CERIAS

The Center for Education and Research in Information Assurance and Security

Code Blue – Gamification of Incident Response

Olivia Anderson and Nicole Hands, Department of Computer Information Technology

SUMMARY

Gamification, or the process of applying game-like elements to non-game scenarios, has been shown to increase learners' skill and knowledge mastery, motivation, interest, and enjoyment. Applying gamification to cybersecurity incident response would allow learners to develop the technical and decision-making skills required to effectively detect and respond to cyber incidents in a more accessible and appealing format. This project looks at improving cybersecurity education through gamification. The solution we've developed utilizes Roguelike games to provide a randomized scenario in which students can practice incident response in real-world like conditions.

BACKGROUND

Gamification, or the application of game-like elements to non-game scenarios, and serious games, or games with a focus on learning, have proven to be an effective tool in teaching. Gamification has been shown to have a positive effect on student engagement, motivation, interest, enjoyment, conceptual understanding, skill development, and speed of mastery. According to the constructivist learning theory, learning occurs more effectively when students are actively involved in the knowledge construction process compared to passively receiving information [4]. Gamification is one method of providing hands on experience and active engagement to students, thereby helping to improve their knowledge construction. The field of cybersecurity has proven to be especially conducive to gamification, and research has found that applying game-like elements to cybersecurity trainings have increased participants skills, involvement, interest, and enjoyment. It allows students to develop their skills and knowledge through experiences that emulate real world scenarios, increasing the applicability of their knowledge. The higher cybersecurity proficiency developed through gamification can directly translate to an improved ability to detect and respond to cybersecurity incidents and improve critical decision-making skills. This project examined applying gamification to incident response to better help cybersecurity students and professionals develop the technical and decision-making skills required to effectively respond to cybersecurity incidents.

KEY ELEMENTS

Roguelike **– popular gaming platform. Provides randomized game maps and scenarios and permadeath.**

Mitre ATT&CK Framework **– cybersecurity standard used to analyze and categorize incidents. Used to breakdown case studies for Code Blue.**

Backdoors and Breaches **– Incident Response card game by Black Hills Security and Active Countermeasures used as a reference for gameplay structure.**

NIST Cybersecurity Framework **– used to supplement the defensive actions and tools players can utilize in gameplay.**

CASE STUDY - SOLARWINDS

MITRE ATT&CK ANALYSIS

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command & Scripting Interpreter	BITS Job	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limit	Data Destruction
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Job	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forget Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container & Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains		Trusted Relationship	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			System Services	Implant Internal Image	Process Injection	File & Directory Permissions Modification	OS Credential Dumping	File & Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	Proxy		System Shutdown/Reboot
				Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Web Service		
				Server Software Component		Indirect Command Execution		Password Policy Discovery					
				Traffic Signaling		Masquerading		Peripheral Device Discovery					
				Valid Accounts		Modify Authentication Process		Permission Groups Discovery					
						Modify Cloud Compute Infrastructure		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image		Remote System Discovery					
						Network Boundary Bridging		Software Discovery					
						Obfuscated Files or Information		System Information Discovery					
						Plist File Modification		System Location Discovery					
						Pre-OS Boot		System Network Configuration Discovery					
						Process Injection		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls		Virtualization/Sandbox Evasion					
						System Binary Proxy Execution							
						System Script Proxy Execution							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Unused Unsupported Cloud Regions							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

Adapted from https://www.socinvestigation.com/solarwinds-hack-mapping-the-indicators-to-mitre-attck-framework/

MITRE ATT&CK MAPPED TO GAMEPLAY FRAMEWORK

Initial Compromise	Pivot & Escalate	C2 & Exfiltration	Persistence
Reconnaissance	Privilege Escalation	Command & Control	Persistence
Resource Development	Lateral Movement	Exfiltration	
Initial Access			

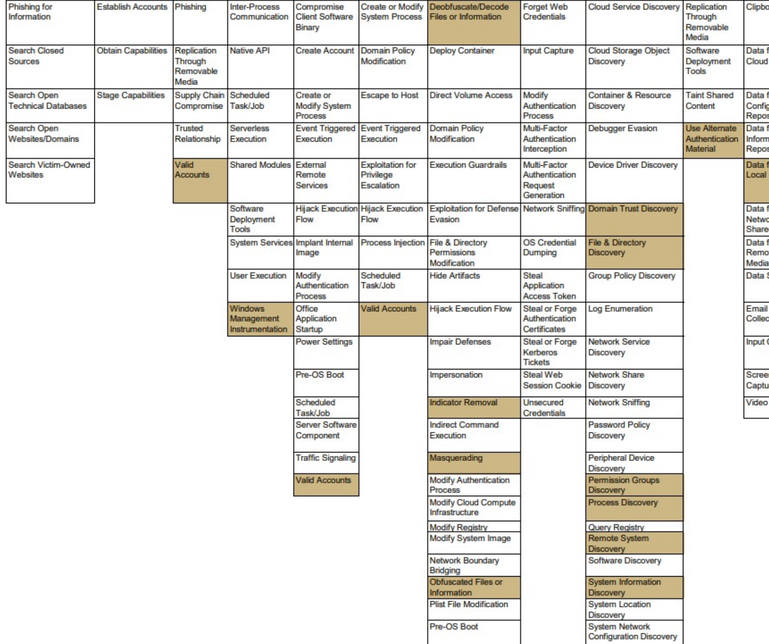
Artefacts
Execution
Defense Evasion
Credential Access
Discovery
Collection
Impact

Procedures
Crisis Management
Server Analysis
Isolation
Firewall Log Review
Security Information & Event Management (SIEM) Log Analysis
Endpoint Security Protection Analysis
User & Entity Behavior Analytics (UEBA)
Endpoint Analysis
Memory Analysis
Network Threat Hunting
Cyber Deception

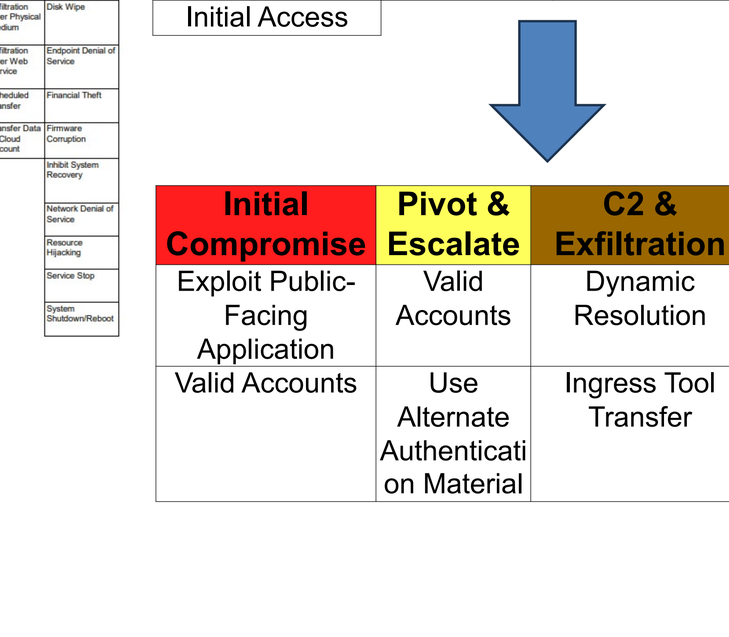
Initial Compromise	Pivot & Escalate	C2 & Exfiltration	Persistence
Exploit Public-Facing Application	Valid Accounts	Dynamic Resolution	Valid Accounts
Valid Accounts	Use Alternate Authenticati on Material	Ingress Tool Transfer	

Artefacts
Windows Management Instrumentation
Deobfuscate/Decode Files or Information
Indicator Removal on Host
Masquerading
Credentials from Password Stores
Account Discovery
Domain Trust Discovery
File & Directory Discovery
Permission Groups Discovery
Process Discovery
Remote System Discovery
System Information Discovery
Data from Local System

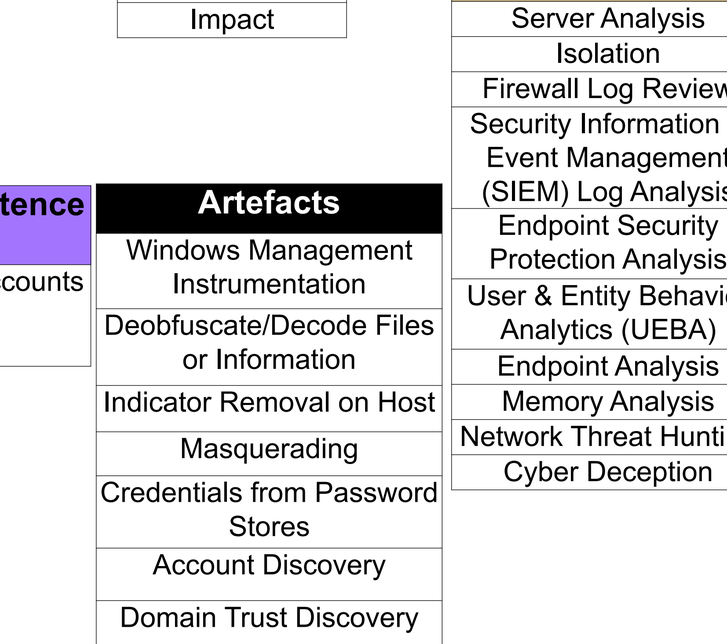
CODE BLUE GAMEPLAY



Code Blue Opening Screen



Code Blue Gameplay – Stopping Malicious Activity



Code Blue Gameplay – Using Items

PURDUE UNIVERSITY

CERIAS