Core Deck v3 - Attack Tool(s) and Detection Link(s) with Blogs

Initial Compromise (Cards 1-10)

1. **Phishing**
    - **Attack Tool(s)**: Modlishka, evilginx, GoPhish, Social-Engineer-Toolkit (SET)
        - Modlishka: https://github.com/drk1wi/Modlishka
        - evilginx: https://github.com/kgretzky/evilginx2
        - GoPhish: https://getgophish.com/
        - SET: https://github.com/trustedsec/social-engineer-toolkit
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "How to Phish for Geniuses" - https://www.blackhillsinfosec.com/how-to-phish-for-geniuses/ - Covers phishing tactics and tools like Modlishka.
        - "Gone Phishing: Installing GoPhish and Creating a Campaign - https://www.blackhillsinfosec.com/installing-gophish-and-creating-a-campaign/ - GoPhish setup and use.
2. **Web Server Compromise**
    - **Attack Tool(s)**: Burp Suite, Caido, sqlmap, Nuclei
        - Burp Suite: https://portswigger.net/burp
        - Caido: https://caido.io/
        - sqlmap: https://sqlmap.org/
        - Nuclei: https://github.com/projectdiscovery/nuclei
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Using Simple Burp Macros to Automate Testing" - https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing/ - Burp Suite automation tips.
3. **Unauthorized Cloud Access**
    - **Attack Tool(s)**: GraphRunner, ROADtools, ScoutSuite, Pacu
        - GraphRunner: https://github.com/dafthack/GraphRunner
        - ROADtools: https://github.com/dirkjanm/ROADtools
        - ScoutSuite: https://github.com/nccgroup/ScoutSuite
        - Pacu: https://github.com/RhinoSecurityLabs/pacu
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Introducing GraphRunner" - https://www.blackhillsinfosec.com/introducing-graphrunner/ - Specific to GraphRunner.
4. **Insider Threat**
    - **Attack Tool(s)**: Company Issued Equipment

        - No specific tool link (conceptual).
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
5. **External Password Spray**
    - **Attack Tool(s)**: CredMaster, MSOLSpray, FireProx, FindMeAccess
        - CredMaster: https://github.com/knavesec/CredMaster
        - MSOLSpray: https://github.com/dafthack/MSOLSpray
        - FireProx: https://github.com/ustayready/fireprox
        - FindMeAccess: https://github.com/absolomb/FindMeAccess
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
6. **Trusted Relationship**
    - **Attack Tool(s)**: Gato-X, Compromised Service Accounts, Publicly Available Breach Data
        - Gato-X: https://github.com/AdnaneKhan/Gato-X
        - Compromised Service Accounts: No specific tool link.
        - Publicly Available Breach Data: https://haveibeenpwned.com/
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
7. **Social Engineering**
    - **Attack Tool(s)**: Open-Source Intelligence Gathering (OSINT), Manipulation of Human Feelings, Sense of Urgency
        - OSINT: https://osintframework.com/
        - Manipulation/Sense of Urgency: No specific tool links.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "The Human Element in Cybersecurity: Understanding Trust and Social Engineering" - http://blackhillsinfosec.com/understanding-trust-and-social-engineering/ - Techniques and detection.
8. **Bring Your Own (Exploited) Device**
    - **Attack Tool(s)**: Malware, Remote Access Trojan (RAT), Malicious Web Ads
        - Malware: General term.
        - RAT: Example - https://github.com/quasar/Quasar
        - Malicious Web Ads: No specific tool link.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Pentesting Dropbox on Steroids" - https://www.blackhillsinfosec.com/pentesting-dropbox-on-steroids/ - BYOD exploitation context.
9. **External Service Exploitation**
    - **Attack Tool(s)**: Nuclei, Metasploit, Exploit-db, Shodan

        - Nuclei: https://github.com/projectdiscovery/nuclei
        - Metasploit: https://www.metasploit.com/
        - Exploit-db: https://www.exploit-db.com/
        - Shodan: https://www.shodan.io/
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "In Through the Front Door - Protecting Your Perimeter" - https://www.blackhillsinfosec.com/in-through-the-front-door-protecting-your-perimeter/
10. **Credential Stuffing**
    - **Attack Tool(s)**: CredMaster, Burp Suite, Hashcat, Hydra
        - CredMaster: https://github.com/knavesec/CredMaster
        - Burp Suite: https://portswigger.net/burp
        - Hashcat: https://hashcat.net/hashcat/
        - Hydra: https://github.com/vanhauser-thc/thc-hydra
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Running Hashcat on Ubuntu" - https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti/ - Hashcat setup.
        - "Using Simple Burp Macros" - https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing/ - Burp Suite tips.

Pivot and Escalate (Cards 11-17)

11. **Internal Password Spray**
    - **Attack Tool(s)**: Kerbrute, NetExec, Net Use, lolbins
        - Kerbrute: https://github.com/ropnop/kerbrute
        - NetExec: https://github.com/Pennyw0rth/NetExec
        - Net Use: Native Windows command.
        - lolbins: https://lolbas-project.github.io/
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Webcast: Attack Tactics 5 - Zero to Hero" - https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack/ - Kerbrute usage.
12. **Kerberoasting**
    - **Attack Tool(s)**: Rubeus, Impacket, Hashcat, NetExec
        - Rubeus: https://github.com/GhostPack/Rubeus
        - Impacket: https://github.com/SecureAuthCorp/impacket

        - Hashcat: https://hashcat.net/hashcat/
        - NetExec: https://github.com/Pennyw0rth/NetExec
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "One Active Directory Account Can Be Your Best Early Warning" - https://www.blackhillsinfosec.com/one-active-directory-account-can-be-your-best-early-warning/
        - "Running Hashcat on Ubuntu" - https://www.blackhillsinfosec.com/running-hashcat-on-ubuntu-18-04-server-with-1080ti/ - Hashcat guide.
13. **Broadcast/Multicast Protocol Poisoning**
    - **Attack Tool(s)**: Responder, Impacket, MITM6, Inveigh
        - Responder: https://github.com/lgandx/Responder
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - MITM6: https://github.com/dirkjanm/mitm6
        - Inveigh: https://github.com/Kevin-Robertson/Inveigh
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "How to Disable LLMNR & Why You Want To" - https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ - Responder and LLMNR poisoning.
        - "MITM6 Strikes Again: The Dark Side of IPv6" - https://www.blackhillsinfosec.com/mitm6-strikes-again-the-dark-side-of-ipv6/ - MITM6 tactics.
14. **Weaponizing Active Directory**
    - **Attack Tool(s)**: BloodHound, PlumHound, ADMiner, SCCMHunter
        - BloodHound: https://github.com/BloodHoundAD/BloodHound
        - PlumHound: https://github.com/PlumHound/PlumHound
        - ADMiner: https://github.com/MAQsecure/ADMiner
        - SCCMHunter: https://github.com/garrettfoster13/sccmhunter
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Webcast: Weaponizing Active Directory" - https://www.blackhillsinfosec.com/webcast-weaponizing-active-directory/ - BloodHound usage.
        - "PlumHound Reporting Engine for BloodHoundAD" - https://www.blackhillsinfosec.com/plumhound-reporting-engine-for-bloodhoundad/ - PlumHound overview.
15. **Credential Harvesting**
    - **Attack Tool(s)**: GraphRunner, DonPAPI, Snaffler, Mimikatz
        - GraphRunner: https://github.com/dafthack/GraphRunner
        - DonPAPI: https://github.com/login-securite/DonPAPI

        - Snaffler: https://github.com/SnaffCon/Snaffler
        - Mimikatz: https://github.com/gentilkiwi/mimikatz
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Domain Goodness: Learned to Love AD Explorer" - https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer/ - Credential harvesting context.
        - "Indecent Exposure: Your Secrets are Showing" - https://www.blackhillsinfosec.com/indecent-exposure-your-secrets-are-showing/ - Snaffler usage.
16. **New Service Creation/Modification**
    - **Attack Tool(s)**: PsExec, PowerShell, ServiceController, Malware
        - PsExec: https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
        - PowerShell: Native Windows tool.
        - ServiceController: .NET class, no external link.
        - Malware: General term.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Digging Deeper: Vulnerable Windows Services" - https://www.blackhillsinfosec.com/digging-deeper-vulnerable-windows-services/ - Service manipulation.
17. **Local Privilege Escalation (LPE)**
    - **Attack Tool(s)**: Impacket, Seatbelt, SharpUp, PEASS-ng
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - Seatbelt: https://github.com/GhostPack/Seatbelt
        - SharpUp: https://github.com/GhostPack/SharpUp
        - PEASS-ng: https://github.com/peass-ng/PEASS-ng
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "PowerShell Without PowerShell" - https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/ - Privilege escalation context.

Persistence (Cards 18-26)

18. **Malicious Service**
    - **Attack Tool(s)**: SharpStay, SharPersist, StayKit, PsExec
        - SharpStay: https://github.com/0xthirteen/SharpStay
        - SharPersist: https://github.com/mandiant/SharPersist

        - StayKit: https://github.com/0xthirteen/StayKit
        - PsExec: https://learn.microsoft.com/en-us/sysinternals/downloads/psexec
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Digging Deeper: Vulnerable Windows Services" - https://www.blackhillsinfosec.com/digging-deeper-vulnerable-windows-services/ - Service persistence.
19. **Dynamic Link Library (DLL) Hijacking**
    - **Attack Tool(s)**: DLLHijackTest, PowerSploit, FaceDancer, PersistBOF
        - DLLHijackTest: https://github.com/slyd0g/DLLHijackTest
        - PowerSploit: https://github.com/PowerShellMafia/PowerSploit
        - FaceDancer: https://github.com/usb-tools/FaceDancer
        - PersistBOF: https://github.com/N4kedTurtle/PersistBOF
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "PowerShell Without PowerShell" - https://www.blackhillsinfosec.com/powershell-without-powershell-how-to-bypass-application-whitelisting-environment-restrictions-av/ - DLL hijacking context.
20. **Malicious Driver**
    - **Attack Tool(s)**: Impacket, PowerShell, Metasploit, Kernel Driver Utility (KDU), SharpStay
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - PowerShell: Native Windows tool.
        - Metasploit: https://www.metasploit.com/
        - KDU: https://github.com/hfiref0x/KDU
        - SharpStay: https://github.com/0xthirteen/SharpStay
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
21. **New User Added**
    - **Attack Tool(s)**: Metasploit, Impacket, Havok, Mythic
        - Metasploit: https://www.metasploit.com/
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
22. **Application Shimming**
    - **Attack Tool(s)**: Metasploit, PowerShell, ShimGenerator, sdb-explorer, Atomic Red Team (ART)
        - Metasploit: https://www.metasploit.com/

        - PowerShell: Native Windows tool.
        - ShimGenerator: https://github.com/mandiant/ShimGenerator
        - sdb-explorer: https://github.com/mandiant/sdb-explorer
        - ART: https://github.com/redcanaryco/atomic-red-team
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Backdoors & Breaches: Logon Scripts" - https://www.blackhillsinfosec.com/backdoors-breaches-logon-scripts/ - Persistence context.
23. **Malicious Browser Plugins**
    - **Attack Tool(s)**: Metasploit, PowerShell, Chromebackdoor, BeEF, Evilginx2
        - Metasploit: https://www.metasploit.com/
        - PowerShell: Native Windows tool.
        - Chromebackdoor: https://github.com/graniet/chromebackdoor
        - BeEF: https://beefproject.com/
        - Evilginx2: https://github.com/kgretzky/evilginx2
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
24. **Logon Scripts**
    - **Attack Tool(s)**: Metasploit, Impacket, Havok, Mythic
        - Metasploit: https://www.metasploit.com/
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Backdoors & Breaches: Logon Scripts" - https://www.blackhillsinfosec.com/backdoors-breaches-logon-scripts/ - Logon script persistence.
25. **Malicious Firmware**
    - **Attack Tool(s)**: CHIPSEC, Flashrom, Impacket, PowerShell, Metasploit
        - CHIPSEC: https://github.com/chipsec/chipsec
        - Flashrom: https://www.flashrom.org/Flashrom
        - Impacket: https://github.com/SecureAuthCorp/impacket
        - PowerShell: Native Windows tool.
        - Metasploit: https://www.metasploit.com/
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
26. **Accessibility Features**
    - **Attack Tool(s)**: Bash Bunny, USB Rubber Ducky, OMGCable
        - Bash Bunny: https://shop.hak5.org/products/bash-bunny
        - USB Rubber Ducky: https://shop.hak5.org/products/usb-rubber-ducky

        - OMGCable: https://shop.hak5.org/products/omg-cable
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "How to Pull Wireless Credentials with the Bash Bunny" - https://www.blackhillsinfosec.com/pull-wireless-credentials-bash-bunny/ - USB-based persistence.

C2 and Exfil (Cards 27-32)

27. **HTTP as EXFIL**
    - **Attack Tool(s)**: Sliver, Havok, Mythic
        - Sliver: https://github.com/BishopFox/sliver
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
28. **HTTPS as EXFIL**
    - **Attack Tool(s)**: Sliver, Havok, Mythic
        - Sliver: https://github.com/BishopFox/sliver
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
29. **DNS as C2**
    - **Attack Tool(s)**: Havok, Mythic
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Bypassing Cylance Part 2: Using dnscat2" - https://www.blackhillsinfosec.com/bypassing-cylance-part-2-using-dnscat2/ - DNS C2 context.
30. **Background Intelligent Transfer Service (BITS) as EXFIL**
    - **Attack Tool(s)**: Leviathan, UBoatRAT
        - Leviathan: https://github.com/deruke/tools
        - UBoatRAT: No official link; malware research via https://attack.mitre.org/software/S0332/
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
31. **Cloud-Based Services as Exfil**
    - **Attack Tool(s)**: Gcat, Sneaky Creeper, Gost

        - Gcat: https://github.com/byt3bl33d3r/gcat
        - Sneaky Creeper: https://github.com/DakotaNelson/sneaky-creeper
        - Gost: https://github.com/ginuerzh/gost
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
32. **Domain Fronting as C2**
    - **Attack Tool(s)**: Sliver, Havok, Mythic
        - Sliver: https://github.com/BishopFox/sliver
        - Havok: https://github.com/HavocFramework/Havoc
        - Mythic: https://github.com/its-a-feature/Mythic
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
        - "Bypass Web Proxy Filtering" - https://www.blackhillsinfosec.com/bypass-web-proxy-filtering/ - Domain fronting techniques.

Detection (Cards 33-45)

33. Server Analysis

- **Detection Tools**: DeepBlueCLI, Velociraptor, SysInternals Suite
    - **DeepBlueCLI**: https://github.com/sans-blue-team/DeepBlueCLI - Open-source PowerShell script for event log analysis.
    - **Velociraptor**: https://docs.velociraptor.app/ - Advanced endpoint monitoring and response tool (official docs link to downloads).
    - **SysInternals Suite**: https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite - Microsoft's collection of system utilities.

34. Security Information and Event Management (SIEM) Log Analysis

- **Detection Tools**: Security Onion, OSSIM, Wazuh, JPCert Tool Analysis
    - **Security Onion**: https://securityonionsolutions.com/ - Open-source SIEM and network monitoring platform.
    - **OSSIM**: https://www.alienvault.com/open-source-siem - Open Source Security Information Management by AT&T Cybersecurity.
    - **Wazuh**: https://wazuh.com/ - Open-source security monitoring platform.
    - **JPCert Tool Analysis**: https://jpcertcc.github.io/ToolAnalysisResultSheet/ - JPCERT/CC's tool analysis resource.

35. Firewall Log Review

- **Detection Tools**: Wazuh, Graylog Open, ELK Stack, Security Onion, Kiwi Syslog Server
    - **Wazuh**: https://wazuh.com/ - Open-source security monitoring platform.
    - **Graylog Open**: https://www.graylog.org/ - Open-source log management tool (formerly Graylog Community Edition).
    - **ELK Stack**: https://www.elastic.co/elastic-stack/ - Elasticsearch, Logstash, and Kibana suite for log analysis.
    - **Security Onion**: https://securityonionsolutions.com/ - Open-source SIEM and network monitoring.
    - **Kiwi Syslog Server**: https://www.solarwinds.com/kiwi-syslog-server/ - Commercial syslog server with free version available.

36. Network Threat Hunting

- **Detection Tools**: Real Intelligence Threat Analytics (RITA), Security Onion, AC-Hunter Community Edition, Passer, espy
    - **Real Intelligence Threat Analytics (RITA)**: https://www.activecountermeasures.com/free-tools/rita/ - Open-source network traffic analysis tool.
    - **Security Onion**: https://securityonionsolutions.com/ - Open-source SIEM and network monitoring.
    - **AC-Hunter Community Edition**: https://www.activecountermeasures.com/free-tools/ - Free version of AC-Hunter for threat hunting (listed under Active Countermeasures tools).
    - **Passer**: https://github.com/byt3bl33d3r/Passer - Tool for parsing network traffic (less common, GitHub primary source).
    - **espy**: No official standalone link; often part of Security Onion or custom scripts (contextual use within threat hunting).

37. Active Defense and Cyber Deception

- **Detection Tools**: CanaryTokens, HoneyBadger, Active Defense Harbinger Distribution (ADHD), MITRE Engage
    - **CanaryTokens**: https://canarytokens.org/ - Free honeytoken service by Thinkst.
    - **HoneyBadger**: https://github.com/davidhowell-tx/HoneyBadger - Open-source tool for honeypot deployment (GitHub primary source).
    - **Active Defense Harbinger Distribution (ADHD)**: https://www.activecountermeasures.com/free-tools/adhd/ - Open-source active defense toolkit.
    - **MITRE Engage**: https://engage.mitre.org/ - Framework and resources for active defense.

38. Endpoint Security Protection Analysis

- **Detection Tools**: Elastic Security, OpenEDR, Velociraptor, OSSEC, Wazuh
    - **Elastic Security**: https://www.elastic.co/security/ - SIEM and endpoint security solution from Elastic.
    - **OpenEDR**: https://www.openedr.com/ - Open-source endpoint detection and response tool.
    - **Velociraptor**: https://docs.velociraptor.app/ - Advanced endpoint monitoring and response.
    - **OSSEC**: https://www.ossec.net/ - Open-source host-based intrusion detection system.
    - **Wazuh**: https://wazuh.com/ - Open-source security monitoring platform.

39. User and Entity Behavior Analytics (UEBA)

- **Detection Tools**: LogonTracer, DeepBlueCLI, OpenUBA, Hayabusa
    - **LogonTracer**: https://github.com/JPCERTCC/LogonTracer - Tool for visualizing logon events.
    - **DeepBlueCLI**: https://github.com/sans-blue-team/DeepBlueCLI - PowerShell script for event log analysis.
    - **OpenUBA**: https://openuba.org/ - Open-source user behavior analytics platform.
    - **Hayabusa**: https://github.com/Yamato-Security/hayabusa - Fast forensics timeline generator and threat hunting tool.

40. Endpoint Analysis

- **Detection Tools**: DeepBlueCLI, Velociraptor, Incident Response Cheat Sheets, OSquery
    - **DeepBlueCLI**: https://github.com/sans-blue-team/DeepBlueCLI - Event log analysis tool.
    - **Velociraptor**: https://docs.velociraptor.app/ - Endpoint monitoring and response.
    - **Incident Response Cheat Sheets**: https://www.sans.org/posters/ - SANS provides various IR cheat sheets (general resource).
    - **OSquery**: https://osquery.io/ - Open-source operating system instrumentation framework.

41. Isolation

- **Detection Tools**: Switch and Router Commands, Host Firewall, Endpoint Detection and Response (EDR) Tools
    - **Switch and Router Commands**: No specific link; refers to vendor-specific CLI commands (e.g., Cisco, Juniper documentation).

    - **Host Firewall**: Native to OS (e.g., Windows Firewall, iptables); no external tool link.
    - **Endpoint Detection and Response (EDR) Tools**: General category; examples include https://www.crowdstrike.com/ (CrowdStrike) or https://www.elastic.co/security/ (Elastic Security).

42. Crisis Management

- **Detection Tools**: Incident Response Plans (IRP), Disaster Recovery Plans (DRP)
    - **Incident Response Plans (IRP)**: No specific tool link; refers to organizational documentation (e.g., NIST SP 800-61 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf).
    - **Disaster Recovery Plans (DRP)**: No specific tool link; organizational documentation (e.g., NIST SP 800-34 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf).

43. Memory Analysis

- **Detection Tools**: Volatility, Velociraptor, Endpoint Detection and Response (EDR) Tools
    - **Volatility**: https://www.volatilityfoundation.org/ - Open-source memory forensics framework.
    - **Velociraptor**: https://docs.velociraptor.app/ - Endpoint monitoring with memory analysis capabilities.
    - **Endpoint Detection and Response (EDR) Tools**: General category; examples include https://www.crowdstrike.com/ or https://www.elastic.co/security/.

44. Cloud Event Log Analysis

- **Detection Tools**: Wazuh, Security Onion, Greylog Open, Falco, Hawk
    - **Wazuh**: https://wazuh.com/ - Open-source security monitoring.
    - **Security Onion**: https://securityonionsolutions.com/ - Open-source SIEM and monitoring.
    - **Greylog Open**: https://www.graylog.org/ - Open-source log management (corrected spelling from "Greylog").
    - **Falco**: https://falco.org/ - Open-source cloud-native runtime security tool.
    - **Hawk**: https://github.com/ClusterLabs/hawk - Monitoring tool for cloud environments (contextual match; less common in this exact context).

45. Permissions Audit

- **Detection Tools**: AD Users and Computers, BloodHound, ScoutSuite, Prowler
    - **AD Users and Computers**: Native Windows tool; no external link (part of Active Directory management).
    - **BloodHound**: https://github.com/BloodHoundAD/BloodHound - AD attack path analysis tool.
    - **ScoutSuite**: https://github.com/nccgroup/ScoutSuite - Multi-cloud security auditing tool.
    - **Prowler**: https://github.com/prowler-cloud/prowler - AWS security assessment tool.

Injects (Cards 46-52)

46. **False Alarm: It was a Penetration Test**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: https://www.blackhillsinfosec.com/
    - **Helpful Blogs (BHIS)**:
47. **Data Uploaded to Pastebin**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
48. **Analyst Returns from Incident Response Training**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
49. **"Policy? What Policy?"**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
50. **Luck of the SOC**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
51. **Bobby the Intern Kills the System You are Reviewing**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**:
52. **Legal Takes Your Most Skilled Handler into a Meeting**
    - **Attack Tool(s)**: None listed.
    - **Detection Link(s)**: None listed in the row.
    - **Helpful Blogs (BHIS)**: