IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15575

Controlling Ethical Hacking: Operating System Security

Dipali Girhe[1], R.V. Daund[2]

Student, Department of Computer Science, KTHM College, Nashik, Maharashtra, India[1]

Assistant Professor, Department of Computer Science, KTHM College, Nashik, Maharashtra, India[2]

Abstract: The rapid advancement of technology has increased the risk of cyberAttacks, making ethical hacking a critical tool for securing information systems. Ethical hacking involves authorized testing of computer systems to identify vulnerabilities before malicious hackers exploit them. This research focuses on controlling ethical hacking through the use of operating systems such as Windows, Kali Linux, and Linux-based security distributions. Data is collected from secondary sources, including journals, research papers, official OS documentation, and cyber security reports, to analyse hacking tools, techniques, and OS-level security features. The study highlights how operating systems provide built-in protections, access controls, logging, auditing, and monitoring mechanisms that can prevent unauthorized access while enabling safe ethical hacking. Additionally, the research explores emerging trends and best practices for secure implementation of ethical hacking. The findings aim to provide a comprehensive understanding of how operating systems can strengthen cyber security defenses and control ethical hacking activities effectively.

Keywords: Ethical Hacking, Operating System, Security Features, Vulnerability Assessment, etc.

I. INTRODUCTION

In today's digital era, cyber threats are becoming increasingly sophisticated, affecting individuals, organizations, and critical infrastructure worldwide. Ethical hacking, also known as penetration testing, is the practice of intentionally probing systems to identify vulnerabilities in a controlled and legal manner. Unlike malicious hacking, ethical hacking helps strengthen system security by proactively discovering and fixing weaknesses.

Operating systems play a crucial role in controlling and supporting ethical hacking activities. Platforms such as Windows, Kali Linux, and other Linux-based distributions provide essential tools and security features, including access control, firewalls, encryption, logging, monitoring, and intrusion detection systems. These features allow ethical hackers to perform testing in a secure environment while minimizing risks to the system.

Additionally, the effectiveness of ethical hacking largely depends on how well these operating systems are configured and maintained, as misconfigurations can lead to security loopholes even in advanced environments.

This report investigates how different operating systems aid in managing ethical hacking, analyzing the tools, techniques, and OS-level mechanisms that prevent unauthorized access. By reviewing recent research, official documentation, and cyber security best practices, the study aims to present a structured approach to controlling ethical hacking and enhancing system security. The ultimate goal is to provide insights into how operating systems can balance the benefits of ethical hacking with the need to safeguard digital assets.

II.LITERATURE REVIEW

Ethical hacking is described through its core concepts and phases, with emphasis on rising cybercrimes, their socio-economic impact, and the need for skilled professionals to mitigate risks.[1]Ethical hacking fundamentals are explained along with practical demonstrations using Kali Linux, covering phishing, DoS attacks, Wi-Fi cracking, and vulnerability assessment techniques.[2]Privilege escalation methods on Linux and Windows are detailed, focusing on misconfigurations and system weaknesses that can be exploited during authorized penetration testing.[3]The phases of ethical hacking are reviewed along with commonly used tools and hacker classifications, though the discussion remains largely theoretical with limited technical depth.[4]Ethical hacking is also presented as an essential practice for addressing increasing cyber threats, stressing continuous security testing and the role of ethical hackers in safeguarding organizational systems.[5]Ethical hacking methodologies are further explored through structured penetration testing frameworks such as OSSTMM and OWASP Testing Guide, which provide standardized approaches for assessing system vulnerabilities and ensuring comprehensive security evaluations[6]. Singh and Sree R (2024) highlight ethical

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

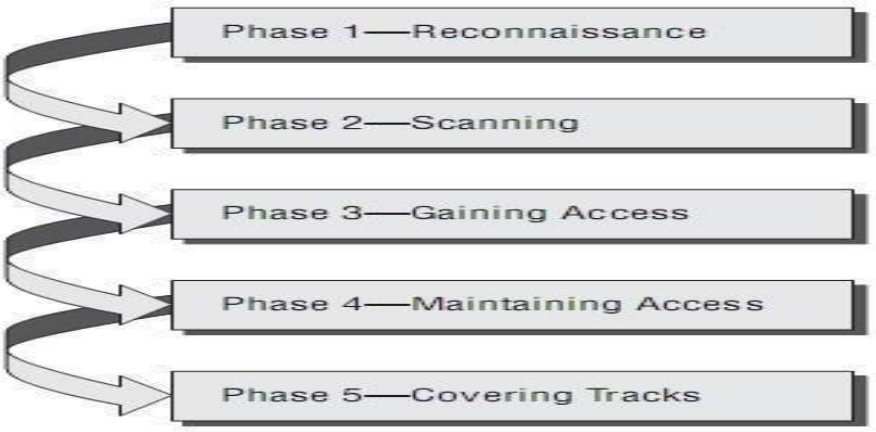
DOI: 10.17148/IJARCCE.2026.15575

hacking as a key method for identifying vulnerabilities and strengthening cyber defense systems[7]. The EC-Council CEH program provides practical training in ethical hacking techniques to improve system security[8]. Beaver (2018) introduces basic ethical hacking concepts[9]. Stallings (2021) explains core network security principles[10].

Research Gap:

1. **Limited Comparative Analysis of Linux vs. Windows Security**
   While preventive measures for both Linux and Windows are described, there is no comparative evaluation of effectiveness, performance impact, or ease of implementation across the two platforms.
2. **Lack of Empirical Validation**
   Most recommendations (e.g., using firewalls, SELinux, UFW, or Windows Defender) are suggested best practices, but there is no experimental data or real-world testing to measure their actual impact in preventing attacks.
3. **Limited Coverage of Specialized Ethical Hacking Scenarios**
   Guidance for Kali Linux focuses on isolated or VM environments, but real-world deployment scenarios, secure tool usage policies, and logging best practices could be further studied.

III.METHODOLOGY



1. Reconnaissance

Identify information about the target system **within the approved scope**, such as OS type, services, and network structure. The OS controls this by limiting information disclosure through permissions, firewall rules, and hardened configurations.

2. Scanning

Check for open ports, active hosts, and potential entry points. The OS oversees this activity with logs, intrusion detection, and network monitoring to ensure scans stay within authorized areas.

3. Gaining Access (Authorized Testing Only)

Test whether vulnerabilities can be exploited **in a controlled environment**. The OS restricts this using least privilege, sandboxing, and virtualization so the testing does not affect production systems.

4. Maintaining Access (For Assessment Purposes Only)

Evaluate how long a tester could remain in the system to measure resilience and detection. Operating systems control this with session monitoring, integrity checks, and auto-revocation of temporary access.

5. Covering Tracks (Observed, Not Practiced in Real Systems)

In ethical testing, this phase is used **only to study attacker behavior**, not to hide tester activity. The OS prevents real track-covering by enforcing strong logging, immutable logs, and centralized monitoring

Actual Work Done with Experimental Setup:

Preventing Hacking Using Linux

Linux is a preferred platform for ethical hackers due to its flexibility and open-source nature. However, it must be properly secured.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15575

1. System Hardening
   - Keep the system up-to-date:

```
> sudo apt update && sudo apt upgrade -y
```

   - Remove unnecessary packages:

```
> sudo apt autoremove
```

   - Use SELinux or AppArmor to enforce access control policies.
   - Disable root login over SSH and use SSH keys instead of passwords.

2. Firewall and Network Protection
   - Enable **UFW Firewall**:

sudo ufw enable

sudo ufw default deny incoming sudo ufw allow ssh

   - Restrict network access to trusted IPs and close unused ports.

3. Intrusion Detection
   - Tools like **Fail2Ban**, **AIDE**, and **Snort** can block repeated failed logins and detect intrusions.
   - Use **auditd** to monitor unauthorized system changes.

4. User Privileges
   - Apply the principle of **least privilege**.
   - Use separate non-root accounts for testing and administration.

5. Security in Kali Linux

Kali Linux is a specialized penetration testing distribution that includes numerous hacking tools. It should be used responsibly and securely.

Preventive Measures:

- Run Kali Linux in a virtual machine or isolated network to avoid unintended access to production systems.
- Regularly update the system and tools.
- Limit network connectivity to test environments only.
- Disable remote login and enforce strong authentication.
- Monitor and log all activities during ethical hacking sessions.

Defensive Note:

Security administrators should watch for typical Kali tool signatures (like nmap, metasploit, hydra) in network logs to detect possible unauthorized scanning.

Preventing Hacking Using Windows:

Windows is one of the most targeted systems by hackers, making prevention vital.

1. **System Updates**
   - Keep Windows Update enabled to patch vulnerabilities automatically. Settings → Windows Update → Turn on automatic updates
2. **Strong Passwords and MFA**
   - Use complex passwords and enable Multi-Factor Authentication (MFA).
   - Use password managers to store credentials securely.

3. **Windows Defender and Firewall**
   - Turn on **Windows Defender Firewall** and **Real-Time Protection** to block unauthorized connections.
     - *Path:* Control Panel → System and Security → Windows Defender Firewall

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15575

- Keep **Windows Security → Virus & Threat Protection** enabled.

4. Disable Remote Desktop (RDP)
If RDP is not needed, disable it using PowerShell:

If RDP is required, use VPN, restrict IPs, and enable Network Level Authentication.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\dsgit> Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 1
>>
```

5. Use Standard User Accounts
Avoid daily work under **Administrator** accounts. Create a **Standard User Account** and elevate privileges only when necessary.

6. Application and Browser Security
- Install software only from trusted sources or the Microsoft Store.
- Avoid pirated or cracked applications.
- Use browsers with **phishing protection** and avoid unknown links or attachments.

7. Encryption and Backup
- Use **BitLocker** to encrypt drives and protect data.
- Set up regular backups using **File History** or **OneDrive**.

8. Monitoring and Auditing
- Use **Windows Event Viewer** to monitor suspicious logins or activities.

Advanced users can install **Sysmon** (Sysinternals) for deep system event tracking

OS Security Commands
Practical Implementation — Controlling Ethical Hacking Through Operating System Security

Windows CMD & PowerShell Security Commands

1. Disable Guest Account
Disables the built-in guest account to prevent unauthorized access.

```
[CMD] net user guest /active:no
```

2. Enable Windows Firewall
Turns on the firewall for all network profiles (domain, private, public).

```
[CMD] netsh advfirewall set allprofiles state on
```

3. Block a Specific IP Address
Creates a firewall rule to block all incoming traffic from a suspicious IP.

```
[CMD] netsh advfirewall firewall add rule name="Block IP" dir=in action=block
remoteip=192.168.1.100
```

4. Check All Open Ports
Lists all active connections and listening ports with their process IDs.

```
[CMD] netstat -ano
```

5. Disable Remote Desktop (RDP)
Disables RDP to prevent remote access if not required.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15575

```
[PowerShell] Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal
Server" -Name "fDenyTSConnections" -Value 1
```

6. Lock Account After Failed Logins

Locks user account for 30 minutes after 5 failed login attempts.

```
[CMD] net accounts /lockoutthreshold:5 /lockoutduration:30
```

7. Check Currently Logged-In Users

Displays all users currently logged into the system.

```
[CMD] query user
```

8. View Failed Login Attempts

Retrieves the last 20 failed login events from the Security log (Event ID 4625).

```
[PowerShell] Get-EventLog -LogName Security -InstanceId 4625 -Newest 20
```

9. Disable USB Storage

Disables USB storage devices by setting the USBSTOR service to disabled.

```
[PowerShell] Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\USBSTOR"
-Name "Start" -Value 4
```

10. Scan System for Malware

Runs a quick scan using Windows Defender.

```
[PowerShell] Start-MpScan -ScanType QuickScan
```

11. Check Running Suspicious Processes

Lists top 20 processes sorted by CPU usage to identify suspicious activity.

```
[PowerShell] Get-Process | Sort-Object CPU -Descending | Select-Object -First 20
```

12. Enable Audit Logging

Enables success and failure audit logging for logon/logoff events.

```
[CMD] auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
```

13. Block Ping (ICMP) Requests

Blocks ICMP ping requests to prevent network reconnaissance.

```
[CMD] netsh advfirewall firewall add rule name="Block ICMP" protocol=icmpv4 dir=in
action=block
```

14. Force Strong Password Policy

Sets minimum password length to 12, max age 30 days, keeps history of 5 passwords.

```
[CMD] net accounts /minpwlen:12 /maxpwage:30 /uniquepw:5
```

15. List All Installed Software

Detects unknown or unauthorized applications installed on the system.

```
[PowerShell] Get-WmiObject -Class Win32_Product | Select-Object Name, Version
```

Linux Terminal Security Commands

1. Enable UFW Firewall

Activates the firewall, denies all incoming traffic by default, and allows SSH.

```
[Terminal] sudo ufw enable
sudo ufw default deny incoming
sudo ufw allow ssh
```

2. Block a Specific IP Address

Uses iptables to drop all incoming traffic from a suspicious IP address.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15575

```
[Terminal] sudo iptables -A INPUT -s 192.168.1.100 -j DROP
```

3. Check All Open Ports

Displays all TCP/UDP ports currently listening along with process names.

```
[Terminal] sudo netstat -tulnp
```

4. Disable Root SSH Login

Prevents root login via SSH — edit sshd_config and restart the service.

```
[Terminal] sudo nano /etc/ssh/sshd_config
# Change: PermitRootLogin yes to PermitRootLogin no
sudo systemctl restart ssh
```

5. Install & Enable Fail2Ban

Installs Fail2Ban to automatically block IPs after repeated failed login attempts.

```
[Terminal] sudo apt install fail2ban
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

6. Check Failed Login Attempts

Displays the last 20 failed SSH password attempts from the auth log.

```
[Terminal] sudo grep "Failed password" /var/log/auth.log | tail -20
```

7. Monitor Live Network Traffic

Captures and displays live packets on the network interface (eth0).

```
[Terminal] sudo tcpdump -i eth0
```

8. Check All Active Users

Shows all users currently logged into the system.

```
[Terminal] who
```

9. Lock a User Account

Locks a specific user account to prevent login.

```
[Terminal] sudo passwd -l username
```

10. Scan for Rootkits

Installs and runs rkhunter to detect rootkits and malware on the system.

```
[Terminal] sudo apt install rkhunter
sudo rkhunter --check
```

Note: All commands must be run with appropriate administrator/root privileges. These are intended for authorized system administration and ethical hacking environments only.

IV.FUTURE SCOPE

The future of ethical hacking and OS-based security focuses on improving safety, efficiency, and adaptability. AI and machine learning can automate threat detection, predict attacks, and enhance monitoring on Linux, Kali Linux, and Windows. Virtual machines, sandboxing, and isolated test environments will allow secure testing of tools without affecting production systems. Cloud and IoT security will become critical as networks expand. Advanced intrusion detection, automated auditing, and predictive analysis will strengthen defenses, while training platforms and simulations will prepare ethical hackers for real-world scenarios. These developments will make ethical hacking safer, more controlled, and more effective.

V.CONCLUSION

Ethical hacking is essential for identifying and addressing system vulnerabilities before they are exploited by malicious actors. Operating systems like Windows, Kali Linux, and other Linux-based distributions provide built-in security features such as access controls, logging, auditing, and monitoring, which help manage and control ethical hacking

DOI: 10.17148/IJARCCE.2026.15575

activities. By combining ethical hacking practices with OS-level protections, organizations can proactively enhance their cybersecurity defenses, prevent unauthorized access, and ensure that testing is conducted safely and lawfully. This approach not only strengthens system security but also supports compliance with industry standards and emerging cybersecurity best practices.

REFERENCES

[1]. Ch. Mary Pushpa, K.V.M. Udaya Lakshmi & S. Hepsibha, "Ethical Hacking: Roles, Phases and Impact on Various Sectors of the Economy," International Journal, India. IJSRCSEIT+1

[2]. Ashish Oberoi, "A Study on Ethical Hacking," International Journal of Innovative Research in Computer Science & Technology, India, 2022. ACS Publisher

[3]. Mithlesh Kumar Yadav & Sukhesh Kothari, "Different Methods of Privilege Escalation on Linux and Windows Machine," Journal of Web Development and Web Designing, India, 2021. matjournals.co.in

[4]. Fiza Abdul Hafiz Qureshi, Mayur Dube, Komal Ramteke & Akshay Akhare, "A Review Paper on Ethical Hacking," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), India, 2023. IJARSCT

[5]. Shallu Dogra, Nitin Singh, Ayush & Sahil, "A Review Paper on Ethical Hacking," International Journal of Scientific Research in Engineering and Management (IJSREM), India, 2024. IJSREM

[6]. Akanksha Yadav, "Ethical Hacking Technique with Penetration Testing for Security," IJARSCT, India, 2022. IJARSCT

[7]. Ananya Singh & Usha Sree R, "Beyond the Surface: Investigating Ethical Hacking for Cyber Defense," IJARSCT, India, 2024. IJARSCT

[8]. EC-Council. (n.d.). *Certified Ethical Hacker (CEH) program*. EC-Council. Retrieved May 5, 2026.

Books

[1]. Beaver, K. (2018). Hacking For Dummies (6th ed.). Wiley Publishing.

[2]. Stallings, W. (2021). Network Security Essentials: Applications and Standards.