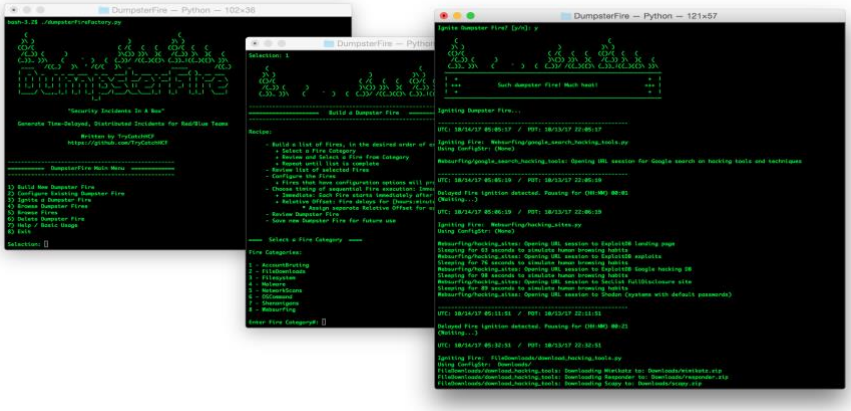
VBA için: base64 payloadını code.txt gibi bir dosyaya kopyalayın.

Daha sonra “python splitvba.py code.txt output.txt” çalıştırın. output.txt dosyasını aşağıdaki koda ekleyin. Aşağıdaki gibi gözükmesi gerekmektedir.

code = ""
code = code & "<base64 code in 100 byte chunk"
code = code & "<base64 code in 100 byte chunk"

Daha sonra tüm payload’ı Word Macrosuna kopyalayın ve kaydedin.

DumpsterFire



DumpsterFire araç seti, modüler olarak tasarlanmış özel güvenlik olayları oluşturmanıza olanak tanıyan cross platform bir çözümdür. Bu olay koleksiyonları (DumpsterFires) daha sonra zaman ayarlı, otomatik süreçler olarak da yürütülebilmektedir. DumpsterFire araç seti, belirlediğiniz senaryoları zaman ayarlı ve otomatik olarak oluşturabilmesi size bazı kolaylıklar sağlamaktadır. Örneğin, Mavi takımınızın dahili ağınızdaki Mirai Botnet aktivitesine nasıl tepki vereceğini merak ediyorsanız, Mirai modülünü aktifleştirebilirsiniz. Bu modül dahili ağ içerisinde kaba kuvvet saldırıları yaparak kullanıcı adı / parola kombinasyonlarını denemektedir. Kısmen Mirai Botnet'i simüle etmektedir.

DumpsterFire zaman damgalı loglar oluşturur, böylece kırmızı ve mavi takım ekipleri olayları koordine edebilir ve izleyebilir. Tüm olaylar UTC zaman dilimine göre gerçekleştirilir; böylece global operasyonlarınız, saat dilimleri ve uluslararası tarih satırları arasındaki dönüşümler hakkında endişe duymadan kolayca ilişkilendirilebilirsiniz.

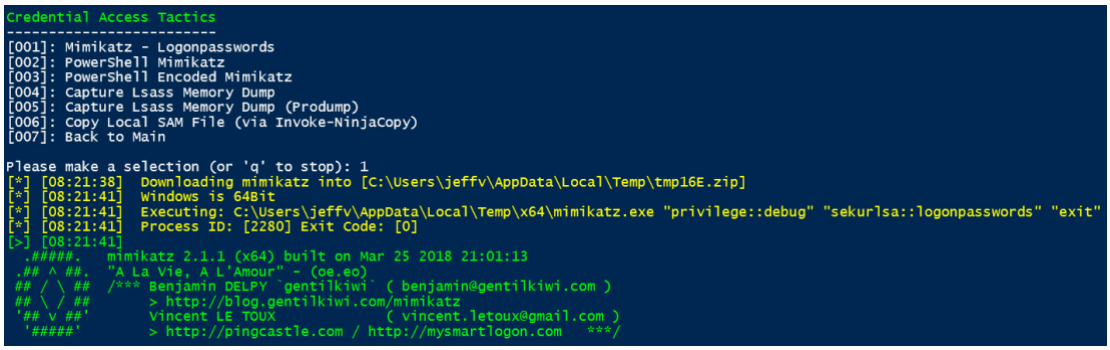
Nasıl Kullanılır?

```
$ ./dumpsterFireFactory.py
```

DumpsterFire, menu-driven bir araçtır. dumpsterFireFactory.py'i çalıştırdığınızda size bir DumpsterFire (senaryo) oluşturmak için menü sunar. Buradaki menüden kendi saldırı senaryolarınızı oluşturmanızı mümkün kılmaktadır.

Github: https://github.com/TryCatchHCF/DumpsterFire

Invoke-Adversary



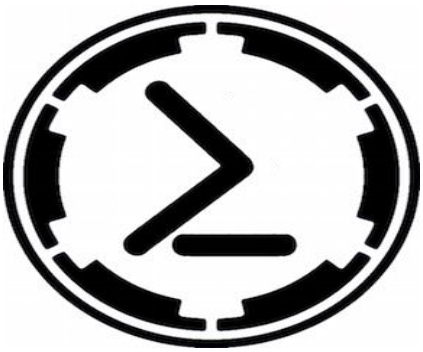
CyberSecurity Kill Chain, Lockheed Martin tarafından siber saldırı aktivitesinin belirlenmesi ve önlenmesi için geliştirilen bir frameworktür. Ataklar aşamalı olarak ortaya çıkabileceğinden, savunmacı olarak tüm süreci tespit etmek veya bozmak için görüş ve kontroller koyabilirsiniz. Birçok şirket, ortamlarını izlemek ve korumak için SIEM, Endpoint Protection Platform (EPP) ve Endpoint Detection & Reponse (EDR) ürünlerini kullanmaktadır.

Invoke-Adversary, güvenlik ürünlerinin ve monitoring (gözetleme) çözümlerinin, APT (Advanced Persistent Threat) saldırılarını ne kadar iyi tespit ettiğini değerlendirmenize yardımcı olan bir PowerShell betiğidir.

Invoke-Adversary, hedef odaklı saldırıyı temsil eden ve bunun için gerekli gerçek verileri oluşturabilen bir araç olmaktadır. Bu şekilde Invoke-Adversary kullanarak Security Monitoring (Güvenlik Gözetleme) ve Endpoint Security (Uç Nokta Güvenliği) ürünlerinizi değerlendirmenize olanak sağlamaktadır.

Proje sayfası ve detay:
https://blogs.technet.microsoft.com/motiba/2018/04/09/invoke-adversary-simulating-adversary-operations/

Empire



Empire, kriptolojik olarak güvenli iletişim sağlayan, esnek bir mimariye dayanan bir PowerShell post-exploitation ajandır (agent). Empire, Powershell.exe'ye gerek kalmadan PowerShell çalıştırmayı sağlayabilen, Keyloggerlardan Mimikatz'a kadar post-exploitation modülleri hızlıca yerleştirilebilin ve ağ tespit sistemlerinden kaçınmak için farklı teknikler barındıran bir uygulamadır. 2015 yılında BSidesLV'de yayınlanmıştır.

Empire hakkında tüm dokümantasyonu ve proje açıklamalarını http://www.powershellempire.com adresinde bulabilirsiniz.

PowerSploit

PowerSploit, bir değerlendirmenin tüm aşamalarında sızma testlerine yardımcı olmak için kullanılabilecek bir Microsoft PowerShell modülleri koleksiyonudur. PowerSploit, aşağıdaki modüller ve komut dosyalarından oluşur:

CodeExecution

Execute code on a target machine.

- Invoke-DllInjection
  Injects a Dll into the process ID of your choosing.
- Invoke-ReflectivePEInjection
  Reflectively loads a Windows PE file (DLL/EXE) in to the powershell process, or reflectively injects a DLL in to a remote process.
- Invoke-Shellcode
  Injects shellcode into the process ID of your choosing or within PowerShell locally.
- Invoke-WmiCommand
  Executes a PowerShell ScriptBlock on a target computer and returns its formatted output using WMI as a C2 channel.

ScriptModification

Modify and/or prepare scripts for execution on a compromised machine.

- Out-EncodedCommand
  Compresses, Base-64 encodes, and generates command-line output for a PowerShell payload script.
- Out-CompressedDll
  Compresses, Base-64 encodes, and outputs generated code to load a managed dll in memory.
- Out-EncryptedScript
  Encrypts text files/scripts.
- Remove-Comments
  Strips comments and extra whitespace from a script.
- Persistence
  Add persistence capabilities to a PowerShell script
- New-UserPersistenceOption
  Configure user-level persistence options for the Add-Persistence function.
- New-ElevatedPersistenceOption
  Configure elevated persistence options for the Add-Persistence function.
- Add-Persistence
  Add persistence capabilities to a script.
- Install-SSP
  Installs a security support provider (SSP) dll.
- Get-SecurityPackages
  Enumerates all loaded security packages (SSPs).

AntivirusBypass

AV doesn't stand a chance against PowerShell!

- Find-AVSignature
  Locates single Byte AV signatures utilizing the same method as DSplit from "class101".

Exfiltration

All your data belong to me!

- Invoke-TokenManipulation
  Lists available logon tokens. Creates processes with other users logon tokens, and impersonates logon tokens in the current thread.
- Invoke-CredentialInjection
  Create logons with clear-text credentials without triggering a suspicious Event ID 4648 (Explicit Credential Logon).
- Invoke-NinjaCopy
  Copies a file from an NTFS partitioned volume by reading the raw volume and parsing the NTFS structures.
- Invoke-Mimikatz
  Reflectively loads Mimikatz 2.0 in memory using PowerShell. Can be used to dump credentials without writing anything to disk. Can be used for any functionality provided with Mimikatz.
- Get-Keystrokes
  Logs keys pressed, time and the active window.
- Get-GPPPassword
  Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

- Get-GPPAutologon
  Retrieves autologon username and password from registry.xml if pushed through Group Policy Preferences.
- Get-TimedScreenshot
  A function that takes screenshots at a regular interval and saves them to a folder.
- New-VolumeShadowCopy
  Creates a new volume shadow copy.
- Get-VolumeShadowCopy
  Lists the device paths of all local volume shadow copies.
- Mount-VolumeShadowCopy
  Mounts a volume shadow copy.
- Remove-VolumeShadowCopy
  Deletes a volume shadow copy.
- Get-VaultCredential
  Displays Windows vault credential objects including cleartext web credentials.
- Out-Minidump
  Generates a full-memory minidump of a process.
- 'Get-MicrophoneAudio'
  Records audio from system microphone and saves to disk

Mayhem

Cause general mayhem with PowerShell.

- Set-MasterBootRecord
  Proof of concept code that overwrites the master boot record with the message of your choice.
- Set-CriticalProcess
  Causes your machine to blue screen upon exiting PowerShell.
- Privesc
  Tools to help with escalating privileges on a target.
- PowerUp
  Clearing house of common privilege escalation checks, along with some weaponization vectors.

Recon

Tools to aid in the reconnaissance phase of a penetration test.

- Invoke-Portscan
  Does a simple port scan using regular sockets, based (pretty) loosely on nmap.
- Get-HttpStatus
  Returns the HTTP Status Codes and full URL for specified paths when provided with a dictionary file.
- Invoke-ReverseDnsLookup
  Scans an IP address range for DNS PTR records.
- PowerView
  PowerView is series of functions that performs network and Windows domain enumeration and exploitation.

Github : https://github.com/PowerShellMafia/PowerSploit

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu", "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.