Red Team Operations

SEMAC 2017

Diego Mariano - diego.campos@**itau-unibanco**.com.br

Rafael Trassi - rafael.trassi@**itau-unibanco**.com.br

03 de outubro de 2017

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x01 - RED TEAM WTF?

- if (“Red Team” == “Time Vermelho”); then...

--[0x01 - RED TEAM WTF?

- Conceito militar
- Simular adversários avançados e altamente especializados
- Como nossa tropa de elite se sairia contra a elite da tropa?

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x02 - PENTEST vs RED TEAMING

- *Pentest*:
  - Testar aplicações *mobile ou web,* rede ou sistemas computacionais, com o objetivo de encontrar vulnerabilidades que um atacante poderia explorar;
  - Descobrir o maior número de brechas exploráveis o mais rápido possível;
  - Demonstrar o impacto e risco associado a ação de atacantes;

--[0x02 - PENTEST vs RED TEAMING

- *Red Teaming* foca em atividades, tais como:
  - Segurança Física;
  - Engenharia Social Profunda;
  - Desenvolvimento de Exploits customizados;
  - Período de testes maior e escopo mais permissivo;
  - Equipe de testes com diferentes habilidades (lembram do CTF?);
  - Mais habilidades → Mais tempo → Mais $$$:)

--[0x02 - PENTEST vs RED TEAMING

	Análise de Vulnerabilidades	Penetration Test	Red Team Operations
Propósito	Catalogar vulns.	Compreender o nível de 'Explorabilidade'	Avaliar a capacidade de Prevenir, Detectar e Responder
Objetivo	Encontrar todas vulns	Comprometer Tecnicamente (Domain Admin)	Comprometimento a nível de Negócio sem ser detectado
Escopo	Definido e Limitado	Definido e Limitado	Toda a Empresa
Metodologia	Automatizada	Misto	Manual
Técnicas	Simples: Escanear	Algumas: Redes, WebApp, Sist. Operacionais	TODAS: Sociais, Físicas, etc.
Cobertura	Ampla e rasa	Moderada	Estreita e Profunda
Cooperação com time de SecOps:	Completa	Limitada	Nenhuma*

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x03 - RED TEAM OPERATIONS

- Red Teaming ou Red Team Operations é uma definição do DoD - *Department of Defense*

- É uma "*operação organizada para simular a eficácia do ataque adversário contra uma missão.*"

- Conceito militar de *pensar como o adversário* que evoluiu para a *emulação de um adversário*.

--[0x03 - RED TEAM OPERATIONS

- Como operacionalizamos isto?

- Foco nos riscos impostos por atacantes avançados:

1. Autonomia do Red Team;
2. Acesso e Manipulação de Dados Sensíveis;
3. Janela 24x7 (o ladrão não te rouba enquanto você dorme? ☺).

--[0x03 - RED TEAM OPERATIONS

- Como operacionalizamos isto?

- Foco nos riscos impostos por atacantes avançados:

1. Autonomia do Red Team;
2. Acesso e Manipulação de Dados Sensíveis;
3. Janela 24x7 (o ladrão não te rouba enquanto você dorme? ☺).

- Somando 1, 2 e 3 obtemos o máximo de REALISMO durante as atividades!

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x04 - TTPs

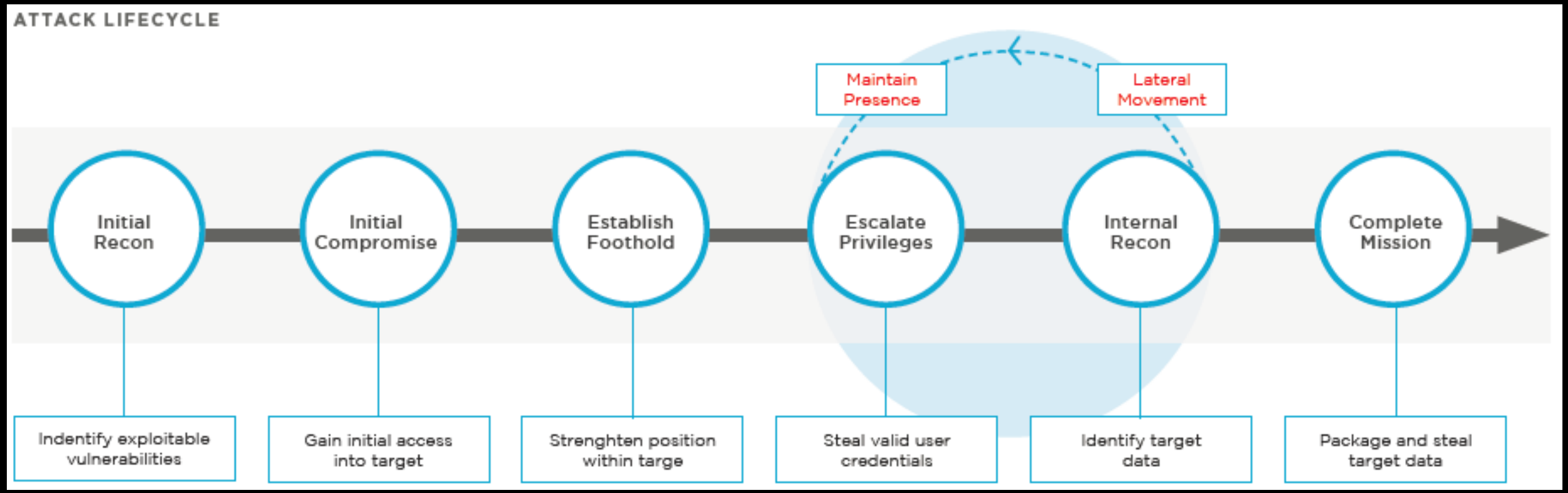
- TTPs = Tools Tactics and Procedures
- Quais as ferramentas, procedimentos e técnicas utilizados por nossos adversários?
- Como enfrentar um adversário capacitado, comprometido e com recursos ilimitados?
- Exemplo: STUXNET

--[0x04 - TTPs

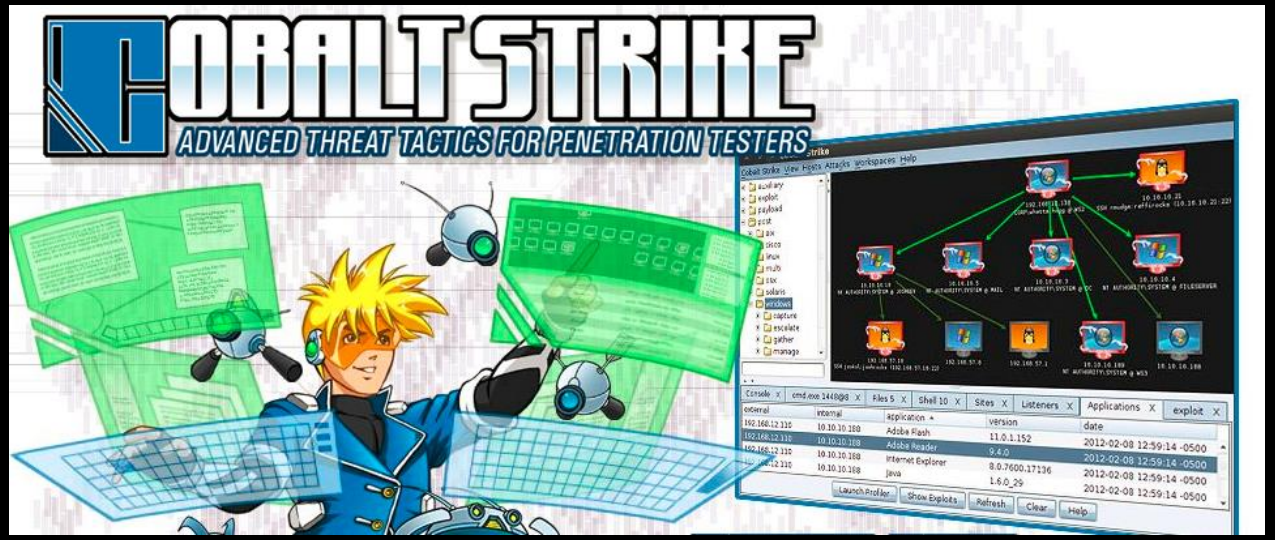
- Obter acesso é uma questão de tempo!
- Filosofia: *assume breach*!
- Focar nas atividades *pós exploração*:

```
┌─ Obter Acesso
└─➤  ┌─ Obter Consciência Situacional
     └─➤ ┌─ Escalar Privilégios
         └─➤  ┌─ Identificar Mais Pontos de Exploração
              └─➤  ┌─ Adquirir Privilégios Administrativos e de Domínio
                   └─➤  ┌─ Estabelecer Persistência
                        └─➤ ┌─ Mineração de Dados buscando Informações Sensíveis
                            └─➤ Identificar pontos que impactam os negócios †
```

--[0x04 - TTPs


ATTACK LIFECYCLE
Maintain Presence
Lateral Movement
Initial Recon
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Complete Mission
Indentify exploitable vulnerabilities
Gain initial access into target
Strenghten position within targe
Steal valid user credentials
Identify target data
Package and steal target data

--[0x04 - TTPs


COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS


I saw your credentials!
mimikatz

--[0x04 - TTPs


WONKA
GOLDEN TICKET
DATE
FEB.1
TIME
10 A.M.(SHARP)
PLACE
FRONT GATES
THIS GOLDEN TICKET ENSURES ADMITTANCE.
COBA
ADVANCED THRE
saw your
edentials!
mikatz

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- Avaliar a capacidade do BLUE TEAM (equipe de *Resposta a Incidentes*) responder a ameaças desconhecidas;

- Avaliar a capacidade e SLA das equipes de NOC e SOC de:
  1. Conhecer;
  2. Antecipar, e;
  3. Reportar ameaças, atividades suspeitas e falhas.

- É fácil ser ZEN quando tudo está em ordem e funciona...

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- Avaliar a capacidade do BLUE TEAM (equipe de *Resposta a Incidentes*) responder a ameaças desconhecidas;

- Avaliar a capacidade e SLA das equipes de NOC e SOC de:
  1. Conhecer;
  2. Antecipar, e;
  3. Reportar ameaças, atividades suspeitas e falhas.

- É fácil ser ZEN quando tudo está em ordem e funciona...

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- O que aconteceria se soltássemos o *Chaos Monkey* na rede da **UNESP**?

- Red Teaming é uma atividade que procura fornecer resposta para este tipo de pergunta.

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- O que aconteceria se soltássemos o *Chaos Monkey* na rede da **UNESP**?

Chaos Monkey is a service which runs in the Amazon Web Services (AWS) that seeks out Auto Scaling Groups (ASGs) and terminates instances (virtual machines) per group. The software design is flexible enough to work with other cloud providers or instance groupings and can be enhanced to add that support. Jul 30, 2012

The Netflix Tech Blog: Chaos Monkey Released Into The Wild
techblog.netflix.com/2012/07/**chaos-monkey**-released-into-wild.html

- Red Teaming é uma atividade que procura fornecer resposta para este tipo de pergunta.

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- As guerras atuais não são disputadas em trincheiras...

- Estas atividades ajudam na capacitação de CDCIBER - Centros de Defesa Cibernética

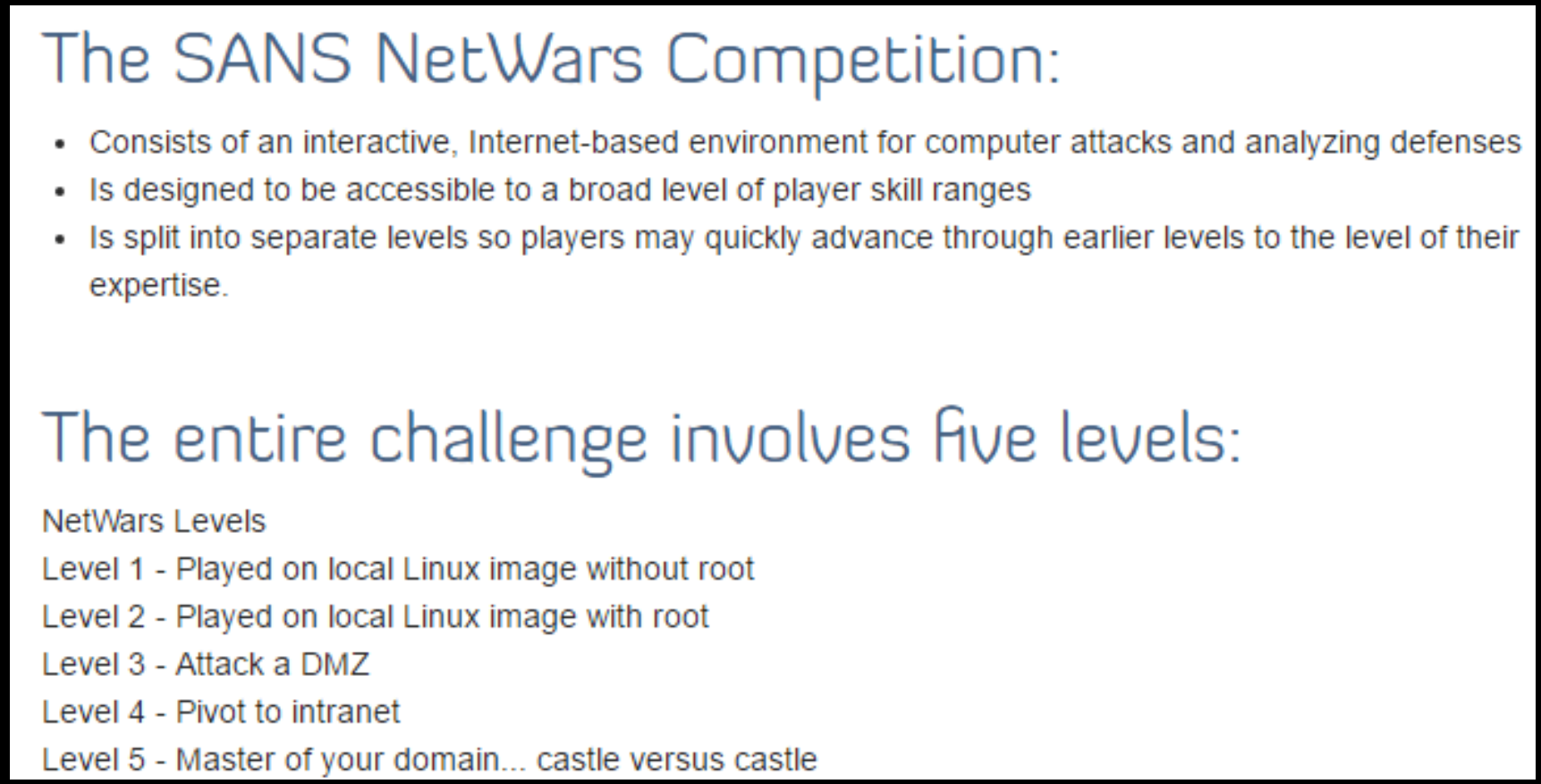
--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- Vamos falar de CTF? ☺
- SANS NetWars;
- HackTheBox
- CCDC
- CTF365

VULNHUB
VULNERABLE BY DESIGN

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

- SANS NetWars;



The SANS NetWars Competition:

- Consists of an interactive, Internet-based environment for computer attacks and analyzing defenses
- Is designed to be accessible to a broad level of player skill ranges
- Is split into separate levels so players may quickly advance through earlier levels to the level of their expertise.

The entire challenge involves five levels:

NetWars Levels
Level 1 - Played on local Linux image without root
Level 2 - Played on local Linux image with root
Level 3 - Attack a DMZ
Level 4 - Pivot to intranet
Level 5 - Master of your domain... castle versus castle

CTF365 Capture The Flag

MAP SCORE BLOG COMMUNITY

Report a vulnerability ChOkO

Most active users

User	Team	Actions
CyberPrepLevel5	TheJokerBand	920150
Suspect X	hex hex	381242
DorsiaSec	-	295414
metalkey	metalkey	227770

Time	Attacker	Target	Attack type
2016-06-22 17:11:14	ƒıβєяgнost	PorciiRozalii	http_inspect:
2016-06-22 17:10:55	ƒıβєяgнost	Deadly Kittens	http_inspect:
2016-06-22 16:53:12	Jordan23	PorciiRozalii	http_inspect:
2016-06-22 11:47:14	Cranch	PorciiRozalii	stream5:
2016-06-22 04:15:40	mysockmonkey	PorciiRozalii	stream5:

```
┌[root@Overlord] [/dev/pts/4]
└[/_RED_TEAM_OPERATIONS_]> agenda
```

--[0x01 - RED TEAM WTF?

--[0x02 - PENTEST vs RED TEAMING

--[0x03 - RED TEAM OPERATIONS

--[0x04 - TTPs

--[0x05 - MOTIVAÇÃO E BENEFÍCIOS

--[0x06 - CONCLUSÃO

--[0x06 - CONCLUSÃO

- O que agrega mais valor à organização:
  1. entregar um relatório informando que invadimos tudo? ☺
  2. entregar um relatório informando como um concorrente poderia comprometer o negócio da empresa roubando segredos comerciais ou como detectar uma ameaça mesmo sem conhece-la?
- *Reality-check*:
  - alguém reclamou quando a aplicação ou o servidor caíram?
  - quando "fizemos barulho" alguém ficou sabendo?
  - alguém reportou?

--[0x06 - CONCLUSÃO

- Descobrir pontos cegos e outras oportunidades de exploração que um atacante poderia utilizar para invadir a empresa.

- Desmistificar a idéia de alguns executivos que suas empresas são "*unhackable*".

- A possibilidade de executar um *engagement* longo pode simular o "conhecimento perfeito" do ambiente de rede (quando um invasor está presente durante vários anos).