Başarılı Bir Siber Saldırının Perde Arkası ve Vaka Analizi

Onur ALANBEL

$ id -un

- Bilgisayar Mühendisi (**İYTE**)
- Uygulama Güvenliği Araştırmacısı
- Kurucu @**cricomtr** (cri.com.tr)
- Geliştirici @**TaintAll** (taintall.com)
- Github: github.com/**onura**
- Twitter: @**onuralanbel**
- https://packetstormsecurity.com/search/?q=onur+alanbel

Hacklendiğinizi Nasıl Anlarsınız?

- Sızan veriye erişimi olan sistemler/uygulamalar
- Erişim yetkisi olan kullanıcılar
- Anormallikler
  - Yetkisiz erişim denemeleri
  - Crash logları
  - Güvenlik alarmları (aksiyon alınan, alınmayan)
  - Saldırı kalıpları / izleri
  - Hedef sistemin bilinen zafiyetleri ve saldırı yüzeyi

Saldırının Adımları?

- İlk Erişim
  - Dışa açık servis ve uygulamalar (sunucu segmenti)
  - Oltalama saldırıları (kullanıcı segmenti)
  - Güvenlik veya temel ağ ürünleri (?)

Saldırının Adımları?

- Yetki yükseltme ve kalıcılık
  - LPE zafiyetleri
  - Temel ağ saldırıları
  - RAT yazılımları

Saldırının Adımları?

- İç ağda yayılma ve veri toplama
- Parola/hash saldırıları
- Servislere geniş erişimden dolayı yeni atak yüzeyi

Saldırının Adımları?

- Veri Sızıntısı
  - Hızlı ama kirli yol, genişbant transfer
  - Parçalara bölüp olağan trafiğe ekleme
  - Stenografi

Hangi Saldırı Nerede Görünür?

- WAF
- IPS
- Firewall
- Antivirus
- ATD
- System Event
- Anti-Spam
- Web Filter (Internal Proxy)
- DLP
- ...

Hangi Saldırı Nerede Görünür?

- Antivirus / APT
- Web Intrusion
- MS Windows
- Linux
- Network
- Data Leakage

Hangi Saldırı Nerede Görünür?

CATEGORY	NAME	STATUS	KILL-CHAIN	TAG NAME
AntiVirus / APT	Malicious File Detected (System)	Exist	LATCH_ON	SYS_MALWARE
AntiVirus / APT	Endpoint Protection System Stopped	Exist	EXPAND	SYS_PROTECTION_APP_DISABLED
AntiVirus / APT	Browser Exploit / Malicious Web Page	Exist	BREAK_IN	CLIENT_EXPLOIT
Web Intrusion	SQL Injection	Exist	BREAK_IN, GATHER, EXFILTRATE	WEB_SQLINJ
Web Intrusion	Cross Site Scripting	Exist	BREAK_IN	WEB_XSS
Web Intrusion	Directory Traversal	Exist	BREAK_IN	WEB_DIR_TRAVERSEL

Use Case >= 83

Hangi Saldırı Nasıl Görünür?

- Alarm
- Event Id

Hangi Saldırı Nasıl Görünür?

- Alarm
- Event Id
- Regex
- Korelasyon

Hangi Saldırı Nasıl Görünür?

```
'name': "APPFW_SQL", 'message': None, 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_SQLINJ},
'name': "APPFW_XSS", 'message': None, 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_XSS},
'name': "APPFW_DENYURL", 'message': "etc|passwd|group|hosts|win\.ini", 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_DIR_TRAVERSE
'name': "APPFW_DENYURL", 'message': "system|eval|passthru", 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_CMDINJ},
'name': "APPFW_SIGNATURE_MATCH", 'message': "corehttp long buffer", 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_ANOMALY},
'name': "APPFW_SIGNATURE_MATCH", 'message': "code injection", 'deviceEID': None, 'riskName': None, 'tag': Tag.WEB_CODEINJ},


'name': "anomaly detected", 'message': None, 'deviceEID': None, 'riskName': "TCP Anomaly", 'tag': Tag.NET_ANOMALY},


'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4728", 'riskName': None, 'tag': Tag.SYS_WIN_ACCOUNT_PR
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4729", 'riskName': None, 'tag': Tag.SYS_WIN_ACCOUNT_PR
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4720", 'riskName': None, 'tag': Tag.SYS_WIN_LOCAL_ACCO
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4726", 'riskName': None, 'tag': Tag.SYS_WIN_USER_ACCOU
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4625", 'riskName': None, 'tag': Tag.SYS_WIN_LOGIN_ANOM
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Security-Auditing:4719", 'riskName': None, 'tag': Tag.SYS_WIN_SEC_POLICY
'name': None, 'message': None, 'deviceEID': "Microsoft-Windows-Eventlog:1102", 'riskName': None, 'tag': Tag.SYS_WIN_LOG_CLEARED},
'name': "added|deleted|changed|removed|updated", 'message': None, 'deviceEID': None, 'riskName': "(Account Management)|(Security Group
'name': "log(.*)cleared", 'message': None, 'deviceEID': "Microsoft.Windows", 'riskName': None, 'tag': Tag.SYS_WIN_LOG_CLEARED},
```

Örnek

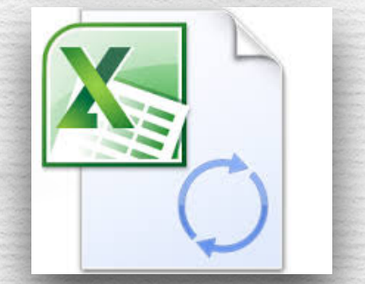
Örnek

Örnek

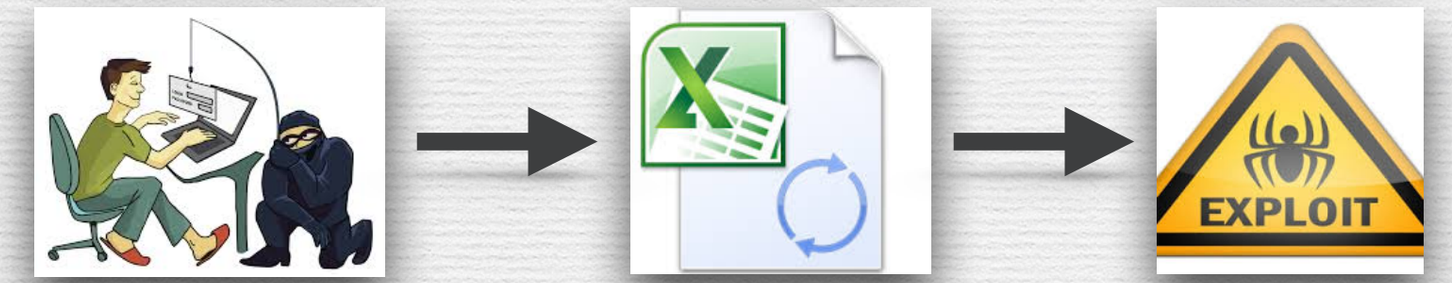
Tutarlılık

Örnek

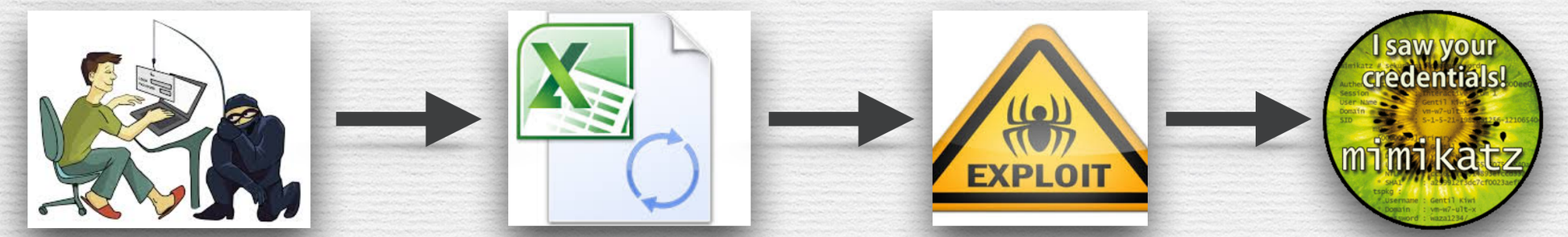
Örnek



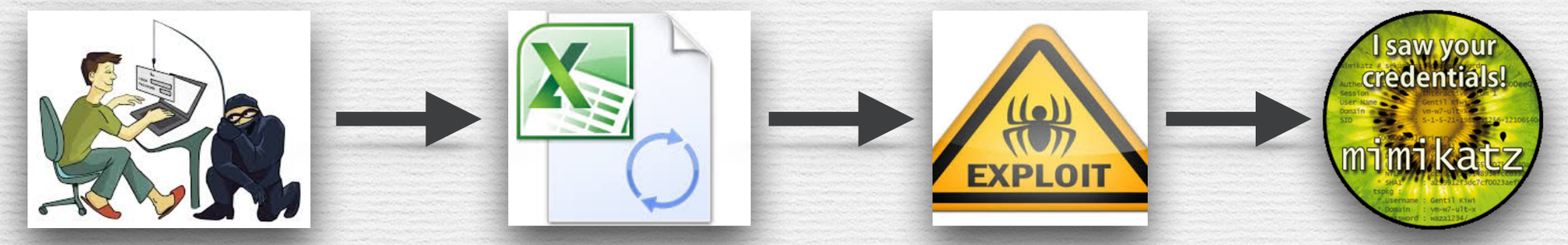
Örnek



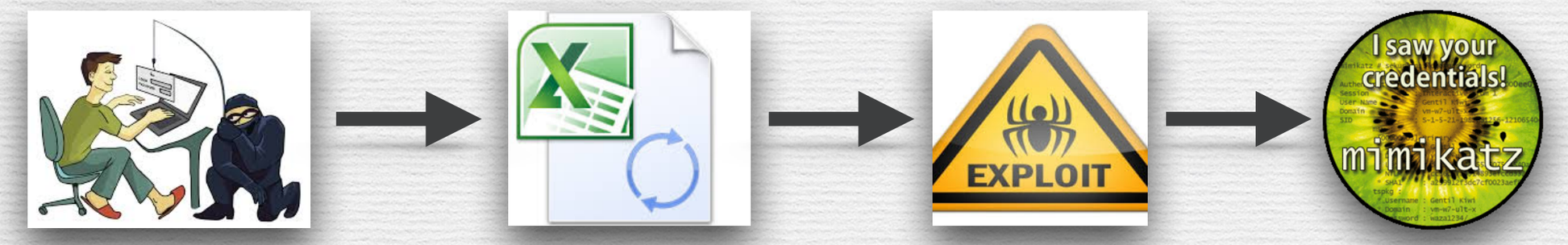
Örnek

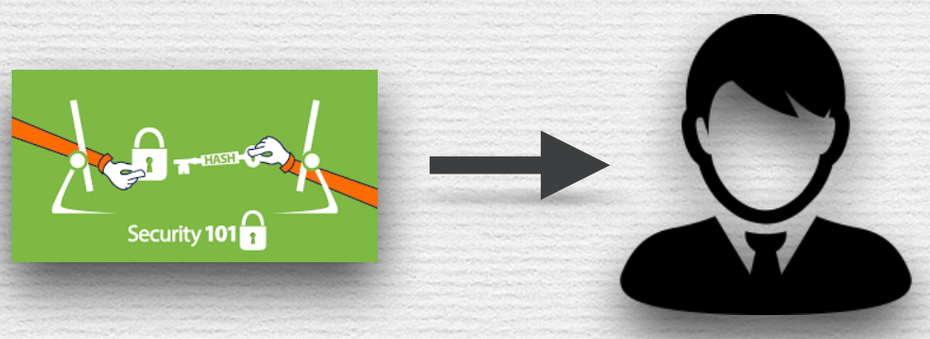


Örnek

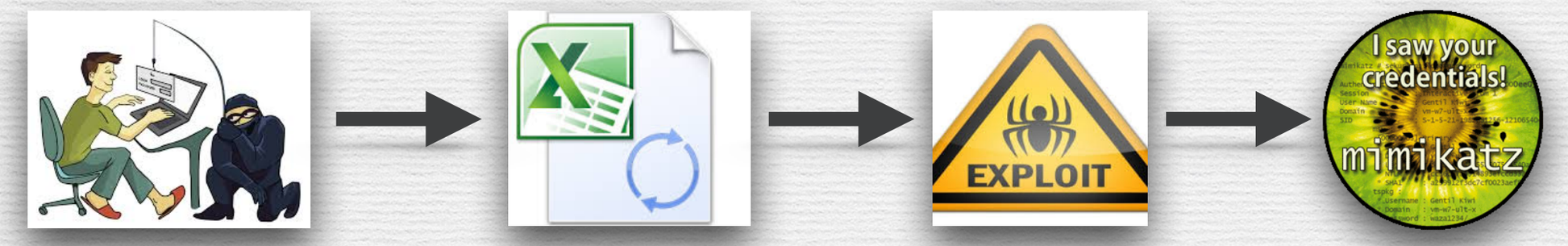


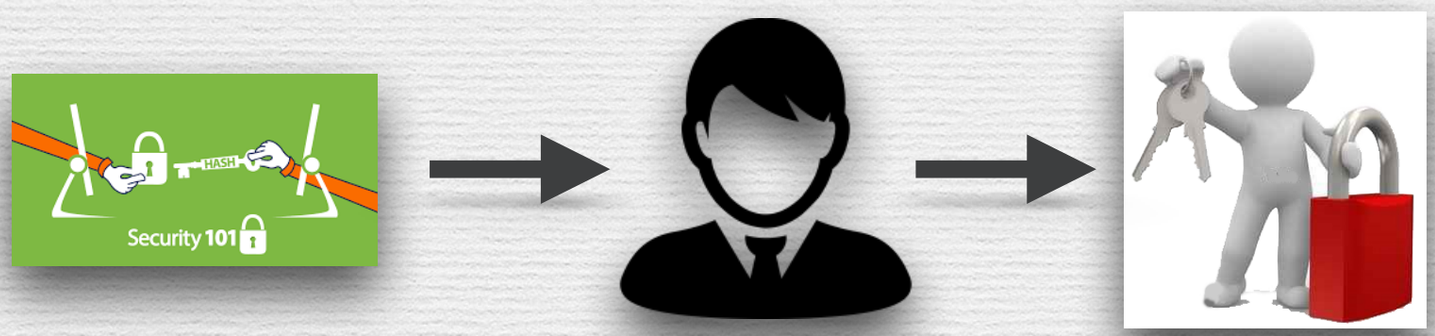
Örnek



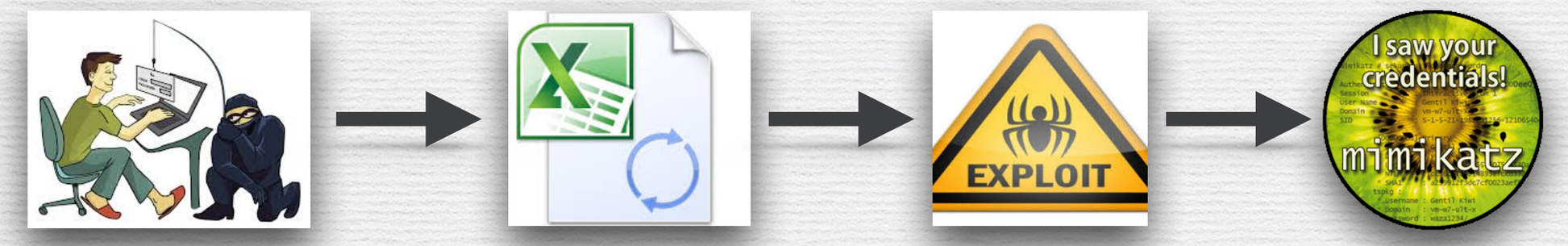


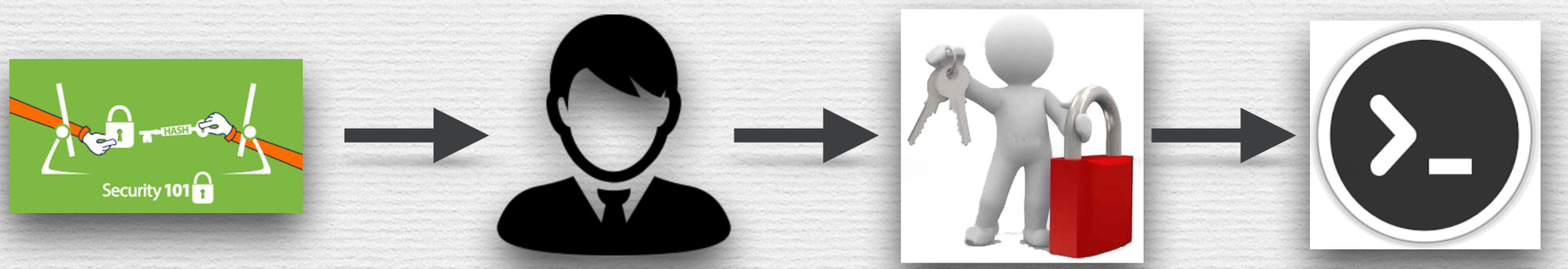
Örnek



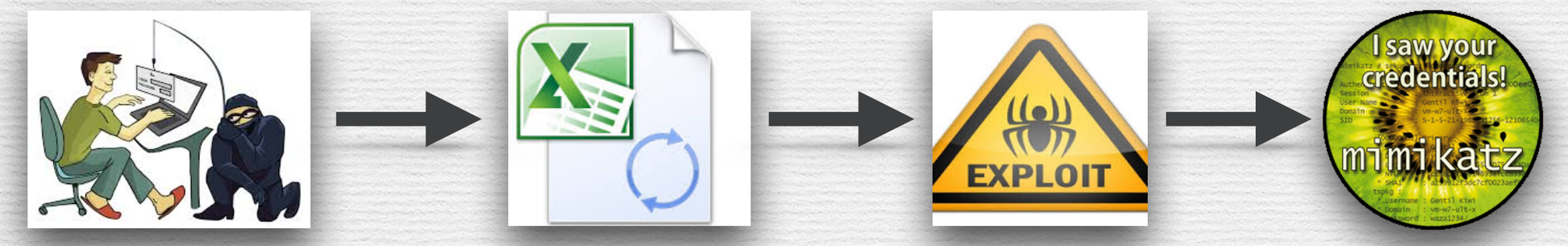


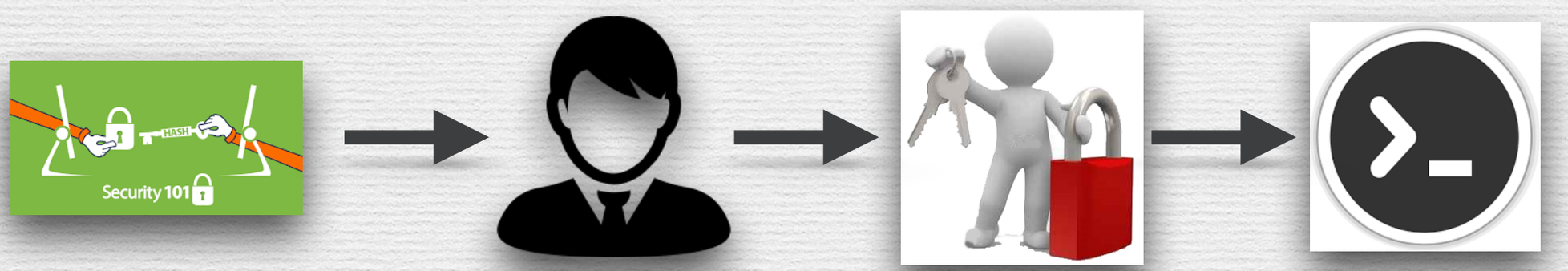
Örnek





Örnek





Sorumluluk