Hooli Inc.

Penetration Test and Security Assessment Report

January 17, 2022

Prepared by: <tester name>

Legal

CONFIDENTIAL AND PROPRIETARY INFORMATION

Any information contained in this document is the sole property of Black Palm Security and the intended client recipient. We strictly prohibit duplication and distribution of this document or work without the permission of Black Palm Security, client, or intended party.

DISCLAIMERS

This report contains sensitive, proprietary, and confidential information concerning Hooli Inc.'s ("Hooli") infrastructure and systems. This report may contain potential vulnerabilities and the tactics, techniques, and procedures for exploiting these discovered vulnerabilities. Black Palm Security ("Black Palm") recommends that necessary precautions and proper sensitive data handling practices be taken to protect the confidentiality of the information disclosed in this document.

The information disclosed in this report is provided as-is and without warranty. Security assessments are based upon currently available information and a point-in-time analysis of known vulnerabilities and threats. As of the date of this report, the technologies, risks, threats, and exposed vulnerabilities may have changed. Engagements are limited in time and in scope, as such this report does not reflect a complete representation of your organization's risk, threat, and exposure. Severity ratings and scoring are used to prioritize the remediation of security deficiencies that may have the most significant impact on business operations.

This report was prepared by Black Palm for the exclusive benefit of Hooli and is proprietary information.

CONTACT INFORMATION

Client Information					
Company Name:	Hooli Inc. “Hooli”				
Contact Name1:	Gavin Belson	**Title:**	Founder/Lead Security Architect		
Telephone:	415-555-5555	**E-mail:**	Gavin.belson@hooli.site		
Contact Name2:		**Title:**			
Telephone		**Email:**			
Business Address:	123 Belson Drive				
City:	Palo Alto	**State:**	CA	**Zip:**	94301
URL:	https://hooli.com				

Consultant Information					
Company Name:	Black Palm Security, LLC				
Contact Name1:	Khalil Hicks	**Title:**	Principal Cyber Security Consultant		
Telephone:		**E-mail:**	secureme@blackpalm.io		
Contact Name2:		**Title:**			
Telephone		**Email:**			
Business Address:	5379 Lyons Rd. #1506				
City:	Coconut Creek	**State:**	FL	**Zip:**	33073
URL:	https://blackpalm.io				

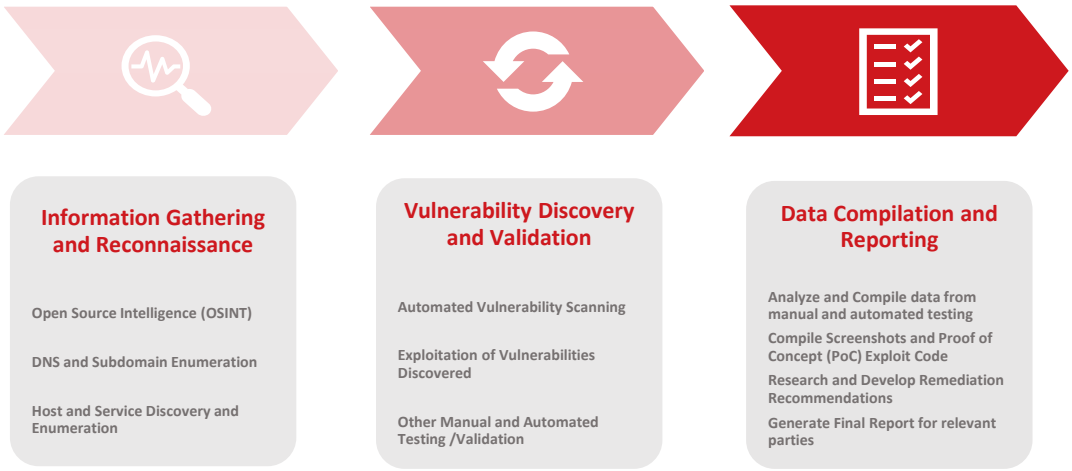
Table of Contents

Overview

To gain insight into the security posture of Hooli's network infrastructure, Black Palm conducted a Penetration Test and Security Assessment (PTSA). Our network assessment methodology incorporates a standard approach using best practices to uncover vulnerabilities and misconfigurations which can be successfully exploited or abused by a threat actor. Throughout the engagement, Black Palm utilized any available exploits and attempted to breach Hooli's environment to achieve unauthorized access. Once we breach the perimeter, our goal is to determine attack paths to access sensitive information, data, or systems. Based on our findings, in this report we will use screenshots, Proof of Concept (PoC) exploit code, and other relevant data to illustrate the impact on the business in the event an attacker can compromise Hooli's infrastructure. After the security assessment, Black Palm compiled the data, developed remediation recommendations, and generated a detailed final report to be shared with the relevant parties.

Methodology

Based on best practices and industry standards such as Open Web Application Security Project (OWASP) and Penetration Testing Execution Standard (PTES), Black Palm follows a well-defined penetration testing methodology. Our testing processes include information gathering, vulnerability scanning, attack, exploitation, and finally, reporting on our findings. We have illustrated this methodology below.



Phase	Description of Activities
Pre-Assessment	Review all data and documentation provided by Hooli personnel concerning the objectives, considerations, operation, and coordination of the PTSA.
Information Gathering (Reconnaissance)	As an initial phase, Black Palm will use both Open-Source Intelligence (OSINT) and commercial tools to gather as much data as possible on Hooli's organization. This phase incorporates two modes of testing: passive and active. The goal of this activity is to simulate what steps an adversary would take before conducting an active attack against

	an organization's internet-facing systems. Several tools will be run to conduct some of the following activities. • OSINT gathering • DNS enumeration and interrogation • Domain and Email enumeration • Host and Service Discovery • Software/Hardware Version Identification
Vulnerability Discovery and Exploitation	Systems and assets identified during the Reconnaissance phase will be further analyzed by conducting vulnerability scans. Black Palm testers will attempt to exploit any uncovered vulnerabilities which are impacting systems and assets within Hooli's infrastructure.
Data Compilation and Analysis	Collect all data from the PTSA activities. Analyze data and results to prepare for the Final Report.
Reporting	To provide a comprehensive report, Black Palm will document and/or screenshot any findings which include vulnerabilities, successful exploitation, sensitive information disclosures, or compromised user accounts during the engagement. Proof of Concept code may also be included in the report. After the engagement, Black Palm will provide a report to Black Palm on all findings and will also recommend remediation actions for the disclosed findings.

Tools

To collect data and discover as many vulnerabilities as possible during the assessment, Black Palm utilized both commercial and open-source tools and applications. These tools incorporate both manual and automated processes to access a target system. In the table below, we have listed some of the tools that we utilized during the assessment of Hooli's infrastructure.

Tool	Description

NMAP (Network mapper)	An open-source scanner used in host, service, and operating system discovery
Burp Suite	A commercial suite of tools that includes a web application vulnerability scanner used for conducting security assessments against web applications and its functionality.
Nessus Vulnerability Scanner	A commercial application used to scan target systems, analyze running services, identify known vulnerabilities, and report findings.
Metasploit	A penetration testing framework used to probe systems and exploit vulnerabilities
SQLmap	An open-source tool used to interrogate databases and test for injection points.
Nikto	A free open-source tool used to scan webservers for vulnerabilities, outdated software, and identify exposed sensitive files/directories

Scoring and Severity Ratings

Remediation of vulnerabilities and mitigating exposure to threats can be an overwhelming effort as well as an expensive one. Investing time and money into properly securing your organization's infrastructure requires careful planning. To help Hooli prioritize remediation actions, Black Palm has provided severity ratings for each finding or vulnerability.

Definition of Severities

Black Palm has classified the findings or vulnerabilities in one of 5 severity ratings: Critical, High, Medium, Low, and Informational. These severity ratings take into account the impact on the

business, level of effort or skill, and the likelihood of a successful attack leading to compromise. Below we have defined the five severity ratings which will be attached to each finding.

- **Critical** – [CVSS V3 9.0 – 10.0] - Vulnerabilities and findings with this rating can be easily exploited with very little skill or effort the exploitation of critical vulnerabilities leads directly to superuser-level access to the system or network
- **High** – [CVSS V3 7.0 – 8.9] - Vulnerabilities and findings with this rating pose a significant risk to the business. An attacker can leverage a vulnerability with little effort to gain unauthorized user-level access to the system. Under the right circumstances, an attacker may be able to leverage this vulnerability to gain superuser-level access to the system or network
- **Medium** - [CVSS V3 4.0 – 6.9] - Vulnerabilities and findings with this rating pose a moderate risk to the business. There may be some mitigating controls already in place that are preventing full exploitation or compromise. An attacker may be able to gain low-privileged access to the system or network.
- **Low** – [CVSS V3 0.1 – 3.9] - Vulnerabilities and findings with this rating pose an inconsequential risk to the business. Usually, these findings consist of information disclosure or data leakage. Although individually these findings are low, an attacker can leverage several together, and therefore increasing the risk and severity
- **Informational** – [N/A] - Findings with this rating pose no risk to the business at this time but should be evaluated later

Scope

This engagement was conducted using a Graybox approach, where Hooli personnel provided Black Palm with a list of network subnets, domains, and wireless network SSIDs. These subnets which included servers, network devices, and applications are implemented across several data centers and geographic regions. The list of subnets that were assessed during the engagement as well as the discovered SSIDs can be found in this document's Appendix.

Executive Summary

From **January 26th, 2022 – March 2nd, 2022,** Hooli requested the assistance of Black Palm's Cyber Team in performing a Network Penetration Test and Security Assessment (PTSA) on Hooli's production external, internal, and wireless networks. Black Palm's PTSA is designed to uncover and validate any deficiencies in the security posture of all networks, applications, and systems deemed in-scope for the engagement. The primary objectives of the engagement are the following:

Objectives:

- Determine Hooli's risks and exposure to ransomware attacks
- Identify vulnerabilities, misconfigurations, and security deficiencies
- Can an unauthorized party gain network access by compromising Hooli's Customer Portal?
- Can an external party gain access to back-end SQL servers and exfiltrate data?

Attack Summary:

- Unauthenticated SQL injection in the Customer Portal led to breaching Hooli's perimeter to gain access to internal systems. Data CAN be exfiltrated outside the Hooli domain.
- Application server misconfiguration in the Customer Portal can lead to compromise of the Hooli domain by an attacker or insider threat
- Black Palm's Cyber Team leveraged weak passwords to move around the Hooli domain and elevate privileges
- Can an unauthorized party gain network access by compromising Hooli's Customer Portal?
- Enumeration and attacks against the SCADA network largely failed due to firewalls, network segmentation, and other in-line security controls

The objectives that were satisfied led us to determine the overall risk of compromise of the organization's infrastructure and accessing of critical data by an attacker to be **HIGH**. Lack of input validation, misconfigurations, exposed sensitive data, and personnel cybersecurity awareness are impacting Hooli which can lead to a malicious actor gaining access to the network and/or sensitive data.

Test Summary

Using both manual testing and automated tools, Black Palm performed a full-scope security assessment to evaluate current security controls and assess the potential risk of compromise of Hooli's infrastructure. The Hooli in-scope assets can be found in the Appendix section of this document. A list of wireless networks that were in-scope can also be find in the Appendix.

Based on our findings and results of this engagement, we have provided some remediation recommendations and best practice suggestions to minimize Hooli's risk and maintain a strong security posture. These recommendations include implementing the last system updates, restricting access to network services, deploying endpoint security software, and establishing a schedule for recurring security assessments.

External

Multiple Hooli web applications and externally facing assets were interrogated and assessed during the engagement. During the testing and validation phases, there were issues identified that were deemed critical as it resulted in exposed PII and PHI data. These findings were reported to the Hooli PoC immediately and were remediated within the next day. Several applications fail to sanitize or validate input into various web application parameters leading to SQL Injections, Cross-Site Scripting issues, and potential data exfiltration.

Internal

Black Palm's Cyber Team was provided with local network access using remote connectivity to a Black Palm-provided testing laptop. After remotely connecting to the laptop, testers were able to carry out the PTSA activities against internal Hooli networks. The Cyber Team discovered applications that were vulnerable to input validation issues. Additionally, unpatched software, weak/default credentials, and insufficient endpoint security issues were impacting various systems in the HOOLI domain. We were able to leverage these vulnerabilities on the internal systems to gain access to the underlying operating system

and files. Ultimately, the Cyber Team was able to gain complete control over the HOOLI domain as Domain Administrator. With this level of access, an attacker or insider threat would be able to distribute malicious software and launch a ransomware campaign. Attempting to pivot from the internal network to the SCADA network was unsuccessful as we were continuously blocked after sending any traffic deemed malicious by the inline firewall/IPS. We were able to reach one host in the SCADA environment via HTTP but did not yield any major findings.

Wireless

Wireless testing was conducted using the same laptop for the internal testing along with USB-based Wi-Fi assessment devices. After attempting to set up rogue Access Points, de-authenticating clients, and capturing WPA-2 handshakes on the SSIDs in range, we were unable to compromise the wireless networks. Hooli is using strong cryptographic controls to protect the wireless infrastructure.

Phishing

We worked with Hooli personnel to conduct an email phishing campaign. As requested, we created a pool of random Hooli email accounts we identified using the mfa.hooli.com website. The objective of the phishing campaign was to give insight into employee cybersecurity awareness and to determine if we could gain access to employee credentials using phishing emails. On 2/24/2022, Black Palm sent phishing emails to the "in-scope" email accounts. When conducting the phishing campaign, we were able to track how many emails were opened and the number of times links were clicked. As a result of the exercise, we were able to obtain what we believe to be an Hooli employee's Azure AD credentials.

We have outlined two (2) primary attack chains or scenarios which illustrates how we obtained unauthorized access to the SQL databases and Hooli Active Directory domain during the engagement.

Attack Chain #1 – Unauthorized Access to multiple Back-end Databases

External Attacker

Black Palm Advisory Cyber Team tasked with attempting to gain access to backend databases and stored sensitive data.

Action

Cyber Team enumerates internal network looking for web applications and associated database connections.

Victim

The Cyber Team identifies an intranet application intranet.hooli.com.

External Attacker

Attacker discovered the application does not sanitize data input into application parameters.

Action

Leveraging the data validation vulnerability, an attacker uses the vulnerable web application parameters to inject malicious SQL queries. The malicious SQL queries are injected into the backend database thus allowing the attacker to dump the contents.

Captured Flag

Unauthorized database access is achieved, and sensitive data can be read or exfiltrated out of the HOOLI network.

Attack Chain #2 – Escalating AD Privileges to Domain Administrator

Internal Attacker

Simulating an insider threat or an attacker with an existing foothold on the internal network, the Cyber Team is trying to elevate privileges and move laterally through the HOOLI domain.

Action

With an established connection on the HOOLI internal network, the Cyber Team uses an open-source tool to poison local SMB communication

Victim

After receiving the poisoned SMB reply, the host system sends its AD user account and NTLMv2 hash to the tester laptop.

	**Internal Attacker** The victim's NTLMv2 hash is captured and cracked to reveal a domain password. Now with credentials, the Cyber Team is able to move laterally. Using the compromised account, the testers further enumerate the Hooli domain and discover an account with admin privileges on a host is using the same password as the compromised account. At this point, the Cyber Team uses admin privileges on a local machine to dump cached credential to uncover the plaintext password of a Domain Administrator.
	**Captured Flag** Domain Administrator credentials are obtained, and the Cyber Team (attacker) is able to move to other systems with administrator privileges.

Observations

There were security controls already in place which thwarted some of our attacks and exploitation efforts. Below, we have highlighted some of the security controls we believe are minimizing your attack surface.

- **Firewall/IDS/IPS** – Internal firewall is effectively protecting access to the SCADA network from untrusted networks. Attempting to scan this network causes the source IP to get blocked for an hour+
- **Wireless Networks** – Wireless networks are using strong enterprise-level authentication controls.
- **Admin Accounts in AD** – HOOLI is using separate user accounts for individuals that need to perform administrative duties

Security Issues

The Cyber Team identified several security issues during the engagement. Below, we have highlights some of the deficiencies in Hooli's security controls and security posture.

- **Application/Server Misconfigurations**
- **Out-of-date operating systems and insufficient patch management**
- **LLMNR is enabled in the domain**
- **SMB signing not required**
- **Weak and/or Default Passwords being used in the domain**
- **User-supplied data is not sanitized or validated before processing leading to XSS and SQL injections**
- **Password resuse present on accounts with administrative privileges**
- **Personnel Cybersecurity awareness issues can lead to compromise via phishing attacks**

Recommendations

Black Palm has analyzed the findings and developed general recommendations based on security best practices and hardening guidelines. Efforts to implement such changes would further reduce the attack surface of the organization. Our recommended remediation items include the following:

Quarterly vulnerability scans at a minimum. We recommend conducting penetration tests quarterly and deploying a vulnerability management program either internally or outsourced to a 3rd party.

Leveraging standard system and application hardening guidelines such as those found in DISA STIGs or CIS benchmarks. Following server hardening guidelines will assist with reducing misconfigurations by system administrators that may leave a system vulnerable to exploitation and abuse.

During testing, several systems and applications were identified that were end-of-life or running without the latest patches. We recommend reviewing and enhancing current patch management practices to ensure all systems are up-to-date and supported by the vendor.

We recommend conducting vulnerability scans and assessments at least quarterly to ultimately identify security gaps and determine your organization's risk of attack.

Black Palm also recommends following best practices concerning authentication. Weak authentication controls can quickly lead to initial access and lateral movement within the

domain. Hooli should enforce strong password policies included complexity and expiration. Passwords were cracked using dictionary-based password attacks. As another layer of defense, Hooli should consider a privilege access management solution.

A commercial and managed endpoint security should be implemented, remain active, and constantly updated with latest updates.

Restricting access to network services or resources to trusted sources only will mitigate unauthorized access to critical services.

Vulnerability Assessment

To quickly gain insight into Hooli's attack surface and identify vulnerabilities impacting the organization's web applications and network infrastructure, Black Palm conducted a vulnerability scan. While automated tools were running, Black Palm manually interacted with Hooli's web applications and other network services to discover potential vulnerabilities that would later be used in correlation with findings from automated scans. In the figure below, we have included a graph that breaks down the vulnerabilities we discovered by severity rating (Critical, High, Medium, Low, Informational). We were able to identify a total of 21 findings of which **2** were **Critical**, **9 High**, **6 Medium**, **1 Low**, and **3 Informational**.

This table provides a summary of vulnerabilities and issues that were uncovered during Black Palm's network penetration testing and assessment. For more information on each finding, please refer to the section Detailed Findings in this report.

Vulnerability ID	Severity	Description
HOL1	Critical	CWE-89 – portal – Stacked/Union Queries SQL Injection - Low parameter
HOL2	High	Active Directory Weak Password Policy/Password Reuse/Improper Use of Description Field
HOL3	High	Phishing/Cyber Security Awareness
HOL4	High	CWE-521 Weak Password Requirements/Default Credentials

HOL5	Medium	SMB Signing Not Required
HOL6	Medium	CWE-79 – Multiple Reflected Cross-Site Scripting (XSS)
HOL7	Informational	CWE-614/1004 Insecure Cookies

Detailed Findings

HOL1 - CWE-89 – portal – Stacked/Union Queries SQL Injection - Low parameter – CRITICAL

Description: A SQL Injection was identified in the ***Low*** parameter in the services.php page.

Risk and Scoring

Likelihood: High
Impact: High
CVSS: 9.8

Affected Host (s)

https://portal.hooli.services.php (172.17.192.118)
Parameter(s): Low

Information, Snippets, and Screenshots

The *Low* parameter on the services.php page for the customer portal application is vulnerable to SQL injection using stacked and union-based queries. User-supplied input to this parameter is not sanitized or escaped and can lead to unauthorized access to the database contents as well as dumping of password hashes that can be used for lateral movement by attackers. To duplicate the issue, an HTTP POST similar to the request below can be issued to the URL with the payload in the *Low* parameter found in the screenshot in Figure 1. After locating a vulnerable parameter, further DB enumeration and dumping can be done using sqlmap.

```
POST /services.php HTTP/1.1
Host: portal.hooli.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Origin: https://portal.hooli.com
```

Connection: close **Referer: https://portal.hooli.com/ services.php** **Upgrade-Insecure-Requests: 1** **ACTION=fetch&LOW=1&HI=1&STATUS=Active&STREET=10TH+-+ST+E%7EPALO+ALTO**

Table1: HTTP request to services.php showing body and parameters

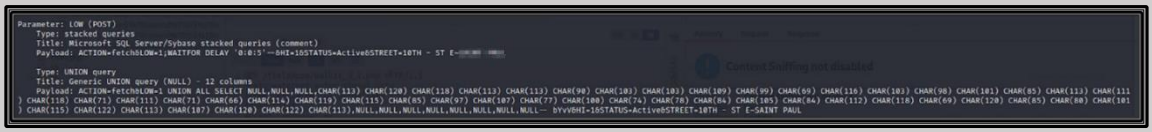


Figure 1: Customer portal Low parameter vulnerable to stacked and union-based queries

Severity

Critical

Remediation and Recommendations

The issue should be remediated by properly escaping/sanitizing any user-based input which is intended to be sent back to a database query, and prepared queries should be used where possible. Utilize PDO libraries and drivers for prepared statements.

References

CWE-89-Improper Neutralization of Special Elements in a SQL Command ('SQL Injection)
Microsoft - PDO Drivers for PHP prepared statements for MSSQL

HOL2 - Active Directory Weak Password Policy/Password Reuse/Improper Use of Description Field – HIGH

Description: Multiple security best practice violations identified in Active Directory

Risk and Scoring

Likelihood: Medium
Impact: High
CVSS: N/A

Affected Host (s)

HOL_DC1-2016 and other domain controllers

Information, Snippets, and Screenshots

Attack Chain

The Cyber Team identified several issues impacting user accounts in the HOOLI Active Directory domain. Once the testers were able to compromise a domain user account and gain a foothold on the network, the team began enumerating Active Directory users, groups, computers, and policies by dumping the AD objects using the ldapdomaindump open-source tool. This tool extracts the domain information and outputs to .json and html formats. These files can be found in attached additional files outlined in the Appendix section of this document. The team was able to crack a weak password related to the jmancini user account. These credentials were used to enumerate Active Directory and view information stored in the Description field of each AD object. Examining the Description field, the Cyber Team observed information very similar to the cracked password of the jmancini user account. Using this information, the testers were able to determine the password to the HOOLI_scheduler user account. Next, the Cyber Team was able to pivot to the 172.17.193.101 system using the credentials for HOOLIE_scheduler via RDP. This account appeared to be an administrator and permitted to RDP into the system. This account could not RDP into other systems. In attempt to elevate privileges further to move laterally to other system, the team dumped the lsass.exe process and moved the resulting file to the tester laptop for parsing. The lsass process can reveal cached passwords or those loaded in memory. After parsing the dumped process file, the Cyber Team recovered the plaintext password of the Domain Admin account (hooli\administrator). At this point, the Cyber Team gained control over the domain and could move freely to other systems.

Figure 1: Output snipper of AD User accounts dump. Password in Description field has been obfuscated

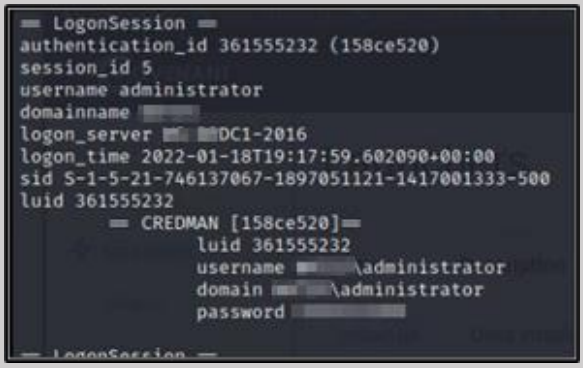


Figure 2: Proof-of-Concept of cached password being recovered by dumping lsass

Additional issues identified

- 1.1 Multiple accounts using the same password or slight variation of a common password (jmancini, hooli_scheduler, Scan_ControlOffice, hBlack Palmenefits, and biotechlab)
- 2.1 AD Password policy is not requiring the use of special characters
- 3.1 User accounts with weak passwords and/or admin privileges set to DO NOT EXPIRE
- 4.1 VNC password for Crew Board found in Description field
- 5.1 Systems storing cached passwords for administrator accounts
- 6.1 Lsass process can be dumped due to Debug permissions

Severity

High

Remediation and Recommendations

Configure the Active Directory domain to require passwords to conform to a strong complexity policy by increasing entropy. Enforce a minimum character length and enforce the use of uppercase characters, numbers, and special characters in passwords. Compliment your organization's password policy with the use of Multi-Factor Authentication if possible or not already implemented.

A password strength policy should contain the following attributes:

- Minimum and Maximum length
- Require mixed character sets (alpha, numeric, special, mixed case)
- Do not contain a user name
- Expiration
- No password reuses

Authentication mechanisms should always require complex passwords and require that they be changed periodically.

Prevent critical servers and hosts from caching passwords. This can be done by setting LSASS protected mode, Credential Manager, or adjusting registry settings for caching passwords.

Description fields should be cleared of any plaintext passwords or sensitive information. Each user account in AD should have unique passwords and passwords should be rotated periodically. Administrators can use a password safe to share passwords for systems they need to regularly access

References

Mitigating Cached Credential Issues
Windows Debug Privileges
Microsoft - Changing Cached Password Settings

HOL3 - Phishing/Cyber Security Awareness – HIGH

Description: A Hooli employee clicked on a "malicious" link and entered networking credentials during a phishing campaign conducted by Black Palm Testers

Risk and Scoring

Likelihood: High
Impact: High
CVSS: N/A

Affected Host (s)

N/A

Information, Snippets, and Screenshots

As part of the pre-assessment objectives, Black Palm's Cyber Team conducted a phishing campaign where phishing emails were sent to a subset (25) of Hooli email addresses. To conduct the phishing campaign, Black Palm's testers purchased the domain mfa-hooli.com with the idea of mimicking a legitimate Hooli subdomain mfa.hooli.com. We were able to clone the legitimate mfa.hooli.com page and host it at mfa-hooli.com. This cloned page contained a link to a fake Microsoft Azure login page and leveraged a previously discovered Cross-Site Scripting (XSS) vulnerability in the workplace.hoolie.com site. Once an employee enters credentials to the fake login page, they are captured on the back end of the Cyber Team's server. The server also captured statistics related to email clicks, email opens, and number of logins to the fake page. After analyzing the statistics, we identified potential Hooli Azure AD credentials for the john.doe account. In capturing credentials, our server was set up to only display the first 3 characters with the remaining characters masked. It should be noted that the Cyber Team decided against creating a prompt for any 2FA one-time passcodes as capturing the credentials was sufficient for this proof-of-concept phishing exercise. Additional statistics are included in the additional files covered in the Appendix section of this document.

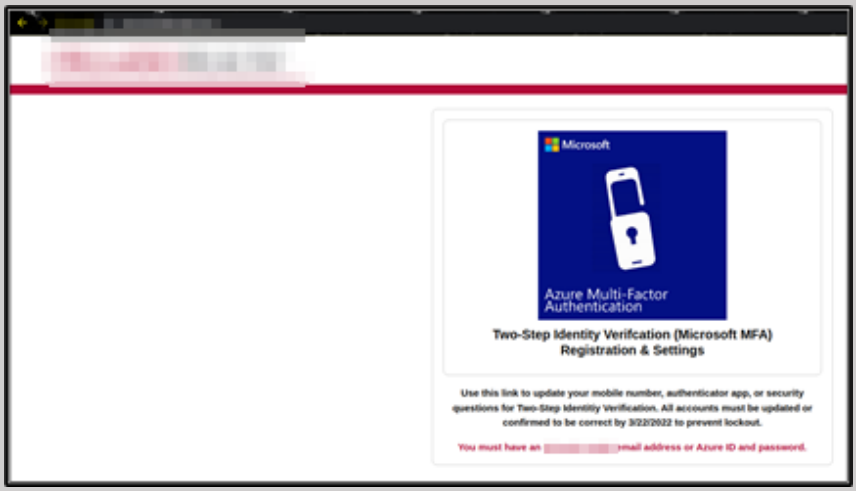


Figure 3: Cloned mfa.hooli.com page hosted on Cyber Team's domain mfa-hooli.com

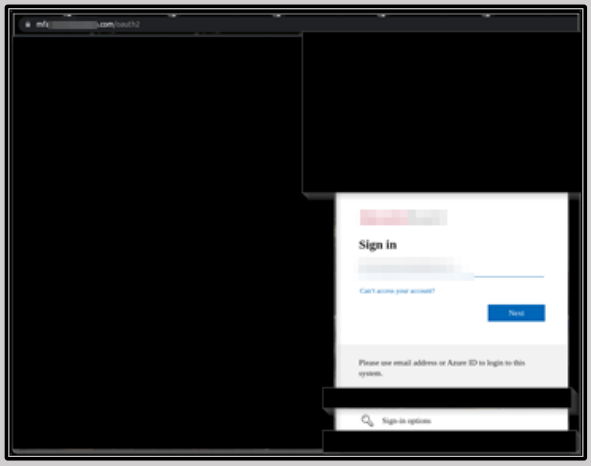


Figure 4: Fake login page where employee entered potential hooli network credentials

Severity

High

Remediation and Recommendations

If not already in place, implement or subscribe to domain monitoring or cyber threat intelligence to strengthen phishing defenses. Services that monitor your organization's domains and brands can be proactive in alerting

your IT/Cyber Teams of potential typosquatting domains that may be used in future phishing campaigns. Once a "malicious" domain is found it can be added and blocked by your email security solutions. Although we do not endorse any particular provider, there are several cyber security vendors that offer targeted proactive threat intelligence services to defend against domain and brand impersonation attacks used in phishing campaigns. We noticed a Proofpoint login page during the engagement, so we provided a reference link to their domain detection service offering.

References

Proofpoint - Domain Discover

HOL4 - CWE-521 Weak Password Requirements/Default Credentials – HIGH

Description: Default credentials are in use on deployed systems and applications

Risk and Scoring

Likelihood: Medium
Impact: High
CVSS: 7.3

Affected Host (s)

https://172.17.192.48:8000, 172.17.192.22:8000, 172.17.192.41:8000, 172.17.193.23:8000, 172.17.192.32:8000, 172.17.192.121.8000, 172.17.192.22:8000, 172.17.223.112:8443

Information, Snippets, and Screenshots

The Black Palm Cyber Team identified several Canon imageRunner devices while performing scans on the subnets permitted for the assessment. After identifying the printers and determining the listening network services, the Cyber Team successfully logged into the web interface (HTTP port 8000) on some of the devices using the default credentials: 7654321 for both the System ID and PIN. Once logged in, an attacker is able to view network and other administrative settings which could lead to additional attack paths. There may be additional Canons that are not listed and should be identified then remediated if necessary.

Additionally, a server running ManageEngine's ADAudit application (https://172.17.216.222:8443) was identified as also using default credentials. Since this application is connected to other systems within HOOLI for auditing, an attacker could gain access to valuable system logs or other information.

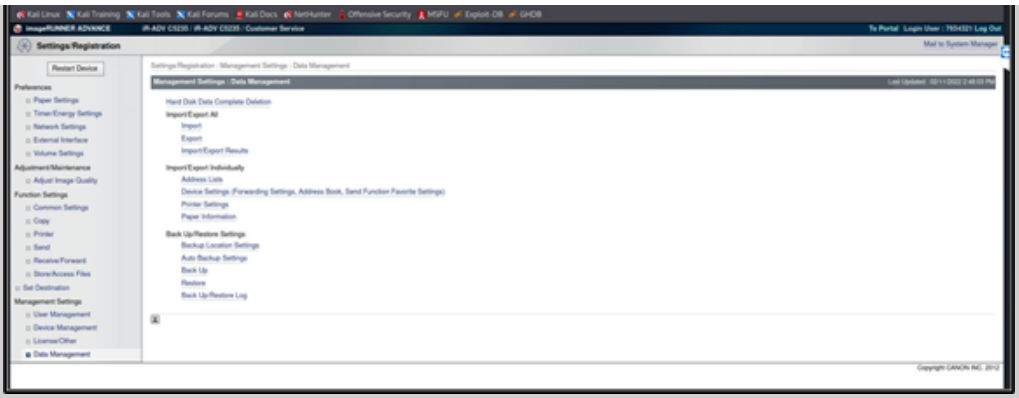


Figure 5: Logged into a Canon imageRunner with default credentials for Admin

Severity

High

Remediation and Recommendations

Ensure default credentials for both software applications and hardware devices are not configured with the default vendor credentials. Implement a password policy requiring complexity, expiry and multifactor authentication.

References

CWE-521 - Weak Password Requirements
NIST - SP 800-53 - IA-5 Security Control

HOL5 SMB Signing Not Required - MEDIUM

Description: Windows systems deployed on the domain that do not require SMB Signing

Risk and Scoring

Likelihood: Medium
Impact: Medium
CVSS: 5.3

Affected Host (s)

172.17.216.42. Multiple hosts within the in-scope subnets (Full list can be found by viewing the Nessus output files)

Information, Snippets, and Screenshots

During the physical assessment, the Cyber Team attempted to capture network credentials to be used to gain access to other hooli.com domain systems. With the Black Palm testing device connected to the 172.17.192.0/24 network, poisoned SMB replies were sent to other systems on the network. Due to the other Windows Systems not requiring SMB signing on communication, the poisoned SMB replies from the tester laptop led to the 172.17.216.142 host sending its NTLMv2 hash to the tester laptop. The Black Palm Cyber Team was able to capture the hash for offline cracking to reveal a weak password, one that was short and did not contain any special characters. The Cyber team was able to validate these credentials (hooli\jmancini) by attempting to log into other systems via SMB, RDP, and WinRm. Although the user did not have access to RDP to systems, the account was used to enumerate the entire Windows Active Directory (AD) domain to pull users, groups, policies, and windows networks shares. Also, some hooli intranet pages required authentication, and we were able to use these credentials to enumerate additional pages. Some of the output files of the AD enumeration are included in the Appendix section in hopes it can be used for reference, AD auditing, and remediation efforts. If an attacker is able to capture hashes from user accounts with elevated privileges on the domain, this issue can have severe consequences.

Severity

Medium

Remediation and Recommendations

Enabling SMB signing and secure SMB communications may not be feasible across the entire domain but should be evaluated to mitigate against man-in-the-middle and poisoning attacks. We realize this is a hooli facility that may have legacy systems or infrastructure that will not work properly with SMB signing being required so necessary research should be done before implementation. The process for enabling SMB signing via Group Policy is referenced in the links below

References

Microsoft - Overview of SMB Signing
Microsoft - Require SMB Signing Signatures
Nessus - SMB Signing

HOL6 - CWE-79 – Multiple Reflected Cross-Site Scripting (XSS) - MEDIUM

Description: The Hooli intranet application does not sanitize input to various parameters resulting in XSS

Risk and Scoring

Likelihood: Medium
Impact: Medium
CVSS: 5.3

Affected Host (s)

https://intranet.hooli.com, https://intranet-dev.hooli.com

Information, Snippets, and Screenshots

Multiple parameters on the intranet and intranet-dev sites are vulnerable to cross-site scripting. These sites fail to properly validate input within the vulnerable parameters, allowing for the injection of malicious JavaScript and HTML.

This vulnerability can allow an attacker to chain XSS attacks with other attacks to hijack sessions or gain access to systems. To duplicate this issue, a user can use any one of the payloads below as input to the vulnerable parameters.

show, <img src=x onerror=alert(1)>, <audio src/onerror=alert(1)> , "><audio src/onerror=alert(1)>, <audio src/onerror=alert(document.cookie)>, <script>alert(1)</script>

Table2: Sample XSS payloads that can be used as input to reproduce XSS vulnerability

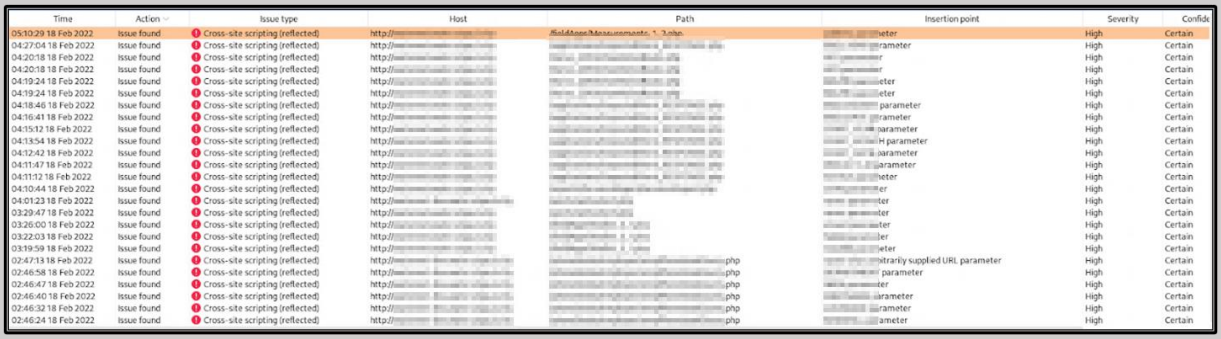


Figure 6: Output from testing tool Burp Suite showing multiple parameters in intranet are vulnerable to XSS

Severity

Medium

Remediation and Recommendations

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks
can be prevented using two layers of defenses:
Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input that fails the validation should be rejected, not sanitized.
User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities

(< > etc.).
In cases where the application's functionality allows users to author content using a restricted subset of HTML
tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to
parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.
Implement a Web Application Firewall (WAF) to look for malicious characters or use regular expressions (Regex) within the application to look for malicious patterns/characters. Regex can be used to whitelist only allowed patterns as well as blacklist commonly used XSS bypass payloads. Placing a WAF in a DMZ or internally a in front of web applications offers enhanced protection against compromised networks and insider threats.

References

CWE-79 - Improper Neutralization of Input During Web page Generation ("Cross-Site Scripting")

HOL7 - CWE-614/1004 Insecure Cookies- INFORMATIONAL

Description: The application is insecurely setting cookies

Risk and Scoring

Likelihood: N/A
Impact: N/A
CVSS: N/A

Affected Host (s)

https://maps.hooli.com/GPS/Query.php

Information, Snippets, and Screenshots

The webserver does not set the PHPSESSID with the “secure” or “httponly” flags. This can allow an attacker to read the contents of the cookie over an insecure HTTP session using JavaScript. This usually chained with a Cross-Site Scripting vulnerability

Severity

Informational

Remediation and Recommendations

Configure the server to set the PHPSESSID cookie with secure and httponly attributes

References

CWE-614 - Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
CWE-1004 - Sensitive Cookie Without 'HttpOnly' Flag

Conclusions

After extensive testing of the Hooli external, internal, and wireless networks, Black Palm has found internal database contents can be accessed by malicious threat actors. Therefore, we have determined an overall risk and likelihood of compromise with the attacker gaining unauthorized access to databases and ransomware attacks on the internal networks as **HIGH**.

To address one of Hooli's main concerns we performed extensive testing to identify outdate software and potential attack vectors to access sensitive data within the Hooli infrastructure.

Employing security best practices can help greatly decrease your organization's attack surface. These practices include installing the latest security patches, following system hardening guidelines, restricting network access to services, and implementing endpoint security capabilities. There are also other options available to assist in being proactive in securing your environment, such as subscribing to cyber threat intelligence services and scheduling quarterly security assessments/audits.

Appendix

Additional Engagement Files

HOOLI -Pentest-2022.7z

- HOOLI-192-Authenticated.nessus
- HOOLI -192-Authenticated.pdf
- HOOLI -213.nessus
- HOOLI -213.pdf
- HOOLI -216.nessus
- HOOLI -216.pdf
- HOOLI -223.nessus
- HOOLI -223.pdf
- domain_computers.grep
- domain_computers.html
- domain_computers.json
- domain_computers_by_os.html
- domain_groups.grep
- domain_groups.html
- domain_groups.json
- domain_policy.grep
- domain_policy.html
- domain_policy.json
- domain_trusts.grep
- domain_trusts.html
- domain_trusts.json
- domain_users.grep

- domain_users.html
- domain_users.json
- domain_users_by group.html

Hostnames In-Scope

Hostnames Tested	
portal.hooli.com	Intranet.hooli.com
docs.hooli.com	*.hooli.com

IP Subnets and Wireless SSIDs In-Scope

In-Scope External Subnets	In-Scope Wireless SSIDS/Hostname
326.77.75.39	SCADAControlAP002
356.77.75.89	Hooli-Guest
363.31.159.112	Hooli-Corp
In-Scope Internal Subnets	SpecialEvents
172.17.203.0/22	DevLab
172.17.192.0/23	
172.17.216.0/23	
172.17.223.0/24	
172.17.213.0/24