

# Assignment 4

Name :Kambala Raj Kumar

College :Dr.Lankapalli Bullayya College

Regd.No :721128805335

Date :01/03/2024

## Step-1: Case Study Analysis -

- The recent cyber attack on XYZ Corporation exemplified the effectiveness of social engineering tactics in breaching security measures. The attackers initiated the breach by orchestrating a targeted phishing campaign, leveraging deceptive emails to manipulate unsuspecting employees into divulging sensitive information or unwittingly granting access to internal systems. This social engineering approach exploited human psychology and trust dynamics within the organisation, circumventing traditional security defences.
- Several vulnerabilities within XYZ Corporation's security posture were exposed during the attack. Primarily, the lack of comprehensive employee awareness training left staff ill-equipped to recognize and respond to phishing attempts effectively. Without proper education on identifying suspicious emails and following established security protocols, employees inadvertently became the weakest link in the organisation's defence.
- Furthermore, inadequate authentication measures exacerbated the breach. Weak password policies, the absence of multi-factor authentication, and lax access controls facilitated unauthorised access once the attackers breached initial defenses. This lack of robust authentication mechanisms allowed the attackers to move laterally within the network, escalating the severity of the breach.
- Moreover, poor email security protocols played a pivotal role in the success of the attack. Insufficient filtering mechanisms failed to adequately detect and block malicious emails, enabling them to reach employees' inboxes unhindered. The absence of comprehensive email security solutions, including threat intelligence and regular security assessments, left the organisation vulnerable to phishing and other email-based threats.

The consequences of the attack on XYZ Corporation were profound and far-reaching. The organisation's reputation suffered a significant blow as news of the breach spread, eroding customer trust and confidence in its ability to safeguard sensitive data.

Additionally, XYZ Corporation faced potential legal and regulatory repercussions, further exacerbating the financial and reputational impact of the breach. In conclusion, the cyber attack on XYZ Corporation underscored the critical importance of addressing vulnerabilities such as lack of employee awareness training, inadequate authentication measures, and poor email security protocols. Organisations must prioritise cybersecurity education, implement robust authentication mechanisms, and deploy comprehensive email security solutions to mitigate the risk of falling victim to social engineering attacks and the ensuing consequences on reputation, finances, and customer trust.

- **To enhance XYZ Corporation's cybersecurity posture and mitigate the risk of future social engineering attacks, the following recommendations should be considered:**
  1. **Regular Security Training for Employees:** Implement comprehensive and ongoing security awareness training programs for all employees. Training sessions should cover topics such as identifying phishing emails, recognizing social engineering tactics, and following established security protocols. Employees should be regularly updated on emerging threats and best practices to ensure they remain vigilant against evolving attack vectors.
  2. **Adopt Multi-Factor Authentication (MFA):** Implement multi-factor authentication across all systems and applications to add an extra layer of security beyond passwords. MFA requires users to verify their identity using additional factors such as SMS codes, biometrics, or hardware tokens, significantly reducing the risk of unauthorised access, even if passwords are compromised.
  3. **Improve Email Filtering Systems:** Enhance email filtering systems to better detect and block malicious emails before they reach employees' inboxes. Utilise advanced threat detection techniques, such as machine learning algorithms and real-time threat intelligence feeds, to identify and quarantine suspicious emails effectively. Regularly update and fine-tune filtering rules to adapt to emerging threats and minimise false positives.
  4. **Implement Security Incident Response Plan:** Develop and implement a robust security incident response plan to effectively detect, contain, and mitigate the impact of future cyber attacks. Define clear procedures for responding to security incidents, including escalation paths, communication protocols, and coordination with internal teams and external stakeholders. Regularly test and update the incident response plan to ensure readiness in the event of a breach.
  5. **Conduct Regular Security Assessments:** Perform regular security assessments, including vulnerability scanning and penetration testing, to identify and address potential security weaknesses proactively. Regular assessments help identify gaps in security controls, validate the effectiveness of existing security measures, and prioritise remediation efforts based on risk exposure.
  6. **Enhance Employee Reporting Mechanisms:** Encourage employees to report suspicious emails or security incidents promptly through established channels. Provide clear instructions on how to report incidents and ensure confidentiality and non-retaliation policies are in place to promote a culture of transparency and accountability.
  7. **Partner with Third-Party Security Experts:** Collaborate with reputable cybersecurity firms or consultants to augment internal expertise and resources. Engage third-party experts to conduct independent security assessments, provide specialised training, and offer strategic guidance on improving overall cybersecurity posture.

By implementing these recommendations, XYZ Corporation can strengthen its defenses against social engineering attacks, reduce the likelihood of successful breaches, and safeguard its reputation, finances, and customer trust. Ongoing vigilance, proactive measures, and a commitment to continuous improvement are essential to effectively mitigate the evolving threat landscape posed by social engineering tactics.

## Step-2: Role-play Exercise-

### Characters:

1. **Raju - The Ethical Hacker**
2. **Shiva - Friend 1 (Victim of the Attack)**
3. **Ramesh - Friend 2**
4. **Ram - Friend 3**

**Setting:** Raju's living room, where the friends often gather to hang out.

- 
- **Raju:** (serious) Hey guys, I have something important to discuss. Shiva, do you remember that suspicious email you received last week?
  - **Shiva:** (hesitant) Yeah, I remember. I thought it was just a regular email from my bank, but it turned out to be a scam, right?
  - **Raju:** (nodding) Exactly. That was a social engineering attack, and unfortunately, you fell victim to it.
  - **Ramesh:** (concerned) Wait, what happened exactly?
  - **Raju:** Well, the attacker impersonated your bank and sent you an email claiming there was an issue with your account. They asked you to click on a link and enter your credentials to resolve the issue.
  - **Shiva:** (realising) Oh no, I did click on that link and entered my details. I didn't think twice because it looked so convincing.
  - **Ram:** (surprised) But how did they get your email in the first place?
  - **Raju:** Social engineering attackers often gather information from various sources, like social media or leaked databases, to craft convincing messages tailored to their targets.
  - **Shiva:** (regretful) I should have been more cautious. Now, what should I do?
  - **Raju:** First, change your passwords immediately and notify your bank about the incident. Then, be more vigilant about emails asking for personal information. Always verify the sender's identity before responding or clicking on any links.
  - **Ramesh:** (thoughtfully) So, it's not just about having strong passwords, but also about being aware of potential threats and staying alert.
  - **Raju:** Exactly, Ramesh. Social engineering attacks exploit human psychology and trust, so it's essential to remain sceptical and verify everything, especially when it involves sensitive information.
  - **Shiva:** (grateful) Thanks, Raju. I'll definitely be more careful from now on.
  - **Ram:** (supportive) Yeah, we've got your back, Shiva. And Raju, thanks for the heads up. It's eye-opening to see how easily someone can fall for these tricks. (Raju nods, glad to have helped his friends understand the importance of cybersecurity and staying vigilant against social engineering attacks.)
-

**In this role play, Raju educates his friends about the social engineering attack that targeted Shiva, highlighting the importance of awareness, scepticism, and verification when dealing with suspicious messages or requests for personal information.**

- 1. Identifying Social Engineering Tactics:** In the role-play scenario, students should be able to recognize common social engineering tactics such as authority exploitation (posing as someone in a position of power or trust), urgency (creating a sense of time pressure to bypass scepticism), and familiarity (establishing a false sense of trust by appearing to know the victim personally or professionally).
- 2. Analysing Victim Susceptibility:** After the role-play, students should discuss why the victim fell for the social engineering tactics employed by the attacker. This could involve factors such as lack of scepticism, failure to verify the request, or insufficient awareness of potential risks.
- 3. Emphasising Scepticism and Verification:** It's crucial to emphasise the importance of scepticism and verification in all communications, especially when dealing with sensitive information or requests. Encouraging individuals to question unexpected requests, verify the identities of those making them, and confirm the legitimacy of any urgent situations can significantly reduce the likelihood of falling victim to social engineering attacks.
- 4. Strategies to Mitigate Attacks:** Implementing strict verification protocols for sensitive information requests is one effective strategy. This might involve requiring multiple layers of authentication or using encrypted communication channels for sensitive data. Additionally, fostering a culture of security awareness within the organisation can help employees recognize and respond appropriately to potential threats. This can include regular training sessions, simulated phishing exercises, and clear communication about security policies and procedures.

**By discussing these points and actively implementing strategies to mitigate social engineering attacks, organisations can significantly enhance their overall security posture and reduce the risk of falling victim to malicious actors.**

### **Step-3: Phishing Email Analysis:**

- 1. Identifying Red Flags:** In addition to misspelt domain names, urgent language, requests for sensitive information, and generic greetings, students should also be aware of other suspicious signs in emails, such as unexpected attachments or links, unusual sender addresses, and requests for confidential information that should not be shared via email.
- 2. Exploring Psychological Factors:** It's important to discuss how psychological factors like curiosity, fear, or urgency can override rational thinking and lead individuals to overlook red flags. For example, a sense of urgency might prompt someone to respond quickly without verifying the legitimacy of a request, while curiosity could drive them to click on a suspicious link out of curiosity about its contents.
- 3. Preventive Measures:** Strategies for email authentication play a key role in preventing phishing attacks. Students should learn how to check email headers to verify the origin of an email and identify any signs of spoofing or manipulation. They

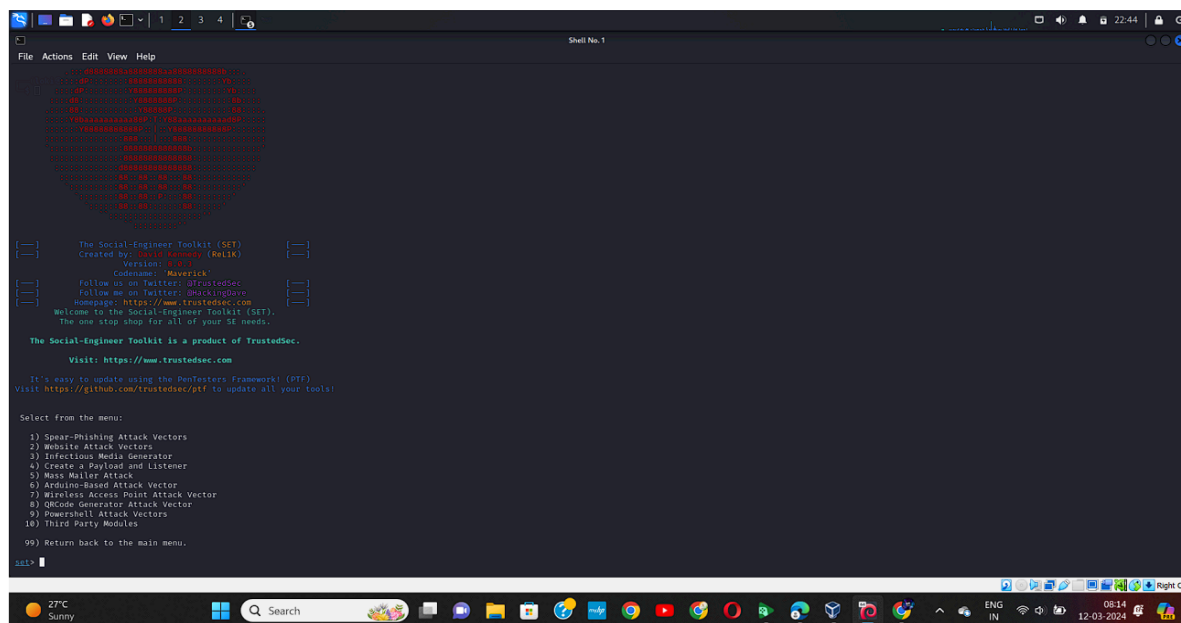
should also be taught to verify sender identities by cross-referencing email addresses with known contacts or official sources.

4. **Additional Preventive Measures:** Alongside email authentication, students should be aware of other preventive measures, such as enabling multi-factor authentication (MFA) for email accounts, using email filtering systems to detect and block phishing attempts, and implementing employee training programs to raise awareness about phishing tactics and how to respond to them appropriately.

**By combining awareness of red flags, understanding psychological factors, and implementing robust preventive measures like email authentication, organisations can significantly reduce their susceptibility to phishing attacks and safeguard their sensitive information and systems.**

## Step -4: Documenting the Exploit Process-

- First we have to open the virtual box to run the kali linux.
- After running the kali linux, find the terminal and give the command “ setoolkit “ to start the social engineering attack.
- After that find the social engineering tool kit in the kali linux search bar.



```
File Actions Edit View Help
Shell No. 1

.....
setoolkit
.....
The Social-Engineer Toolkit (SET)
Created By: TrustedSec (Rul1k)
Version: 4.0.1
Codename: Maverick
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @mackingdove
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SI needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set>
```

**And then select the first option to ensure the social-engineering attacks.**

```
Shell No.1
/home/loki
File Actions Edit View Help

[Logo]
[+] The Social-Engineer Toolkit (SET)
[+] Created by: David Kennedy (ReL1K)
[+] Version: 8.0.3
[+] Codename: 'Maverick'
[+] Follow us on Twitter: @TrustedSec
[+] Follow us on Twitter: @BlackingDove
[+] Homepage: https://www.trustedsec.com
[+] Welcome to the Social-Engineer Toolkit (SET).
[+] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

- Select the second option for the website attack vectors.

```
root@loki: /home/loki
Text Editor
Simple Text Editor - hp

[Logo]
[+] Social-Engineer Toolkit
[+] Free
[+] Bugs
[+] By: TrustedSec
[+] https://www.trustedsec.com

[+] [Logo] Social-Engineer Toolkit (SET)
[+] Created by: David Kennedy (ReL1K)
[+] Version: 8.0.3
[+] Codename: 'Maverick'
[+] Follow us on Twitter: @TrustedSec
[+] Follow us on Twitter: @BlackingDove
[+] Homepage: https://www.trustedsec.com
[+] Welcome to the Social-Engineer Toolkit (SET).
[+] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit: https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

- Select the third option for the credential harvester attack method.

```
root@kali: ~/home/loki
99) Return to Main Menu
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, engent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web-Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
```

- Then select the second option site cloner.

```
root@kali: ~/home/loki
99) Return to Main Menu
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, engent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web-Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
```

- Then give the ip address to port forwarding to the NAT ip address.

```
Shell No. 1
Simple Text Editor - IP
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] To harvest credentials or parameters from a website as well as place them into a report
*** IMPORTANT *** READ THIS BEFORE ENTERING IN THE IP ADDRESS *** IMPORTANT ***
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.177.221]: 192.168.177.221
**** Important Information ****
For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/settoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then
```

- A screenshot of a web browser displaying the Google Account sign-in page. The browser's address bar shows the URL "192.168.177.221" and a "Not secure" warning. The page features the Google logo at the top, followed by the text "Sign in with your Google Account". Below this is a large, light gray rectangular box containing a circular profile picture placeholder, an "Email" input field, a password input field with masked characters, and a blue "Sign in" button. A link for "Need help?" is positioned below the sign-in button. At the bottom of the box is a link to "Create an account". Below the box, the text "One Google Account for everything Google" is displayed, followed by a row of icons for various Google services. The browser's status bar at the bottom shows the Google logo, links for "Privacy" and "Terms", and a language selector set to "English (United States)". The Windows taskbar at the very bottom displays the system clock as 18:29 on 13-03-2024, along with weather information (29°C, Partly cloudy) and several application icons.

- ```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000
```

This process make me a expert to make a cloning attack because i just did this process for several times to get a better result.