السلام عليكم..... نحن مجموعة من طلاب الامن السيبراني مستوى ثالث جامعة السعيدة قمنا بعمل اداءه اسمها Gemini تقوم بأكثر من عمل سوف نتكلم عنها فيما بعد.

- المهندسين الذين قام بعمل هذي الأداء:

١- م/محمد سعيد يسر

٢- م/مساعد عبد الحكيم المخلافي

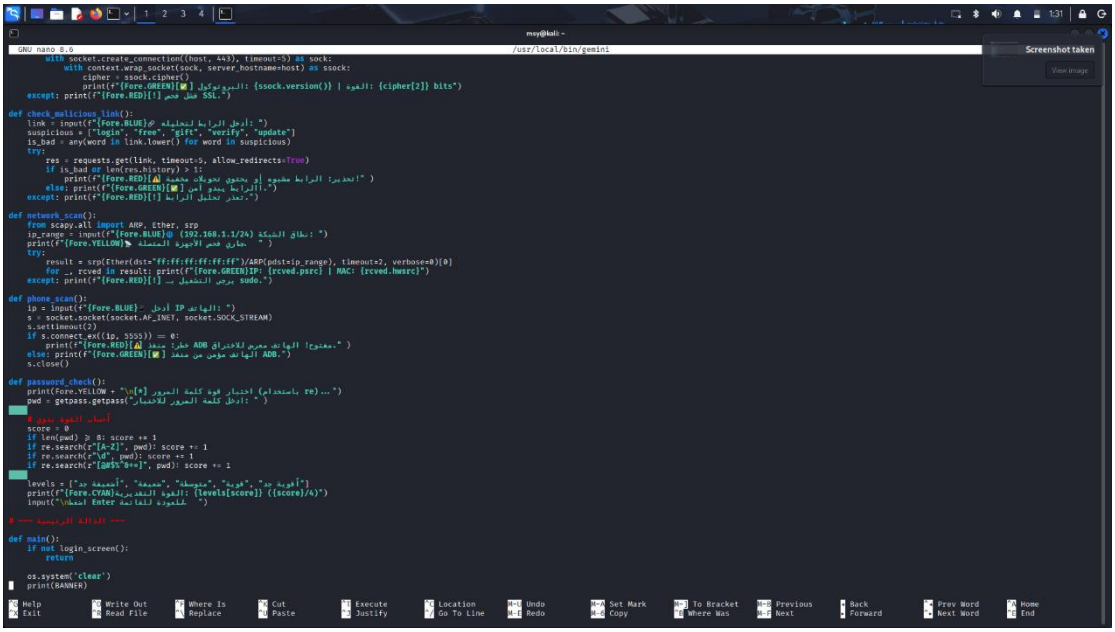
٣- م/الياس منصور مأمون

٤- م/ايمن غالب الفضل

تحت اشراف الدكتور الفاضل / عادل معوضه

اداءة Geminiهي بلغة python تقوم بالعمل في نظام kali

صور توضيحية ل كود الأداء



الكود يشمل مكاتب ودوال لكل اداءه

- واجهة الأداء

نقوم بكتابة كلمة المرور ل الدخول.

اول ما تعرض لك الاداءة تقوم بالترحيب بك صوتياً

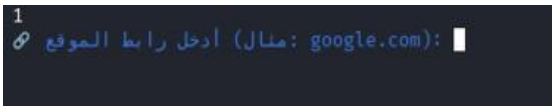
وتعرض لك المهام التي تقوم بها وكل اداءه مربوطة برقم

```
# ترحيب صوتي عند الدخول الناجح
speak("Access granted. Welcome back commander. How can I help you today?")

print(f"{Fore.GREEN}مرحباً بك في أداة الفحص الذكية!")
print(f"{Fore.WHITE}أنا مساعدك الأمني، جاهز لتنفيذ المهام المطلوبة.\n")
```

اداءه Geminiتجمع بين ٦ أدوات تعمل كل أداة بعمل خاص بها سوف اشرح كل أداء على حدا.

١-



هذي الاداءه نقوم بإدخال رابط الموقع وهي توم بفحصة ان الموقع مومان ولا يوجد به ثغرات.

```
def web_scan():
    url = input(f"{Fore.BLUE}🔗 أدخل رابط الموقع (مثال: google.com): ")
    if not url.startswith('http'): url = 'https://' + url
    print(f"{Fore.YELLOW}🔍 جاري فحص الرؤوس الأمنية لـ {url}...")
    try:
        r = requests.get(url, timeout=5)
        headers = {"X-Frame-Options": "Clickjacking", "Content-Security-Policy": "XSS", "X-Content-Type-Options": "Sniffing"}
        for h, desc in headers.items():
            status = f"{Fore.GREEN}[✅] مؤمن" if h in r.headers else f"{Fore.RED}[❌] معرض لثغرة {desc}"
            print(f"{h}: {status}")
    except: print(f"{Fore.RED}[!] تعذر الوصول للموقع.")
```

٢-

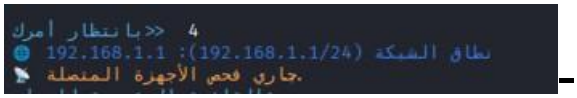
نقوم بإدخال رابط الموقع من اجل تحليل نوع وقوة التشفير المستخدم في الموقع.

```
def check_ssl():
    host = input(f"{Fore.BLUE}🛡️ أدخل الدومين لفحص التشفير: ")
    if "://" in host: host = urlparse(host).netloc
    try:
        context = ssl.create_default_context()
        with socket.create_connection((host, 443), timeout=5) as sock:
            with context.wrap_socket(sock, server_hostname=host) as ssock:
                cipher = ssock.cipher()
                print(f"{Fore.GREEN}[✅] البروتوكول: {ssock.version()} | القوة: {cipher[2]} bits")
    except: print(f"{Fore.RED}[!] فشل فحص SSL.")
```

٣-

هذي الأداء تقوم بفحص الروابط هل هي محمية ولا ملغمة بكود خبيث.

```
def check_malicious_link():
    link = input(f"{Fore.BLUE}🔗 أدخل الرابط لتحليله: ")
    suspicious = ["login", "free", "gift", "verify", "update"]
    is_bad = any(word in link.lower() for word in suspicious)
    try:
        res = requests.get(link, timeout=5, allow_redirects=True)
        if is_bad or len(res.history) > 1:
            print(f"{Fore.RED}[⚠] تحذير: الرابط مشبوه أو يحتوي تحويلات مخفية!")
        else: print(f"{Fore.GREEN}[✅] الرابط يبدو آمناً.")
    except: print(f"{Fore.RED}[!] تعذر تحليل الرابط.")
```



٤-

تقوم بفحص الأجهزة المتصلة بهذي الشبكة.

```
def network_scan():
    from scapy.all import ARP, Ether, srp
    ip_range = input(f"{Fore.BLUE}🌐 نطاق الشبكة (192.168.1.1/24): ")
    print(f"{Fore.YELLOW}📡 جاري فحص الأجهزة المتصلة...")
    try:
        result = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=ip_range), timeout=2, verbose=0)[0]
        for _, rcved in result: print(f"{Fore.GREEN}IP: {rcved.psrc} | MAC: {rcved.hwsrc}")
    except: print(f"{Fore.RED}[!] يرجى التشغيل بـ sudo.")
```

٥-

هذي الأداة تقوم بفحص الهاتف هل مومن ولا قد تم اختراقة.

```
def phone_scan():
    ip = input(f"{Fore.BLUE}📱 أدخل IP الهاتف: ")
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2)
    if s.connect_ex((ip, 5555)) == 0:
        print(f"{Fore.RED}[⚠] خطر: منفذ ADB مفتوح! الهاتف معرض للاختراق.")
    else: print(f"{Fore.GREEN}[✅] الهاتف مؤمن من منفذ ADB.")
    s.close()
```

```
باانتظار أمرك>> 6

[*] اختبار قوة كلمة المرور (باستخدام re)...
ادخل كلمة المرور للاختبار:
القوة التقديرية: متوسطة (2/4)
```

٦-

هذي الاداءة تقوم بفحص كلمة المرور هل هيا قوية ولا ضعيفة .

```python
def password_check():
    print(Fore.YELLOW + "\n[*] اختبار قوة كلمة المرور (باستخدام re)...")
    pwd = getpass.getpass("ادخل كلمة المرور للاختبار: ")

    # حساب القوة يدوياً
    score = 0
    if len(pwd) >= 8: score += 1
    if re.search(r"[A-Z]", pwd): score += 1
    if re.search(r"\d", pwd): score += 1
    if re.search(r"[@#$%^&+=]", pwd): score += 1

    levels = ["ضعيفة جداً", "ضعيفة", "متوسطة", "قوية", "قوية جداً"]
    print(f"{Fore.CYAN}القوة التقديرية: {levels[score]} ({score}/4)")
    input("\nاضغط Enter للعودة للقائمة...")
```