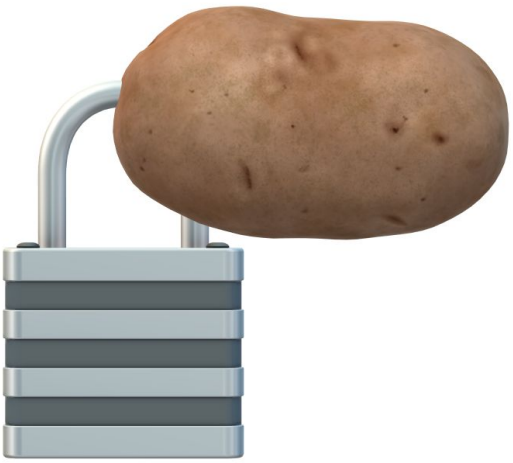
Starch Consulting



인프라 침투 테스트

RVAPTHosting

2020년 4월 22일

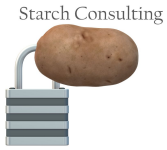
의해서 준비되었다:

제이콥 루드
에매뉴얼 아데웰
오마르 알잘라우드
압둘말리크 바나세르

발표자:

밥 디노
조 뱅크
존 도우

목차



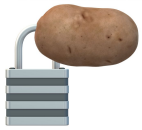
부인 성명

Starch Consulting은 이 테스트 결과가 회사의 인프라 내에 존재하는 모든 위험을 절대적으로 식별할 것이라고 보장하지 않으며 제안된 모든 완화 기술을 구현한 후에도 위반이 발생하는 경우 책임을 질 수 없습니다.

요약

스타치컨설팅 외 al은 회사 인프라에 대한 포괄적인 평가를 수행하기 위해 RVAPTHosting("회사"라고도 함)과 계약을 맺었습니다. 이 평가의 목표는 해당 인프라에 존재할 수 있는 취약성의 결과로 조직에 대한 잠재적인 위험을 결정하는 것이었습니다. 이 테스트는 "블랙 박스 평가"로 설계되었습니다. 즉, Starch Consulting은 호스팅 DMZ에 대한 VPN 액세스 이외의 인프라에 대한 지식을 제공받지 못했습니다. 모든 테스트는 생산 환경에서 수행되었으므로 The Company가 가동 중지 시간을 최대한 줄이도록 조치를 취했습니다. RVAPTHosting과 고객은 계약 기간 동안 테스트가 진행된다는 사실을 알게 되었습니다. 모든 테스트는 사용자 계정 정보와 금융 데이터를 안전하게 유지한다는 최종 목표로 수행되었습니다.개요 .이 보고서의 섹션.

조사 결과에 따라 회사는 시스템 및 네트워크 손상 또는 민감한 고객 정보 공개를 통해 비즈니스 영향을 받을 수 있습니다. 취약한 비밀번호 저장 및 사용 정책이 인프라에 적용되면 중요한 네트워크 엔드포인트가 손상되거나 다운타임이 발생하여 재정적 영향과 고객 불만이 발생할 수 있습니다. 또한 고객 재무 정보의 노출은 PCI-DSS 및 GDPR을 포함한 여러 규정 준수 위반에 해당하며 부적절하게 처리할 경우 잠재적인 소송을 의미할 수 있습니다. Starch Consulting은 정상적인 비즈니스 운영에 중대한 영향을 미치지 않도록 가능한 한 빨리 이러한 문제를 해결할 것을 제안합니다.



경영개요

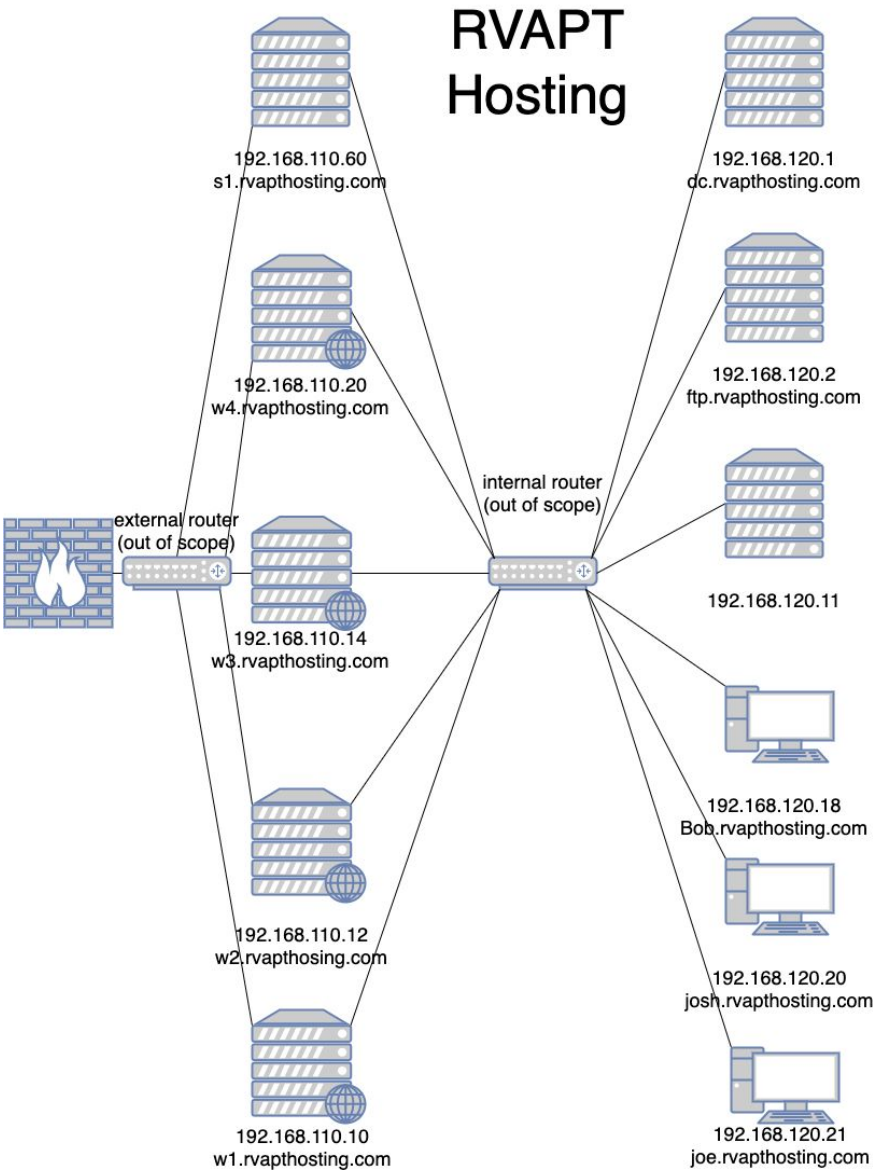
The Company의 기업 인프라를 조사한 후 Starch Consulting은 **기본 자격 증명 사용**뿐만 아니라**민감한 클라이언트 정보가 손상됨**회사의 네트워크에서. 이 두 가지 결과는높은우선 순위를 정하고 가능한 한 빨리 완화해야 합니다.

일반 텍스트 비밀번호 저장그리고**비밀번호 재사용**도 발견되었습니다. 이러한 결과는 중간우선순위 위험. 회사는 사례별로 위험을 수정하거나 수용하기 위한 일정을 개발해야 합니다.

마침내 스타치컨설팅이 찾아낸**활성 레거시 장치**그리고**활성 은퇴 사용자 계정**인프라에서 사용할 수 있습니다. 이러한 결과는낮은우선순위 위험. 회사는 이러한 위험을 수용하거나 개선하기로 결정할 수 있습니다.

토폴로지

Starch Consulting은 계약 중에 다음과 같은 네트워크 토폴로지를 생성할 수 있었습니다. 알 수 없는 장치는 가능한 한 빨리 조사해야 합니다.

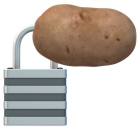


참여 일정(2020년 4월 6~16일)

- 4월 7일
  - 기본 자격 증명을 사용하여 192.168.110.60(webmin)에 액세스
  - 내부망 존재 발견
  - ssh 개인 키 발견
  - 192.168.110.0/24 서브넷의 모든 호스트에 대한 액세스 권한을 얻었습니다.
  - 192.168.110.14에서 실행되는 VNC에 대한 자격 증명을 찾았습니다.
    - 두 개의 계정:
      - 실크로드
      - 192.168.110.1
- 4월 8일
  - sysadminmike 암호 해독(외부 네트워크에 대한 ssh 액세스 허용)
  - 내부 네트워크 추가 열거(아직 접근 불가)
  - 더 많은 일반 텍스트 암호 발견
- 4월 10일
  - 내부망 접속
  - 이전 FTP 서버에 대한 액세스 자격 증명을 찾았습니다.
  - 다른 사용자로 접근 권한 획득
    - 두 개의 도메인 계정에 액세스
- 4월 11일
  - Josh의 자격 증명으로 Joe의 컴퓨터에 로그인
- 4월 12일
  - APT 활동 발견(Joe에게 보고)
- 4월 16일(마지막 날)
  - DC 발견/액세스
  - 데이터베이스에 들어가 민감한 정보를 찾았습니다.
  - 다양한 수준의 권한으로 내부 네트워크의 모든 컴퓨터에 액세스했습니다.

위험 수준 방법론

기술적 위험이 식별되면 CVSS(Common Vulnerability Scoring System) 점수를 기반으로 심각도에 따라 분류됩니다. 이는 비즈니스 운영에 대한 가능성과 영향에 따라 결정됩니다.



위험가치는 기술적 위험이 회사의 기반시설에 미치는 위험을 나타내며 아래 표를 사용하여 산정됩니다.

위험 수준 방법론	영향			
있을 수 있는 일		낮은	중간	높은
	낮은	낮은	낮은	낮은
	중간	낮은	중간	중간
	높은	낮은	중간	높은

표 1: 위험 수준 매트릭스

위험 등급은 다음 기본 원칙에 따라 완화 계획을 추진하는 데 도움이 됩니다.

- 높음: 완화는 가능한 한 빨리 일정을 잡아야 합니다. CVSS 점수 7.0-10.0
- 매체: 회사는 사례별로 위험을 수정하거나 수용하기 위한 일정을 개발해야 합니다. 4.0-6.9의 CVSS 점수
- 낮음: 회사는 위험을 감수하거나 개선하기로 결정할 수 있습니다. 0.0-3.9의 CVSS 점수

권장 완화 계획

회사는 다음 매개변수를 기반으로 완화를 계획해야 합니다.

1. **위험 수준**- 높은 위험 수준의 취약점을 먼저 해결해야 하며 중간 및 낮은 위험 항목은 낮은 우선 순위를 갖습니다.
2. **완화할 시간**- 시간이 가장 짧은 완화가 먼저 처리되어야 하며 시간이 긴 항목은 우선 순위가 낮습니다.

기술적 위험

위험	있을 수 있는 일	영향	우선 사항
기본 자격 증명	.높은	높은	높은
손상된 클라이언트 정보	높은	높은	높은
일반 텍스트 암호 저장	중간	높은	중간
비밀번호 재사용	높은	중간	중간
활성 레거시 장치	높은	낮은	낮은
활성 은퇴 사용자 계정	높은	낮은	낮은

표 2 - 기술적 위험

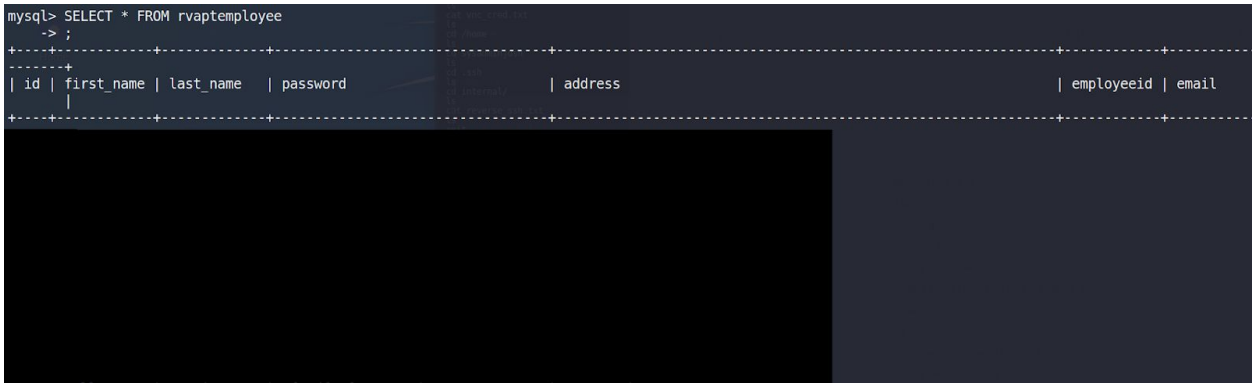
높음우선순위 위험

- 기본 자격 증명(CVSS 9.0)
  - **설명**: 중요한 서버(webmin) 중 하나에 기본 자격 증명이 있습니다. 이것은 네트워크에 대한 Starch Consulting의 초기 액세스로 이어집니다.
  - **있을 수 있는 일**(높음) - 기본 암호를 사용하면 공격자가 웹 서버에서 바로 로그인하여 시스템 명령을 실행할 수 있습니다.
  - **영향**(높음): 이것은 공격자가 시스템에 침입해야 할 때 침입자의 항목이 될 수 있습니다. SSH 키를 서버에 저장하여 지속성을 설정할 수 있습니다.
  - **증거**: webmin의 기본 비밀번호로 로그인하면 누구나 웹 서버에 로그인할 수 있습니다.
  - **완화:**.기본 cred를 보다 안전하고 복잡한 암호로 변경합니다.

● 손상된 클라이언트 정보(CVSS 10.0)

- ○ **설명**: Starch Consulting은 루트 사용자의 취약한 암호를 통해 SQL 코어 호스팅 데이터베이스에 액세스했습니다. 이를 통해 공격자는 코어 데이터베이스에 로그인하여 Rvapthositng 직원 및 클라이언트를 보고 수정할 수 있습니다.

- ○ **있을 수 있는 일**(높음) - 재사용 가능한 암호를 사용하면 공격자가 데이터베이스에 액세스하는 데 사용할 암호를 추측할 수 있습니다.
- ○ **영향**(높음): 공격자가 클라이언트의 데이터를 판매할 수 있기 때문에 데이터베이스를 변경하는 기능은 Rvapthosting에 매우 중요합니다.
- ○ **증거**:



- ○ **완화**: 데이터베이스에 더 복잡한 비밀번호를 사용하고 데스크탑과 같이 찾기 쉬운 위치에 저장하지 않습니다.

매체우선순위 위험

- 일반 텍스트 암호 저장소(CVSS 5.0)
  - **설명**- 일반 텍스트로 된 사용자 계정 및 암호 저장이 네트워크 전체에서 발견되었습니다.
  - **있을 수 있는 일**(매체) - 기본 열거 및 일반 텍스트 이름은 추가 자격 증명을 찾도록 안내합니다.
  - **영향**(높음) - 공격자는 내부 네트워크를 확장할 수 있으며 이로 인해 추가 피해가 발생할 수 있습니다.
  - **증거**- C 드라이브로 이동하여 oldftp에 대한 자격 증명이 있는 일반 텍스트를 찾습니다.

```
    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/17/2020  11:04 PM                Abyss Web Server
d-----         3/18/2019   9:52 PM                PerfLogs
d-r---         3/17/2020   5:48 AM                Program Files
d-r---         3/16/2020   8:35 PM                Program Files (x86)
d-----         3/28/2020   1:49 PM                share
d-----         3/16/2020   6:43 PM                tools
d-r---         3/28/2020   1:40 PM                Users
d-----         3/17/2020   4:52 AM                Windows
-a----         3/17/2020  10:15 PM            108 oldftp.txt


*Evil-WinRM* PS C:\> type oldftp.txt
josh:[redacted]          - for the old ftp server
*Evil-WinRM* PS C:\>
```

```
[admin@s1 internal]# ls
 reverse_ssh.txt
[admin@s1 internal]# cat reverse_ssh.txt
 rvapthosting.com\josh:[redacted]

 [Our domain - rvapthosting.com]
 [My comp]
 192.168.120.20:22
[admin@s1 internal]#
```

  - **완화**- 이상적인 솔루션은 일반 텍스트 비밀번호 저장과 관련된 위험을 제거하기 위해 중요한 정보가 포함된 일반 텍스트를 암호화하거나 삭제하는 것입니다.

- 비밀번호 재사용(CVSS 4.5)
  - **설명**- Starch Consulting은 RVAPTHosting 직원 중 일부가 다른 시스템이나 다른 서비스에서 비밀번호를 재사용한다는 사실을 알아냈습니다.
  - **있을 수 있는 일**(매체) - 암호 재사용은 사람들이 해서는 안 되는 일반적인 관행이므로 공격자는 다른 사용자/서비스에서 찾은 암호를 사용하려고 시도합니다.
  - **영향**(높음) - 공격자가 권한 있는 사용자에 대한 액세스 권한을 매우 쉽게 얻을 수 있습니다.
  - **증거**- 비밀번호 재사용은 스타치컨설팅이 조쉬 비밀번호를 사용하여 mysql 서비스에 접근할 수 있을 뿐만 아니라 내부 네트워크의 모든 조쉬 계정에 접근할 수 있도록 합니다.
  - **완화**- 직원들이 서로 다른 기계 및 서로 다른 서비스에 대해 고유한 암호를 사용하도록 강제합니다.

낮음우선순위 위험

- 활성 레거시 장치(CVSS 2.0)
  - **설명**- 의 레거시 장치가 내부 네트워크에서 여전히 활성 상태인 것으로 확인되었습니다. 이 장치의 요청된 삭제를 암시하는 문서도 발견되었습니다.
  - **있을 수 있는 일**(매체) - 내부 네트워크의 간단한 스캔으로 위치 장치를 정확히 찾아낼 수 있었습니다. 약간 더 많은 열거를 통해 우리는 이 장치가 레거시 소프트웨어를 실행 중이며 삭제되어야 한다는 것을 확인할 수 있었습니다.
  - **영향**(낮음) - FTP 서버에서 찾은 정보는 네트워크의 현재 구성에 따라 최신 정보가 아니므로 공격자가 사용할 수 없습니다.
  - **증거**- 이 파일은 이전 직원에 대한 정보가 포함된 FTP 서버에서 발견되었습니다.

```
Passwd for Bob
  - Make sure to do routine cleanup on his desktop after he leaves work
  - MAke sure to update his personal computer whenever he takes vacation

rvapthosting.com\bob:[redacted]

# Powershell oneliner for access bob's workstation
enter-pssession -computer 192.168.120.18 -credentials rvapthosting.com\bob
enter-pssession -computer bob.rvapthosting.com -credentials rvapthosting.com\bob

# RDP

# PSexec
```

○ **완화**- 가능하면 레거시 서버를 네트워크에서 제거하십시오. 그렇지 않은 경우 제조업체에서 출시한 최신 보안 업데이트가 있는지 확인하여 해당 장치와 관련된 위험을 최소화하십시오.

● 사용 중지된 활성 사용자 계정(CVSS 3.0)

○ **설명**- 테스트 결과 삭제 예정인 것으로 보였지만 삭제되지 않은 활성 사용자 계정이 나타났습니다.

○ **가능성**(매체) - 이러한 계정에 대한 정보는 해당 계정이 상주하는 시스템을 손상시킨 후에만 사용할 수 있습니다. 즉, 공격자는 이전 사용자 계정이 활성화되어 있는지 확인하기 위해 시스템에 액세스해야 합니다.

○ **영향**(낮음) - 이전 계정은 각 시스템에 대한 권한 수준이 매우 낮았으므로 손상되더라도 네트워크에 치명적일 수 있는 리소스에 대한 액세스가 제한되었습니다.

○ **증거**-도메인 컨트롤러(192.168.120.1)의 각 사용자 계정을 면밀히 조사한 후 이전 사용자 계정에서 이전 계정을 제거하려는 의도를 표현하는 댓글이 발견되었습니다.

"논평 FFS 이 친구는 8년 동안 은퇴했습니다. 조쉬, 그를 치워버려. -단발"

○ **완화**-이전 사용자 계정은 삭제하지 않으면 최소한 비활성화해야 합니다. 이것은 불만을 품은 직원이나 오래된 자격 증명과 관련된 모든 종류의 위험을 제거합니다.