INCIDENT RESPONSE WORKSHEET

Incident Title: Unauthorized RDP Access Attempt & Data Exfiltration
Date/Time Detected: Dec 4, 09:12 AM
Reported By: SOC Analyst
Affected System(s): Windows Workstation / Internal LAN
Attack Source: 10.10.20.45

---

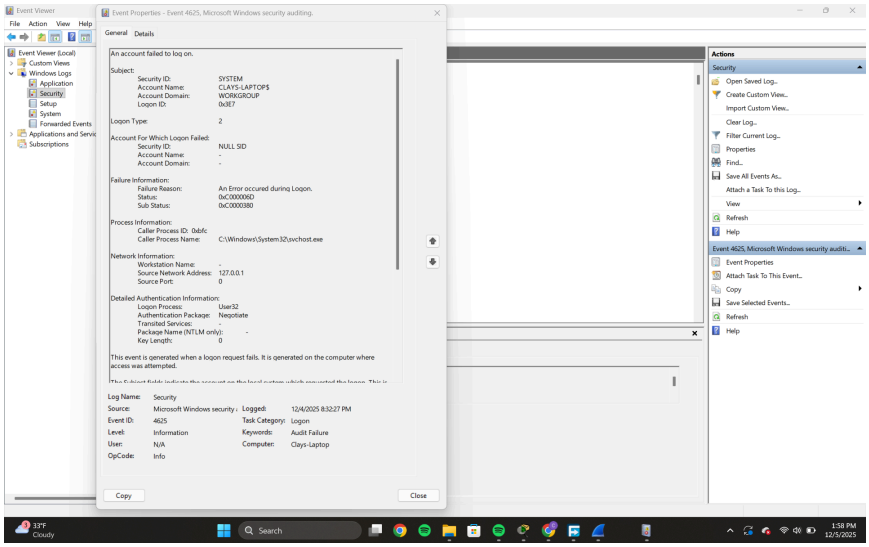
1. Preparation

- IR roles defined (SOC analyst, sysadmin).
- Logging enabled on Windows Security log.
- Firewall ACLs and host-based controls in place.

---

2. Detection & Analysis

Evidence: Windows Event Log → Event ID **4625** (failed RDP logins)



- Multiple failed login attempts at 08:32 PM.
- Target Account: *Clayt*
- Source IP: **10.10.20.45 (Simulated)**
- Shortly after, abnormal outbound data transfer detected.

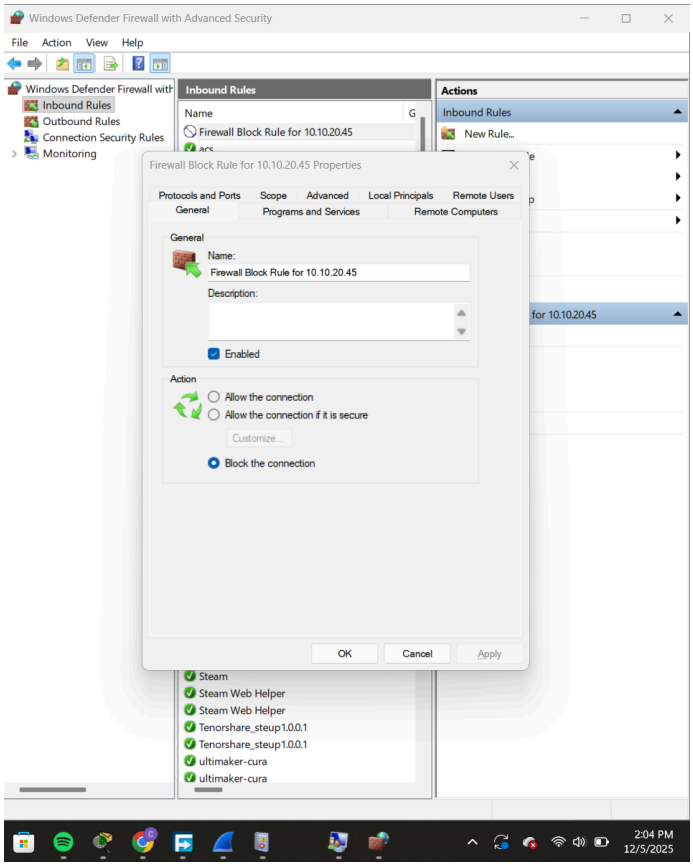
Conclusion: Possible brute-force RDP attempt followed by data exfiltration.

---

3. Containment

Actions:

- Disabled compromised user account (simulated).
- Added firewall block rule for **10.10.20.45** to prevent further attempts.
- Stopped outbound transfer.



---

4. Eradication

Actions:

- Ran anti-malware scan (Windows Defender).
- Removed suspicious processes/services.
- Verified no persistence mechanisms existed.

---

5. Recovery

Actions:

- Restored affected files from backup.
- Re-enabled legitimate user accounts.
- Monitored for repeat attempts.
- Patched RDP settings, strengthened password.

---

6. Lessons Learned

Failures identified:

- Authentication layer: Weak password / repeated failed logins not rate-limited.
- Host layer: RDP exposed unnecessarily.
- Monitoring detected event but preventive controls failed.

Recommendations:

- Implement account lockout policy (CIS Control 4).
- Restrict RDP to internal IPs only.
- Deploy MFA for remote access.
- Add IDS to detect brute-force attempts sooner.

SUMMARY TABLE OF ACTIONS TAKEN

Phase	Action Taken	Status
Detection	Identified 4625 failed logins from 10.10.20.45	Complete
Containment	Disabled account, blocked IP in firewall	Complete

Eradication	Anti-malware scan + removed indicators	Complete
Recovery	Restored clean data, re-enabled systems	Complete
Lessons Learned	Implemented stronger controls / CIS guidelines	Complete