Milestone 3 — Incident Response Plan

Student Name: Clayton Holden

Date Submitted: 12/5/2025
Course: CYBR-2102 Network Defense Fundamentals
Instructor: Norma DePriest

1️⃣ Incident Overview

Field	Entry
Incident Title	Unauthorized RDP Brute Force & Data Exfiltration Attempt
Date / Time Detected	December 4, 09:12 AM
Detected By	☑ SOC Tool ☐ User ☐ Administrator
Detection Method / Source	Windows Security Log Event ID 4625 (Failed RDP Logins)
Systems Affected	Windows Workstation, Internal Network Boundary
Severity Level	High
Current Status	☐ Open ☑ Contained ☐ Closed

2️⃣ Incident Response Team Structure

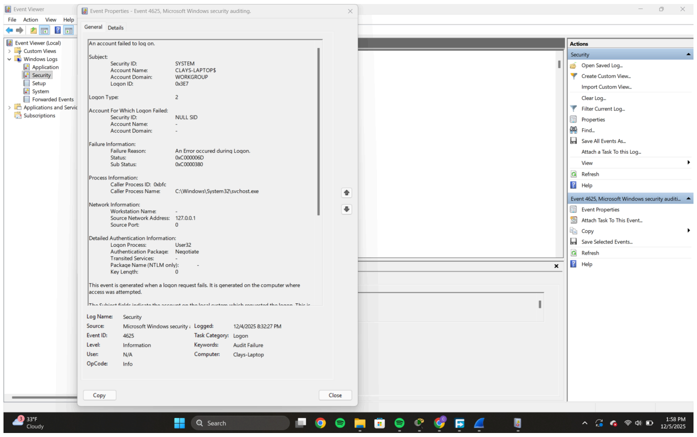
Role	Name / Responsibility	Contact Info
Incident Manager	Oversees response, approves containment	incident.manager@example.com

Technical Lead	Conducts analysis, applies containment steps	tech.lead@example.com
Communications Officer	Handles internal/external communication	comms@example.com
Legal / Compliance	Ensures IR actions satisfy regulations	legal@example.com
HR / Management Liaison	Coordinates with leadership & HR	hr@example.com

3️⃣ Response Phases – NIST SP 800-61 Framework

Phase	Actions Taken	Evidence / Verification	Framework Reference
Preparation	Logging enabled, IR roles defined, host firewall active	System baseline, IR documentation	NIST 800-61: Preparation / CIS Control 8
Detection & Analysis	SOC detected repeated Event ID 4625 from 10.10.20.45. Analyst reviewed logs and confirmed failed RDP attempts.	Screenshot of 4625 Security Log	NIST 800-61: Detection / CIS Control 6
Containment	Disabled compromised account and blocked 10.10.20.45 on firewall. Terminated outbound transfer.	Screenshot of blocked IP / disabled account	NIST 800-61: Containment / CIS Control 4
Eradication	Ran anti-malware scan, removed suspicious artifacts, verified clean system state.	Defender scan results	NIST 800-61: Eradication
Recovery	Restored affected files from backups, monitored system for new login attempts, re-enabled legitimate accounts.	Recovery logs / restored files list	NIST 800-61: Recovery / CIS Control 11

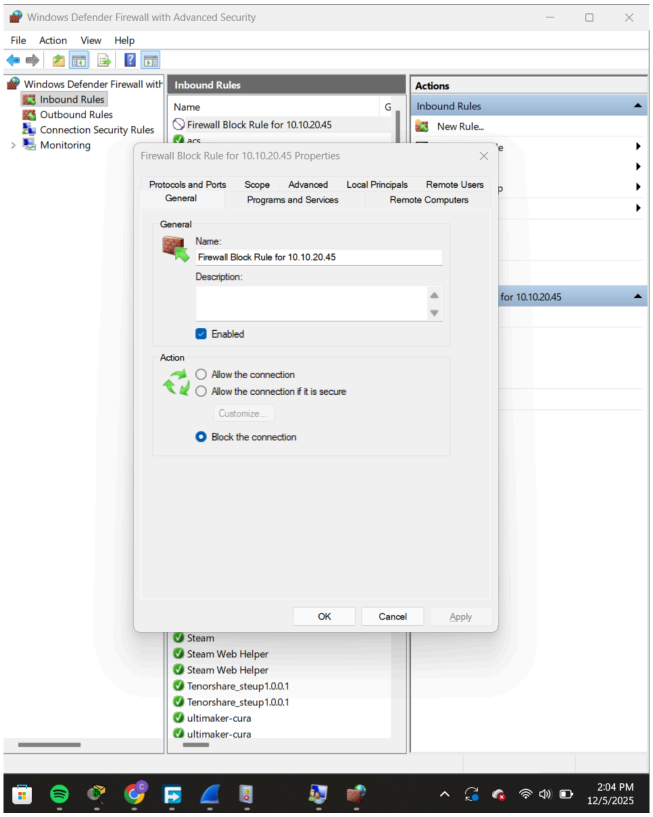
Post-Incident Activity	Conducted review. Identified weak authentication and exposed RDP service. Updated controls and policy.	Lessons learned report	NIST 800-61: Post-Incident Activity



Event Properties - Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           CLAYS-LAPTOP$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -

Failure Information:
        Failure Reason:         An Error occured during Logon.
        Status:                 0xC000006D
        Sub Status:             0xC0000380

Process Information:
        Caller Process ID:  0xbfc
        Caller Process Name:    C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       -
        Source Network Address: 127.0.0.1
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where
access was attempted.
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:         12/4/2025 8:32:27 PM
Event ID:   4625                           Task Category:  Logon
Level:      Information                    Keywords:       Audit Failure
User:       N/A                            Computer:       Clays-Laptop
OpCode:     Info
```



Firewall Block Rule for 10.10.20.45 Properties

General

Name: Firewall Block Rule for 10.10.20.45

Description:

☑ Enabled

Action

○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

---

4 Timeline of Events

Time Stamp	Event Description	Action Taken	Responsible Party
09:12 AM	Multiple failed RDP logins from 10.10.20.45	SOC alert triggered	Analyst
09:14 AM	Reviewed Security Log (4625 entries)	Detection confirmed	SOC Lead
09:18 AM	Outbound data transfer detected	Verified unusual behavior	Analyst
09:20 AM	Disabled compromised local account	Containment implemented	Admin
09:22 AM	Blocked source IP via firewall rule	Prevented further access attempts	Admin
09:30 AM	Anti-malware scan completed	System cleaned	Technical Lead
09:45 AM	Restored affected data from backup	Recovery	Technical Lead
10:00 AM	Conducted incident review	Documented findings	IR Manager

5️⃣ Root Cause Analysis & Findings

The attack was caused by an external adversary using brute-force attempts against Remote Desktop Protocol (RDP). Weak authentication controls and lack of account lockout thresholds allowed repeated login attempts without triggering preventive controls. The exposed RDP service increased the attack surface. Initial outbound exfiltration attempt indicates partial compromise before containment.

6️⃣ Recommendations / Preventive Actions

Control Area	Recommended Action	Priority	Verification Step
Access Control	Implement MFA, RDP allowed only through VPN, enforce account lockout after 3–5 failed attempts	High	Test lockout policy, verify MFA works

Patch Management	Regularly update RDP services and OS patches	Medium	Patch scan shows system compliant
Firewall Rules	Restrict RDP to internal IP addresses only, block untrusted sources	High	Test inbound rules and verify block
User Awareness Training	Train staff to report unusual login alerts	Medium	Attendance records, phishing simulations

---

7️⃣ Evidence Checklist

☑ Security Log screenshots
☑ Firewall update evidence
☑ IR Plan table complete
☑ Timeline filled
☑ Recommendations included
☑ File named correctly (`Holden_CYBR2102_M3.pdf`)

8️⃣ Sign-Off

Step	Completed By	Date	Verified By (Instructor)
Incident Response Plan Created	Clayton Holden	12/5/2025	
Evidence Attached	Clayton Holden	12/5/2025	
Recommendations Documented	Clayton Holden	12/5/2025	