**REPORT RED TEAM**

Joas A Santos

### **Introdução**

O envolvimento é realizado por técnicas usadas por adversários do mundo real empregadas para atingir os sistemas em teste. A sequência de atividades nesta abordagem envolve coleta, exploração e ataque, a fim de realizar impactos operacionais específicos de objetivos.

**Objetivos:**

* Coletar credenciais do XXX via Spear-Phishing
* Exfiltrar dados

### **Pontos positivos**

Embora os compromissos da Red Team se concentrem nas fraquezas de segurança

1 - Os usuários foram resilientes em clicar no e-mail e colocar suas credenciais

2 -

3- Abertura de chamado

**Pontos negativos:**

* Contudo foi feito o bloqueio do remetente e não do domínio, permitindo que o ataque continuasse através de outro remetente.

### **Metodologia**

Os compromissos da Red Team realizados pelo time de OffSec da XXX empregam técnicas de adversários reais para atingir os sistemas. Usando um modelo de Red Team que emula ferramentas, técnicas e procedimentos (TTPs) de adversários reais, orientados por cenários e objetivos de ataque. Ao contrário de um PenTest tradicional, o exercício de red team permite testar todo o escopo de segurança de uma organização, incluindo pessoas, processos e tecnologia.

### **Cenários**

O Exercício do Red Team foi baseado em um ataque de phishing coordenado para iniciar o teste contra usuários que não tinham conhecimento do envolvimento.

### **Plano de Testes com base no Att&ck**

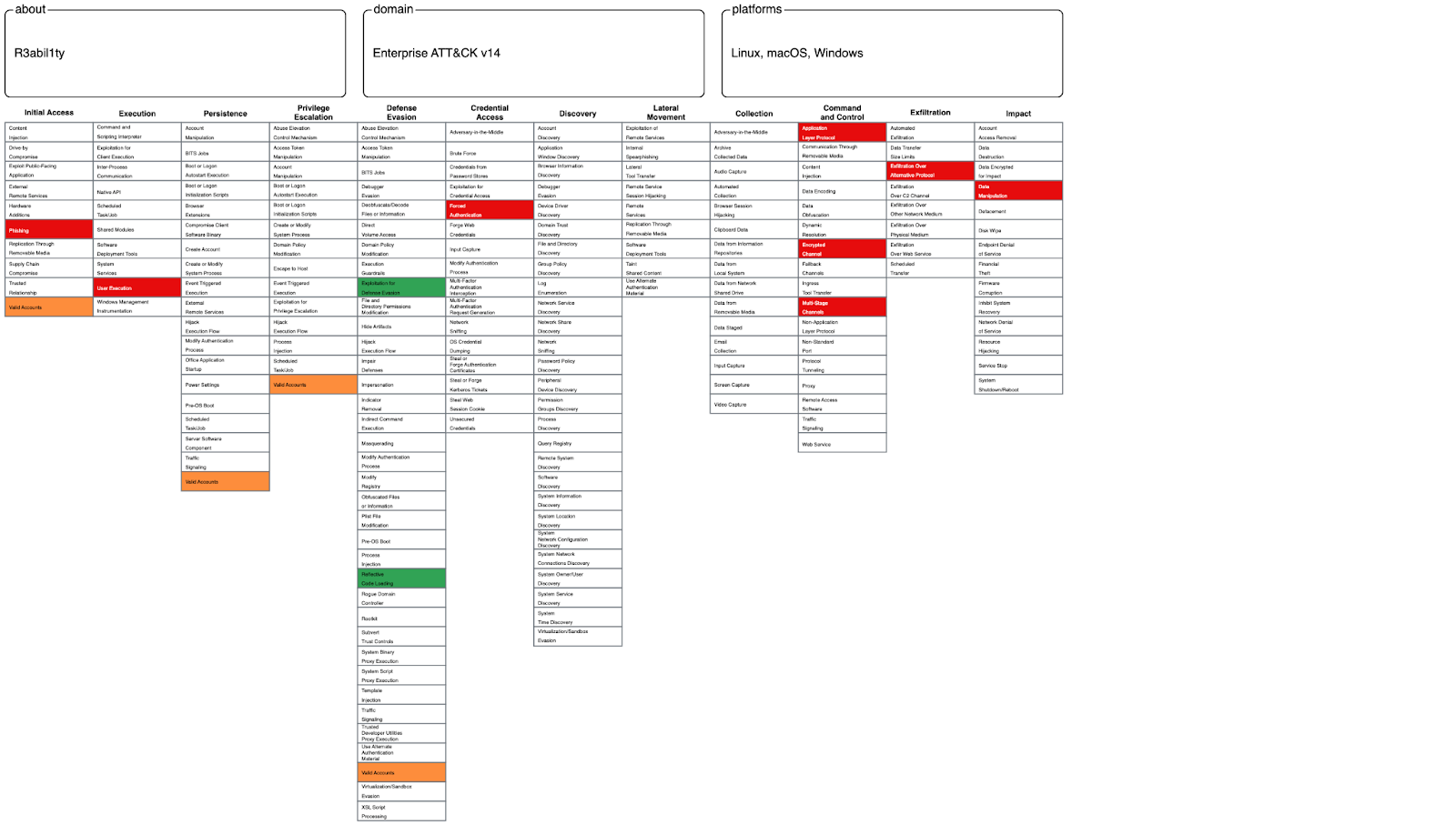


Figura 1: TTPs do exercício

Vermelho: Indica técnicas críticas que são ativamente utilizadas em campanhas maliciosas e que requerem atenção imediata para mitigação. Como os métodos de acesso inicial como spear phishing, execução de códigos maliciosos, comando e controle e exfiltração de dados.

Laranja: Pode representar técnicas de alto risco que, ainda representam uma ameaça significativa. Como contas válidas que podem dar acesso a serviços internos.

Verde: Geralmente estão associados a técnicas que são menos críticas ou menos comuns, mas que ainda precisam ser endereçadas pelas equipes de segurança. Como métodos de persistência como uso de serviços legítimos ou táticas de evasão de defesa como a desativação de controles de segurança.

### **Escopo**

O Escopo é a infraestrutura da XXX e os usuários da área xxxx

### **Diversos**

Sem informações extras

### **Narrativa do Ataque**

A seção a seguir descreve a sequência de eventos e destaca os pontos-chave durante o envolvimento:

**Figura 2: Fluxo de ataque - Spear-Phishing e C2**

**Recon**

Para iniciar, os atacantes realizam uma pesquisa detalhada sobre o alvo, coletando informações que podem incluir nomes de funcionários, cargos, detalhes de contato e qualquer outra informação relevante que possa aumentar a veracidade do ataque.

**Acesso Inicial**

**Credencial de Acesso**

Em relação ao acesso às credenciais, a estratégia consiste em capturar essas credenciais para, então, acessar outros ambientes internos. Uma vez dentro, o foco se volta para a coleta de informações confidenciais e dados valiosos.

### **OpSec**

Lista de técnicas de OpSec utilizadas:

* Escolher alvos que provavelmente têm as informações desejadas e são suscetíveis ao ataque.
* Utilizar técnicas para disfarçar o phishing e evitar detecção por filtros de e-mail e software antivírus.
* Registrar domínios que são visualmente semelhantes aos legítimos e dificilmente detectáveis como fraudulentos. Como o uso do IDN Homograph para criar um dominio quase parecido.
* Executar campanhas de teste para medir a eficácia e detecção dos e-mails de phishing.
* Usar técnicas para minimizar a pegada digital deixada nas comunicações e hospedagem.
* Variar os tempos de comunicação e a quantidade de dados transmitidos para evitar a criação de padrões detectáveis.

### **Passo a passo**

| Spear Phishing | **01** |
| --- | --- |

**Descrição:**

**Prova de Conceito:**

**Lições aprendidas:**

1. Email SMTP da Godaddy entrou em blacklist e adquirimos um na hostgator também
2. Trocamos o Evilginx pro Modlishka, pois precisaria criar um phishlet e não tínhamos tempo hábil para isso
3. Foi necessário comprar um outro domínio em outra empresa de hospedagem para continuar as campanhas
4. Para evitar a blacklist a recomendação não é spammar emails para testar

### **Conclusão**

A XXX realizou um envolvimento da Red Team para determinar o impacto total de uma ameaça de spear-phishing realista. Não foi possível exfiltrar muitos dados….

# **Controles de versão**

|  |  |
| --- | --- |
| Report feito por | Report revisado por |
| Joas A Santos |  |