DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

DETECTION AND RESPONSE GAME

PERSISTENCE

SSH AUTHORIZED KEYS

The hacker adds their own public key to the SSH authorized_keys file to maintain persistence.

MITIGATION

Restrict access to the authorized_keys file

DETECTION

Monitor the authorized_keys file

LOGON SCRIPT

The hacker uses the Windows logon script which is executed when a certain user logs in to achieve persistence.

MITIGATION

Proper permissions for registry hives

DETECTION

Monitor for changes to registry values

SYSTEM FIRMWARE

The hacker overwrites the BIOS firmware with custom updates that allow him persistence.

MITIGATION

Regular BIOS and EFI patches

DETECTION

Monitoring for system firmware manipulation

DOMAIN ACCOUNT

The hacker creates a new domain account that he can access at any time.

MITIGATION

Multi-factor authentication

DETECTION

Monitor for account creation without naming scheme

SCHEDULED TASK

The hacker uses at.exe to execute malicious code at specified intervals.

MITIGATION

Run tasks under the authenticated account

DETECTION

Monitor for svchost.exe executions

BOOTKIT

The hacker installs a bootkit that looks like a Microsoft Net.exe utility and enables him to deliver backdoors.

MITIGATION

Secure or trusted boot process

DETECTION

Integrity checking on MBR and VBR

PORT KNOCKING

The hacker sends connection attempts to closed ports in a certain order which leads to the opening of a port.

MITIGATION

Stateful firewalls

DETECTION

Monitor for extraneous packets

EXTERNAL REMOTE SERVICES

The hacker uses Windows Remote Management with a valid account to have access to the systems at any time.

MITIGATION

Block unnecessary remote services

DETECTION

Monitor for access outside of normal business hours