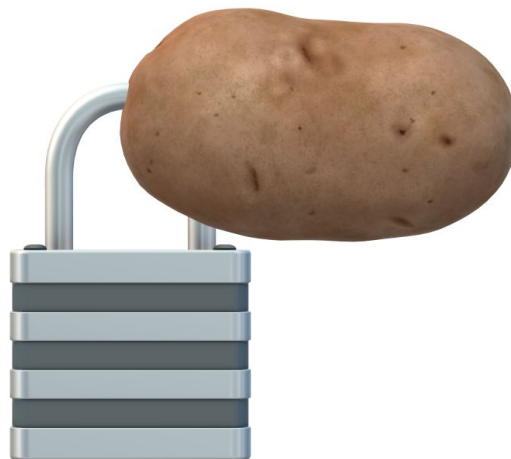


Starch Consulting



인프라 침투 테스트 RVAPTHosting

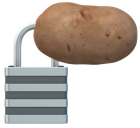
2020년 4월 22일

의해서 준비되었다:

제이콥 루드
에매뉴얼 아데웰
오마르 알잘라우드
압둘말리크 바나세르

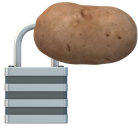
발표자:

밥 디노
조 뱅크
존 도우



목차

목차	2
부인 성명	삼
요약	삼
경영개요	4
토폴로지	5
참여 일정(2020년 4월 6-16일) 위험 수준 방법	6
론	6
권장 완화 계획	7
기술적 위험	8
우선 순위가 높은 위험	8
기본 자격 증명(CVSS 9.0) 손상된 클라이언트 정보	8
(CVSS 10.0) 중간 우선 순위 위험	9
	10
일반 텍스트 암호 저장소(CVSS 5.0) 암호 재	10
사용(CVSS 4.5)	11
우선 순위가 낮은 위험	11
활성 레거시 장치(CVSS 2.0) 활성 은퇴 사용자	11
계정(CVSS 3.0)	12



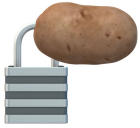
부인 성명

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.

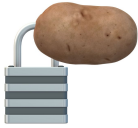


경영개요

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

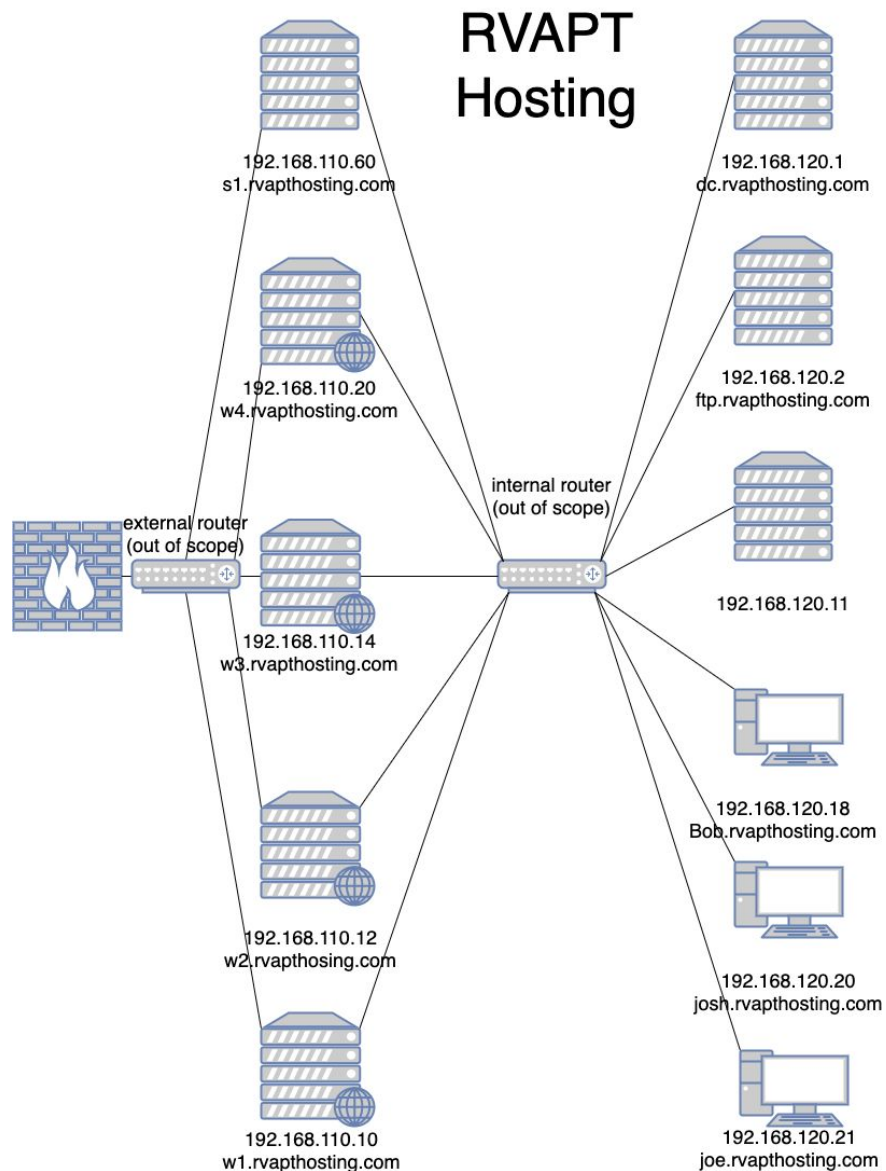
일반 텍스트 비밀번호 저장 그리고 **비밀번호 재사용**도 발견되었습니다. 이러한 결과는 **중간** 우선순위 위험. 회사는 사례별로 위험을 수정하거나 수용하기 위한 일정을 개발해야 합니다.

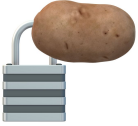
마침내 스타치컨설팅이 찾아낸 **활성 레거시 장치** 그리고 **활성 은퇴 사용자 계정** 인프라에서 사용할 수 있습니다. 이러한 결과는 **낮은** 우선순위 위험. 회사는 이러한 위험을 수용하거나 개선하기로 결정할 수 있습니다.



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

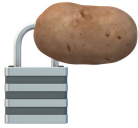
- APT 활동 발견(Joe에게 보고)

● 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			
		낮은	중간	높은
있을 수 있는 일	낮은	낮은	낮은	낮은
	중간	낮은	중간	중간
	높은	낮은	중간	높은

표 1: 위험 수준 매트릭스

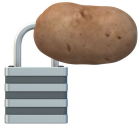
위험 등급은 다음 기본 원칙에 따라 완화 계획을 추진하는 데 도움이 됩니다.

- **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

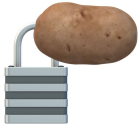
위험	있을 수 있는 일	영향	우선 사항
기본 자격 증명	높은	높은	높은
손상된 클라이언트 정보	높은	높은	높은
일반 텍스트 암호 저장	중간	높은	중간
비밀번호 재사용	높은	중간	중간
활성 레거시 장치	높은	낮은	낮은
활성 은퇴 사용자 계정	높은	낮은	낮은

표 2 - 기술적 위험

높음우선순위 위험

● 기본 자격 증명(CVSS 9.0)

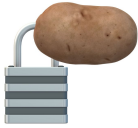
- **설명:** 중요한 서버(webmin) 중 하나에 기본 자격 증명이 있습니다. 이것은 네트워크에 대한 Starch Consulting의 초기 액세스로 이어집니다.
- **있을 수 있는 일(높음)** - 기본 암호를 사용하면 공격자가 웹 서버에서 바로 로그인하여 시스템 명령을 실행할 수 있습니다.
- **영향(높음):** 이것은 공격자가 시스템에 침입해야 할 때 침입자의 항목이 될 수 있습니다. SSH 키를 서버에 저장하여 지속성을 설정할 수 있습니다.
- **증거:** webmin의 기본 비밀번호로 로그인하면 누구나 웹 서버에 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 Rvaphositng 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 Rvaphosting에 매우 중요합니다.
- **증거:**

```
mysql> SELECT * FROM rvaptemployee
-> ;
+-----+-----+-----+-----+-----+-----+-----+
| id | first_name | last_name | password | address | employeeid | email |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | John | Doe | 123456 | 123 Main St | 1 | john.doe@starch.com |
| 2 | Jane | Smith | 123456 | 456 Main St | 2 | jane.smith@starch.com |
| 3 | Bob | Johnson | 123456 | 789 Main St | 3 | bob.johnson@starch.com |
| 4 | Alice | Brown | 123456 | 101 Main St | 4 | alice.brown@starch.com |
| 5 | Charlie | Davis | 123456 | 202 Main St | 5 | charlie.davis@starch.com |
| 6 | David | Miller | 123456 | 303 Main St | 6 | david.miller@starch.com |
| 7 | Emily | Wilson | 123456 | 404 Main St | 7 | emily.wilson@starch.com |
| 8 | Frank | Moore | 123456 | 505 Main St | 8 | frank.moore@starch.com |
| 9 | Grace | Taylor | 123456 | 606 Main St | 9 | grace.taylor@starch.com |
| 10 | Henry | Anderson | 123456 | 707 Main St | 10 | henry.anderson@starch.com |
| 11 | Irene | Thomas | 123456 | 808 Main St | 11 | irene.thomas@starch.com |
| 12 | Jack | White | 123456 | 909 Main St | 12 | jack.white@starch.com |
| 13 | Karen | Harris | 123456 | 1010 Main St | 13 | karen.harris@starch.com |
| 14 | Leo | Clark | 123456 | 1111 Main St | 14 | leo.clark@starch.com |
| 15 | Mia | Lewis | 123456 | 1212 Main St | 15 | mia.lewis@starch.com |
| 16 | Noah | King | 123456 | 1313 Main St | 16 | noah.king@starch.com |
| 17 | Olivia | Scott | 123456 | 1414 Main St | 17 | olivia.scott@starch.com |
| 18 | Peter | Green | 123456 | 1515 Main St | 18 | peter.green@starch.com |
| 19 | Quinn | Adams | 123456 | 1616 Main St | 19 | quinn.adams@starch.com |
| 20 | Ryan | Baker | 123456 | 1717 Main St | 20 | ryan.baker@starch.com |
| 21 | Sophia | Nelson | 123456 | 1818 Main St | 21 | sophia.nelson@starch.com |
| 22 | Tyler | Hill | 123456 | 1919 Main St | 22 | tyler.hill@starch.com |
| 23 | Victoria | Young | 123456 | 2020 Main St | 23 | victoria.young@starch.com |
| 24 | William | King | 123456 | 2121 Main St | 24 | william.king@starch.com |
| 25 | Zoe | Wright | 123456 | 2222 Main St | 25 | zoe.wright@starch.com |
| 26 | Adam | Lopez | 123456 | 2323 Main St | 26 | adam.lopez@starch.com |
| 27 | Bella | Hill | 123456 | 2424 Main St | 27 | bella.hill@starch.com |
| 28 | Carter | Scott | 123456 | 2525 Main St | 28 | carter.scott@starch.com |
| 29 | Daniel | King | 123456 | 2626 Main St | 29 | daniel.king@starch.com |
| 30 | Evelyn | Green | 123456 | 2727 Main St | 30 | evelyn.green@starch.com |
| 31 | Frank | Adams | 123456 | 2828 Main St | 31 | frank.adams@starch.com |
| 32 | Grace | Baker | 123456 | 2929 Main St | 32 | grace.baker@starch.com |
| 33 | Henry | Nelson | 123456 | 3030 Main St | 33 | henry.nelson@starch.com |
| 34 | Irene | Hill | 123456 | 3131 Main St | 34 | irene.hill@starch.com |
| 35 | Jack | Scott | 123456 | 3232 Main St | 35 | jack.scott@starch.com |
| 36 | Karen | King | 123456 | 3333 Main St | 36 | karen.king@starch.com |
| 37 | Leo | Green | 123456 | 3434 Main St | 37 | leo.green@starch.com |
| 38 | Mia | Adams | 123456 | 3535 Main St | 38 | mia.adams@starch.com |
| 39 | Noah | Baker | 123456 | 3636 Main St | 39 | noah.baker@starch.com |
| 40 | Olivia | Nelson | 123456 | 3737 Main St | 40 | olivia.nelson@starch.com |
| 41 | Peter | Hill | 123456 | 3838 Main St | 41 | peter.hill@starch.com |
| 42 | Quinn | Scott | 123456 | 3939 Main St | 42 | quinn.scott@starch.com |
| 43 | Ryan | King | 123456 | 4040 Main St | 43 | ryan.king@starch.com |
| 44 | Sophia | Green | 123456 | 4141 Main St | 44 | sophia.green@starch.com |
| 45 | Tyler | Adams | 123456 | 4242 Main St | 45 | tyler.adams@starch.com |
| 46 | Victoria | Baker | 123456 | 4343 Main St | 46 | victoria.baker@starch.com |
| 47 | William | Nelson | 123456 | 4444 Main St | 47 | william.nelson@starch.com |
| 48 | Zoe | Hill | 123456 | 4545 Main St | 48 | zoe.hill@starch.com |
| 49 | Adam | Scott | 123456 | 4646 Main St | 49 | adam.scott@starch.com |
| 50 | Bella | King | 123456 | 4747 Main St | 50 | bella.king@starch.com |
| 51 | Carter | Green | 123456 | 4848 Main St | 51 | carter.green@starch.com |
| 52 | Daniel | Adams | 123456 | 4949 Main St | 52 | daniel.adams@starch.com |
| 53 | Evelyn | Baker | 123456 | 5050 Main St | 53 | evelyn.baker@starch.com |
| 54 | Frank | Nelson | 123456 | 5151 Main St | 54 | frank.nelson@starch.com |
| 55 | Grace | Hill | 123456 | 5252 Main St | 55 | grace.hill@starch.com |
| 56 | Henry | Scott | 123456 | 5353 Main St | 56 | henry.scott@starch.com |
| 57 | Irene | King | 123456 | 5454 Main St | 57 | irene.king@starch.com |
| 58 | Jack | Green | 123456 | 5555 Main St | 58 | jack.green@starch.com |
| 59 | Karen | Adams | 123456 | 5656 Main St | 59 | karen.adams@starch.com |
| 60 | Leo | Baker | 123456 | 5757 Main St | 60 | leo.baker@starch.com |
| 61 | Mia | Nelson | 123456 | 5858 Main St | 61 | mia.nelson@starch.com |
| 62 | Noah | Hill | 123456 | 5959 Main St | 62 | noah.hill@starch.com |
| 63 | Olivia | Scott | 123456 | 6060 Main St | 63 | olivia.scott@starch.com |
| 64 | Peter | King | 123456 | 6161 Main St | 64 | peter.king@starch.com |
| 65 | Quinn | Green | 123456 | 6262 Main St | 65 | quinn.green@starch.com |
| 66 | Ryan | Adams | 123456 | 6363 Main St | 66 | ryan.adams@starch.com |
| 67 | Sophia | Baker | 123456 | 6464 Main St | 67 | sophia.baker@starch.com |
| 68 | Tyler | Nelson | 123456 | 6565 Main St | 68 | tyler.nelson@starch.com |
| 69 | Victoria | Hill | 123456 | 6666 Main St | 69 | victoria.hill@starch.com |
| 70 | William | Scott | 123456 | 6767 Main St | 70 | william.scott@starch.com |
| 71 | Zoe | King | 123456 | 6868 Main St | 71 | zoe.king@starch.com |
| 72 | Adam | Green | 123456 | 6969 Main St | 72 | adam.green@starch.com |
| 73 | Bella | Adams | 123456 | 7070 Main St | 73 | bella.adams@starch.com |
| 74 | Carter | Baker | 123456 | 7171 Main St | 74 | carter.baker@starch.com |
| 75 | Daniel | Nelson | 123456 | 7272 Main St | 75 | daniel.nelson@starch.com |
| 76 | Evelyn | Hill | 123456 | 7373 Main St | 76 | evelyn.hill@starch.com |
| 77 | Frank | Scott | 123456 | 7474 Main St | 77 | frank.scott@starch.com |
| 78 | Grace | King | 123456 | 7575 Main St | 78 | grace.king@starch.com |
| 79 | Henry | Green | 123456 | 7676 Main St | 79 | henry.green@starch.com |
| 80 | Irene | Adams | 123456 | 7777 Main St | 80 | irene.adams@starch.com |
| 81 | Jack | Baker | 123456 | 7878 Main St | 81 | jack.baker@starch.com |
| 82 | Karen | Nelson | 123456 | 7979 Main St | 82 | karen.nelson@starch.com |
| 83 | Leo | Hill | 123456 | 8080 Main St | 83 | leo.hill@starch.com |
| 84 | Mia | Scott | 123456 | 8181 Main St | 84 | mia.scott@starch.com |
| 85 | Noah | King | 123456 | 8282 Main St | 85 | noah.king@starch.com |
| 86 | Olivia | Green | 123456 | 8383 Main St | 86 | olivia.green@starch.com |
| 87 | Peter | Adams | 123456 | 8484 Main St | 87 | peter.adams@starch.com |
| 88 | Quinn | Baker | 123456 | 8585 Main St | 88 | quinn.baker@starch.com |
| 89 | Ryan | Nelson | 123456 | 8686 Main St | 89 | ryan.nelson@starch.com |
| 90 | Sophia | Hill | 123456 | 8787 Main St | 90 | sophia.hill@starch.com |
| 91 | Tyler | Scott | 123456 | 8888 Main St | 91 | tyler.scott@starch.com |
| 92 | Victoria | King | 123456 | 8989 Main St | 92 | victoria.king@starch.com |
| 93 | William | Green | 123456 | 9090 Main St | 93 | william.green@starch.com |
| 94 | Zoe | Adams | 123456 | 9191 Main St | 94 | zoe.adams@starch.com |
| 95 | Adam | Baker | 123456 | 9292 Main St | 95 | adam.baker@starch.com |
| 96 | Bella | Nelson | 123456 | 9393 Main St | 96 | bella.nelson@starch.com |
| 97 | Carter | Hill | 123456 | 9494 Main St | 97 | carter.hill@starch.com |
| 98 | Daniel | Scott | 123456 | 9595 Main St | 98 | daniel.scott@starch.com |
| 99 | Evelyn | King | 123456 | 9696 Main St | 99 | evelyn.king@starch.com |
| 100 | Frank | Green | 123456 | 9797 Main St | 100 | frank.green@starch.com |
| 101 | Grace | Adams | 123456 | 9898 Main St | 101 | grace.adams@starch.com |
| 102 | Henry | Baker | 123456 | 9999 Main St | 102 | henry.baker@starch.com |
| 103 | Irene | Nelson | 123456 | 10000 Main St | 103 | irene.nelson@starch.com |
| 104 | Jack | Hill | 123456 | 10101 Main St | 104 | jack.hill@starch.com |
| 105 | Karen | Scott | 123456 | 10202 Main St | 105 | karen.scott@starch.com |
| 106 | Leo | King | 123456 | 10303 Main St | 106 | leo.king@starch.com |
| 107 | Mia | Green | 123456 | 10404 Main St | 107 | mia.green@starch.com |
| 108 | Noah | Adams | 123456 | 10505 Main St | 108 | noah.adams@starch.com |
| 109 | Olivia | Baker | 123456 | 10606 Main St | 109 | olivia.baker@starch.com |
| 110 | Peter | Nelson | 123456 | 10707 Main St | 110 | peter.nelson@starch.com |
| 111 | Quinn | Hill | 123456 | 10808 Main St | 111 | quinn.hill@starch.com |
| 112 | Ryan | Scott | 123456 | 10909 Main St | 112 | ryan.scott@starch.com |
| 113 | Sophia | King | 123456 | 11010 Main St | 113 | sophia.king@starch.com |
| 114 | Tyler | Green | 123456 | 11111 Main St | 114 | tyler.green@starch.com |
| 115 | Victoria | Adams | 123456 | 11212 Main St | 115 | victoria.adams@starch.com |
| 116 | William | Baker | 123456 | 11313 Main St | 116 | william.baker@starch.com |
| 117 | Zoe | Nelson | 123456 | 11414 Main St | 117 | zoe.nelson@starch.com |
| 118 | Adam | Hill | 123456 | 11515 Main St | 118 | adam.hill@starch.com |
| 119 | Bella | Scott | 123456 | 11616 Main St | 119 | bella.scott@starch.com |
| 120 | Carter | King | 123456 | 11717 Main St | 120 | carter.king@starch.com |
| 121 | Daniel | Green | 123456 | 11818 Main St | 121 | daniel.green@starch.com |
| 122 | Evelyn | Adams | 123456 | 11919 Main St | 122 | evelyn.adams@starch.com |
| 123 | Frank | Baker | 123456 | 12020 Main St | 123 | frank.baker@starch.com |
| 124 | Grace | Nelson | 123456 | 12121 Main St | 124 | grace.nelson@starch.com |
| 125 | Henry | Hill | 123456 | 12222 Main St | 125 | henry.hill@starch.com |
| 126 | Irene | Scott | 123456 | 12323 Main St | 126 | irene.scott@starch.com |
| 127 | Jack | King | 123456 | 12424 Main St | 127 | jack.king@starch.com |
| 128 | Karen | Green | 123456 | 12525 Main St | 128 | karen.green@starch.com |
| 129 | Leo | Adams | 123456 | 12626 Main St | 129 | leo.adams@starch.com |
| 130 | Mia | Baker | 123456 | 12727 Main St | 130 | mia.baker@starch.com |
| 131 | Noah | Nelson | 123456 | 12828 Main St | 131 | noah.nelson@starch.com |
| 132 | Olivia | Hill | 123456 | 12929 Main St | 132 | olivia.hill@starch.com |
| 133 | Peter | Scott | 123456 | 13030 Main St | 133 | peter.scott@starch.com |
| 134 | Quinn | King | 123456 | 13131 Main St | 134 | quinn.king@starch.com |
| 135 | Ryan | Green | 123456 | 13232 Main St | 135 | ryan.green@starch.com |
| 136 | Sophia | Adams | 123456 | 13333 Main St | 136 | sophia.adams@starch.com |
| 137 | Tyler | Baker | 123456 | 13434 Main St | 137 | tyler.baker@starch.com |
| 138 | Victoria | Nelson | 123456 | 13535 Main St | 138 | victoria.nelson@starch.com |
| 139 | William | Hill | 123456 | 13636 Main St | 139 | william.hill@starch.com |
| 140 | Zoe | Scott | 123456 | 13737 Main St | 140 | zoe.scott@starch.com |
| 141 | Adam | King | 123456 | 13838 Main St | 141 | adam.king@starch.com |
| 142 | Bella | Green | 123456 | 13939 Main St | 142 | bella.green@starch.com |
| 143 | Carter | Adams | 123456 | 14040 Main St | 143 | carter.adams@starch.com |
| 144 | Daniel | Baker | 123456 | 14141 Main St | 144 | daniel.baker@starch.com |
| 145 | Evelyn | Nelson | 123456 | 14242 Main St | 145 | evelyn.nelson@starch.com |
| 146 | Frank | Hill | 123456 | 14343 Main St | 146 | frank.hill@starch.com |
| 147 | Grace | Scott | 123456 | 14444 Main St | 147 | grace.scott@starch.com |
| 148 | Henry | King | 123456 | 14545 Main St | 148 | henry.king@starch.com |
| 149 | Irene | Green | 123456 | 14646 Main St | 149 | irene.green@starch.com |
| 150 | Jack | Adams | 123456 | 14747 Main St | 150 | jack.adams@starch.com |
| 151 | Karen | Baker | 123456 | 14848 Main St | 151 | karen.baker@starch.com |
| 152 | Leo | Nelson | 123456 | 14949 Main St | 152 | leo.nelson@starch.com |
| 153 | Mia | Hill | 123456 | 15050 Main St | 153 | mia.hill@starch.com |
| 154 | Noah | Scott | 123456 | 15151 Main St | 154 | noah.scott@starch.com |
| 155 | Olivia | King | 123456 | 15252 Main St | 155 | olivia.king@starch.com |
| 156 | Peter | Green | 123456 | 15353 Main St | 156 | peter.green@starch.com |
| 157 | Quinn | Adams | 123456 | 15454 Main St | 157 | quinn.adams@starch.com |
| 158 | Ryan | Baker | 123456 | 15555 Main St | 158 | ryan.baker@starch.com |
| 159 | Sophia | Nelson | 123456 | 15656 Main St | 159 | sophia.nelson@starch.com |
| 160 | Tyler | Hill | 123456 | 15757 Main St | 160 | tyler.hill@starch.com |
| 161 | Victoria | Scott | 123456 | 15858 Main St | 161 | victoria.scott@starch.com |
| 162 | William | King | 123456 | 15959 Main St | 162 | william.king@starch.com |
| 163 | Zoe | Green | 123456 | 16060 Main St | 163 | zoe.green@starch.com |
| 164 | Adam | Adams | 123456 | 16161 Main St | 164 | adam.adams@starch.com |
| 165 | Bella | Baker | 123456 | 16262 Main St | 165 | bella.baker@starch.com |
| 166 | Carter | Nelson | 123456 | 16363 Main St | 166 | carter.nelson@starch.com |
| 167 | Daniel | Hill | 123456 | 16464 Main St | 167 | daniel.hill@starch.com |
| 168 | Evelyn | Scott | 123456 | 16565 Main St | 168 | evelyn.scott@starch.com |
| 169 | Frank | King | 123456 | 16666 Main St | 169 | frank.king@starch.com |
| 170 | Grace | Green | 123456 | 16767 Main St | 170 | grace.green@starch.com |
| 171 | Henry | Adams | 123456 | 16868 Main St | 171 | henry.adams@starch.com |
| 172 | Irene | Baker | 123456 | 16969 Main St | 172 | irene.baker@starch.com |
| 173 | Jack | Nelson | 123456 | 17070 Main St | 173 | jack.nelson@starch.com |
| 174 | Karen | Hill | 123456 | 17171 Main St | 174 | karen.hill@starch.com |
| 175 | Leo | Scott | 123456 | 17272 Main St | 175 | leo.scott@starch.com |
| 176 | Mia | King | 123456 | 17373 Main St | 176 | mia.king@starch.com |
| 177 | Noah | Green | 123456 | 17474 Main St | 177 | noah.green@starch.com |
| 178 | Olivia | Adams | 123456 | 17575 Main St | 178 | olivia.adams@starch.com |
| 179 | Peter | Baker | 123456 | 17676 Main St | 179 | peter.baker@starch.com |
| 180 | Quinn | Nelson | 123456 | 17777 Main St | 180 | quinn.nelson@starch.com |
| 181 | Ryan | Hill | 123456 | 17878 Main St | 181 | ryan.hill@starch.com |
| 182 | Sophia | Scott | 123456 | 17979 Main St | 182 | sophia.scott@starch.com |
| 183 | Tyler | King | 123456 | 18080 Main St | 183 | tyler.king@starch.com |
| 184 | Victoria | Green | 123456 | 18181 Main St | 184 | victoria.green@starch.com |
| 185 | William | Adams | 123456 | 18282 Main St | 185 | william.adams@starch.com |
| 186 | Zoe | Baker | 123456 | 18383 Main St | 186 | zoe.baker@starch.com |
| 187 | Adam | Nelson | 123456 | 18484 Main St | 187 | adam.nelson@starch.com |
| 188 | Bella | Hill | 123456 | 18585 Main St | 188 | bella.hill@starch.com |
| 189 | Carter | Scott | 123456 | 18686 Main St | 189 | carter.scott@starch.com |
| 190 | Daniel | King | 123456 | 18787 Main St | 190 | daniel.king@starch.com |
| 191 | Evelyn | Green | 123456 | 18888 Main St | 191 | evelyn.green@starch.com |
| 192 | Frank | Adams | 123456 | 18989 Main St | 192 | frank.adams@starch.com |
| 193 | Grace | Baker | 123456 | 19090 Main St | 193 | grace.baker@starch.com |
| 194 | Henry | Nelson | 123456 | 19191 Main St | 194 | henry.nelson@starch.com |
| 195 | Irene | Hill | 123456 | 19292 Main St | 195 | irene.hill@starch.com |
| 196 | Jack | Scott | 123456 | 19393 Main St | 196 | jack.scott@starch.com |
| 197 | Karen | King | 123456 | 19494 Main St | 197 | karen.king@starch.com |
| 198 | Leo | Green | 123456 | 19595 Main St | 198 | leo.green@starch.com |
| 199 | Mia | Adams | 123456 | 19696 Main St | 199 | mia.adams@starch.com |
| 200 | Noah | Baker | 123456 | 19797 Main St | 200 | noah.baker@starch.com |
| 201 | Olivia | Nelson | 123456 | 19898 Main St | 201 | olivia.nelson@starch.com |
| 202 | Peter | Hill | 123456 | 19999 Main St | 202 | peter.hill@starch.com |
| 203 | Quinn | Scott | 123456 | 20000 Main St | 203 | quinn.scott@starch.com |
| 204 | Ryan | King | 123456 | 20101 Main St | 204 | ryan.king@starch.com |
| 205 | Sophia | Green | 123456 | 20202 Main St | 205 | sophia.green@starch.com |
| 206 | Tyler | Adams | 123456 | 20303 Main St | 206 | tyler.adams@starch.com |
| 207 | Victoria | Baker | 123456 | 20404 Main St | 207 | victoria.baker@starch.com |
| 208 | William | Nelson | 123456 | 20505 Main St | 208 | william.nelson@starch.com |
| 209 | Zoe | Hill | 123456 | 20606 Main St | 209 | zoe.hill@starch.com |
| 210 | Adam | Scott | 123456 | 20707 Main St | 210 | adam.scott@starch.com |
| 211 | Bella | King | 123456 | 20808 Main St | 211 | bella.king@starch.com |
| 212 | Carter | Green | 123456 | 20909 Main St | 212 | carter.green@starch.com |
| 213 | Daniel | Adams | 123456 | 21010 Main St | 213 | daniel.adams@starch.com |
| 214 | Evelyn | Baker | 123456 | 21111 Main St | 214 | evelyn.baker@starch.com |
| 215 | Frank | Nelson | 123456 | 21212 Main St | 215 | frank.nelson@starch.com |
| 216 | Grace | Hill | 123456 | 21313 Main St | 216 | grace.hill@starch.com |
| 217 | Henry | Scott | 123456 | 21414 Main St | 217 | henry.scott@starch.com |
| 218 | Irene | King | 123456 | 21515 Main St | 218 | irene.king@starch.com |
| 219 | Jack | Green | 123456 | 21616 Main St | 219 | jack.green@starch.com |
| 220 | Karen | Adams | 123456 | 21717 Main St | 220 | karen.adams@starch.com |
| 221 | Leo | Baker | 123456 | 21818 Main St | 221 | leo.baker@starch.com |
| 222 | Mia | Nelson | 123456 | 21919 Main St | 222 | mia.nelson@starch.com |
| 223 | Noah | Hill | 123456 | 22020 Main St | 223 | noah.hill@starch.com |
| 224 | Olivia | Scott | 123456 | 22121 Main St | 224 | olivia.scott@starch.com |
| 225 | Peter | King | 123456 | 22222 Main St | 225 | peter.king@starch.com |
| 226 | Quinn | Green | 123456 | 22323 Main St | 226 | quinn.green@starch.com |
| 227 | Ryan | Adams | 123456 | 22424 Main St | 227 | ryan.adams@starch.com |
| 228 | Sophia | Baker | 123456 | 22525 Main St | 228 | sophia.baker@starch.com |
| 229 | Tyler | Nelson | 123456 | 22626 Main St | 229 | tyler.nelson@starch.com |
| 230 | Victoria | Hill | 123456 | 22727 Main St | 230 | victoria.hill@starch.com |
| 231 | William | Scott | 123456 | 22828 Main St | 231 | william.scott@starch.com |
| 232 | Zoe | King | 123456 | 22929 Main St | 232 | zoe.king@starch.com |
| 233 | Adam | Green | 123456 | 23030 Main St | 233 | adam.green@starch.com |
| 234 | Bella | Adams | 123456 | 23131 Main St | 234 | bella.adams@starch.com |
| 235 | Carter | Baker | 123456 | 23232 Main St | 235 | carter.baker@starch.com |
| 236 | Daniel | Nelson | 123456 | 23333 Main St | 236 | daniel.nelson@starch.com |
| 237 | Evelyn | Hill | 123456 | 23434 Main St | 237 | evelyn.hill@starch.com |
| 238 | Frank | Scott | 123456 | 23535 Main St | 238 | frank.scott@starch.com |
| 239 | Grace | King | 123456 | 23636 Main St | 239 | grace.king@starch.com |
| 240 | Henry | Green | 123456 | 23737 Main St | 240 | henry.green@starch.com |
| 241 | Irene | Adams | 123456 | 23838 Main St | 241 | irene.adams@starch.com |
| 242 | Jack | Baker | 123456 | 23939 Main St | 242 | jack.baker@starch.com |
| 243 | Karen | Nelson | 123456 | 24040 Main St | 243 | karen.nelson@starch.com |
| 244 | Leo | Hill | 123456 | 24141 Main St | 244 | leo.hill@starch.com |
| 245 | Mia | Scott | 123456 | 24242 Main St | 245 | mia.scott@starch.com |
| 246 | Noah | King | 123456 | 24343 Main St | 246 | noah.king@starch.com |
| 247 | Olivia | Green | 123456 | 24444 Main St | 247 | olivia.green@starch.com |
| 248 | Peter | Adams | 123456 | 24545 Main St | 248 | peter.adams@starch.com |
| 249 | Quinn | Baker | 123456 | 24646 Main St | 249 | quinn.baker@starch.com |
| 250 | Ryan | Nelson | 123456 | 24747 Main St | 250 | ryan.nelson@starch.com |
| 251 | Sophia | Hill | 123456 | 24848 Main St | 251 | sophia.hill@starch.com |
| 252 | Tyler | Scott | 123456 | 24949 Main St | 252 | tyler.scott@starch.com |
| 253 | Victoria | King | 123456 | 25050 Main St | 253 | victoria.king@starch.com |
| 254 | William | Green | 123456 | 25151 Main St | 254 | william.green@starch.com |
| 255 | Zoe | Adams | 123456 | 25252 Main St | 255 | zoe.adams@starch.com |
| 256 | Adam | Baker | 123456 | 25353 Main St | 256 | adam.baker@starch.com |
| 257 | Bella | Nelson | 123456 | 25454 Main St | 257 | bella.nelson@starch.com |
| 258 | Carter | Hill | 123456 | 25555 Main St | 258 | carter.hill@starch.com |
| 259 | Daniel | Scott | 123456 | 25656 Main St | 259 | daniel.scott@starch.com |
| 260 | Evelyn | King | 123456 | 25757 Main St | 260 | evelyn.king@starch.com |
| 261 | Frank | Green | 123456 | 25858 Main St | 261 | frank.green@starch.com |
| 262 | Grace | Adams | 123456 | 25959 Main St | 262 | grace.adams@starch.com |
| 263 | Henry | Baker | 123456 | 26060 Main St | 263 | henry.baker@starch.com |
| 264 | Irene | Nelson | 123456 | 26161 Main St | 264 | irene.nelson@starch.com |
| 265 | Jack | Hill | 123456 | 26262 Main St | 265 | jack.hill@starch.com |
| 266 | Karen | Scott | 123456 | 26363 Main St | 266 | karen.scott@starch.com |
| 267 | Leo | King | 123456 | 26464 Main St | 267 | leo.king@starch.com |
| 268 | Mia | Green | 123456 | 26565 Main St | 268 | mia.green@starch.com |
| 269 | Noah | Adams | 123456 | 26666 Main St | 269 | noah.adams@starch.com |
| 270 | Olivia | Baker | 123456 | 26767 Main St | 270 | olivia.baker@starch.com |
| 271 | Peter | Nelson | 123456 | 26868 Main St | 271 | peter.nelson@starch.com |
| 272 | Quinn | Hill | 123456 | 26969 Main St | 272 | quinn.hill@starch.com |
| 273 | Ryan | Scott | 123456 | 27070 Main St | 273 | ryan.scott@starch.com |
| 274 | Sophia | King | 123456 | 27171 Main St | 274 | sophia.king@starch.com |
| 275 | Tyler | Green | 123456 | 27272 Main St | 275 | tyler.green@starch.com |
| 276 | Victoria | Adams | 123456 | 27373 Main St | 276 | victoria.adams@starch.com |
| 277 | William | Baker | 123456 | 27474 Main St | 277 | william.baker@starch.com |
| 278 | Zoe | Nelson | 123456 | 27575 Main St | 278 | zoe.nelson@starch.com |
| 279 | Adam | Hill | 123456 | 27676 Main St | 279 | adam.hill@starch.com |
| 280 | Bella | Scott | 123456 | 27777 Main St | 280 | bella.scott@starch.com |
| 281 | Carter | King | 123456 | 27878 Main St | 281 | carter.king@starch.com |
| 282 | Daniel | Green | 123456 | 27979 Main St | 282 | daniel.green@starch.com |
| 283 | Evelyn | Adams | 123456 | 28080 Main St | 283 | evelyn.adams@starch.com |
| 284 | Frank | Baker | 123456 | 28181 Main St | 284 | frank.baker@starch.com |
| 285 | Grace | Nelson | 123456 | 28282 Main St | 285 | grace.nelson@starch.com |
| 286 | Henry | Hill | 123456 | 28383 Main St | 286 | henry.hill@starch.com |
| 287 | Irene | Scott | 123456 | 28484 Main St | 287 | irene.scott@starch.com |
| 288 | Jack | King | 123456 | 28585 Main St | 288 | jack.king@starch.com |
| 289 | Karen | Green | 123456 | 28686 Main St | 289 | karen.green@starch.com |
| 290 | Leo | Adams | 123456 | 28787 Main St | 290 | leo.adams@starch.com |
| 291 | Mia | Baker | 123456 | 28888 Main St | 291 | mia.baker@starch.com |
| 292 | Noah | Nelson | 123456 | 28989 Main St | 292 | noah.nelson@starch.com |
| 293 | Olivia | Hill | 123456 | 29090 Main St | 293 | olivia.hill@starch.com |
| 294 | Peter | Scott | 123456 | 29191 Main St | 294 | peter.scott@starch.com |
| 295 | Quinn | King | 123456 | 29292 Main St | 295 | quinn.king@starch.com |
| 296 | Ryan | Green | 123456 | 29393 Main St | 
```



매체 우선순위 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:
- for the old ftp server
*Evil-WinRM* PS C:\>

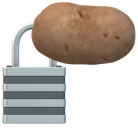
```

```

[admin@sl internal]# ls
reverse ssh.txt
[admin@sl internal]# cat reverse ssh.txt
rvapthosting.com\josh:
[Our domain - rvapthosting.com]
[My comp]
192.168.120.20:22
[admin@sl internal]#

```

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



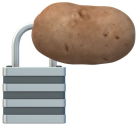
● 비밀번호 재사용(CVSS 4.5)

- **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 사용자에게 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.