National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

NSA Methodology for Adversary Obstruction

August 2015
MTR U/OO/813823-15

NSA Methodology for Adversary Obstruction

Threats and Attack Lifecycle

From nation states to terrorist groups to loose hacker collectives and organized crime, the intent and capability to conduct malicious cyber activity against the United States Government (USG) and partner networks is clear and improving. For most of these networks, the question is not if a system will be compromised but when. Therefore, the most effective and least costly way to defend a network is analogous to fire prevention and response. By pre-posturing defensive capabilities and response processes prior to the fire or intrusion breaking out, the issue can be contained and fixed; greatly increasing the survivability and security of the network.

Regardless of the classification or sensitivity of information managed on your networks, proven best practices for minimizing your risk of becoming a victim or reducing the impact if you are victimized involve basic actions that impede the objectives of the intruder in each of the three main phases of an intrusion. The phases are *Access, Persistence,* and *Control* and they leverage common threat vectors.

Access (A) refers to how an intruder connects to your network, often enabled by poor basic security practices by employees. The intruder then aims for *persistence (P)* by creating a "foothold" in the network to allow a sustained presence. All of these actions are focused on gaining *control (C)* to achieve the final objective, whether it is to interfere, monitor, steal or alter data, deceive, disable or destroy.

Threat vectors include:	Phases
- **Spear phishing**	A
- **Improperly configured servers or servers with unpatched software vulnerabilities**	A
- **Malicious software**	A, P, C
- **Stolen, legitimate credentials**	A, P, C
- **Destructive/data manipulation attacks**	C
- **Insider threat**	A, P, C
- **Social Engineering**	A
- **Vulnerable networks connected to the target network that enjoy a trust relationship**	A, P
- **USG personnel, at home and at work**	A, P, C

Defendable Network Methodology

A defendable network is one which provides the network defense team a chance to quickly and effectively detect, counter, and expel an adversary. The methods NSA recommends greatly increase the

effort and cost a threat actor expends to break into a network and by doing so decreases the tools, tactics, and procedures said threat actor can utilize.

The ability to create a defendable network resides in ensuring the following focus areas are implemented:

- **Generate a plan to respond and ensure it is fully implemented without exceptions.**
- **Reduce the attack surface** to reduce external attack vectors into the network
- **Harden devices** to reduce internal and external attack vectors into the network
- **Implement Credential Protections** to degrade the adversaries' ability to maneuver on the network
- **Align defensive resources** to improve detection of and response to adversary activity
- **Segregate networks and functions** to contain damage when an intrusion occurs
- **Develop a culture of cyber professionalism, to include leaders who set expectations**

Under each of these groups there are multiple, tailored options for satisfying the focus area. By utilizing the tailored mitigations within these groups, network administrators and incident response teams can measurably increase their network's resilience and their abilities to respond to adversarial attacks.

Targeted Mitigation Techniques

The following list of mitigations satisfy the aforementioned focus areas and are the basis for taking a network from being highly exploitable to a more effectively defended state. Along with the below, there is extensive reference information and there are experienced resources available from the Department of Homeland Security, the National Institutes of Standards and Technology, the National Security Agency and the United States Cyber Command to help CIOs, CISOs, or information technology leadership customize a plan of action.

1. ***Protect Credentials*** [i,ii]***:*** By implementing the following credential protections, the threat actor's ability to gain highly privileged account access and move throughout a network is severely hampered.
    a. ***Implement Least Privilege:*** Least privilege is the limiting of rights assigned to each group of accounts on a network to only the rights required for the user, as in a normal user is only granted user level privileges and cannot perform any administrative tasks such as installing software.
    b. ***Restrict Local Accounts:*** By restricting the usage of local accounts, especially local administer accounts, you are able to reduce the amount of usable credentials found within a network. When utilizing local accounts, passwords and their corresponding hashes are stored on the host and are more readily available for harvesting by an adversary who seeks to establish persistence. Adversaries are known to use this information to move across the network through Pass the Hash.
    c. ***Limit Lateral Movement:*** This mitigation reduces the adversary's ability to go from exploiting one machine to taking over the entire network. Host firewall rules, Active Directory structuring, and/or Group Policy settings, can be tailored to stop communications between systems and increase the survivability and defensibility of a network under attack.

d. ***Admin Access Segregation:*** Once an adversary gains administrator credentials, especially domain administrator credentials, the network becomes wide open to their malicious activity. By decreasing the surface area where admin credentials can be stolen, through restricting where and when administrators can use their accounts and what they can use their accounts for, the threat actor will have a much harder time fully compromising a network. Having different passwords and credentials for user, local administrator, and domain administrator accounts prevents an adversary from reusing a stolen credential from one to gain more access.

e. ***Admin Access Protection:*** Using unencrypted protocols across the network where credentials, especially administrative credentials, are sent in the clear enables an adversary to grab them in transit and reuse them. Be sure to use encrypted protocols (e.g., HTTPS, SSH, RDP, SFTP, etc.) for all management connections where credentials are passed, and disable the use of unencrypted protocols (e.g., Telnet, FTP, HTTP, etc.).

f. Ensure Administrative Accounts do not have email accounts or Internet access[iii]

g. ***Utilize Strong Authentication***[iv]***:*** *By enforcing multi-factor authentication (e.g., using smart cards), especially for privileged account and remote access (e.g. VPNs), you dramatically reduce when and where stolen credentials can be reused by an adversary. Until then, create, enforce, and maintain strong password policies across the organization. The use of strong password policies must be mandated for all users and is especially critical for administrator accounts and service accounts. Passwords should be complex and contain a combination of letters, numbers, and special characters, and they should be of a sufficient length (greater than 14 characters); require regular password changes for all administrative and other privileged account; and prevent the reuse of usernames and passwords across multiple domains and/or multiple systems.*

h. ***Log and Monitor Privileged Admin Account Usage***[v]***:*** *Implementing logging and monitoring capabilities on privileged accounts can provide insight to system owners and incident response professionals of account misuse, potential compromise, or unauthorized accounts by malicious actors. For instance, it may be discovered that a domain admin is logging in at 2200 every night even though that admin is done working for the day and gone from the building. This mitigation would also enable discovery of any privileged admin accounts that were created/deleted/modified by the actor for persistence.*

i. ***Log and Monitor Use of Administrative Tools:*** *Non-administrative use of built-in OS administrative tools should be locked down in accordance with applicable guidance and hardening policies. Use of these tools, such as Windows® PowerShell®*[1] *and Windows Management Instrumentation Command-line (WMIC), should be logged and monitored to help enable early detection of a compromise. Though administration activities take place on a constant basis, certain behaviors, or sets of activities, in concert with others, are suspicious and can lead to a discovery of intrusion. For example, the 'ping' command by itself has legitimate uses. However, the 'ping' command, followed by a PowerShell command from one workstation to another is very suspicious.*

[1] Windows®, Windows PowerShell® are registered trademarks of Microsoft Corp.

2. Segregate Networks and Functions:

a. ***Know your Network***[vi]***:*** *Enterprise networks often become unmanageable leading to inefficient administration and ineffective security. In order to have any sort of control over your network, you first need to know what and where everything is and does. Ensure information about your network is documented and is updated regularly. Create an accurate list of ALL devices and ALL protocols that are running on your network. Identify network enclaves and examine your network trust relationships within and between those enclaves as well as with external networks to determine whether they are really necessary for your organization's mission.*

b. ***DMZ Isolation:*** *By ensuring that the DMZ is properly segregated both through physical and logical network architecture and admin/user accounts, a network owner can greatly decrease the external attack surface. Since webservers and corresponding databases usually sit in this location and are also externally accessible, they regularly are the first target during CNO. If these systems are compromised and the DMZ is not configured properly or at all, it could mean the loss of the entire enterprise.*

c. ***Network Function Segregation*** [vii]***:*** *A network owner should implement a tiered system when determining the switching within a network. This way the lower security systems, like user workstations or machines with email and internet access, cannot insecurely communicate with higher security systems like domain controllers and other member servers. This can be achieved through multiple methods including VLANs, physical network topologies, and Firewall rule sets. In the same vein, networks need to apply the same segregation principle to the various tiers of accounts within a network, ensuring highly privileged accounts cannot access lower security tiered systems and low privilege accounts cannot access higher security tiered systems.*

d. ***Limit Workstation-to-Workstation Communications*** [viii]***:*** *Pass-the-Hash (PtH) and other forms of legitimate credential reuse are serious vulnerabilities existing in all environments that implement Single Sign-on. PtH allows an attacker to reuse legitimate administrator or user credentials to move from system to system on a network without ever having to crack a password. Once an attacker compromises a single host, s/he will typically reuse stolen hashed credentials to spread to other systems on the network, gain access to a privileged user's workstation, grab domain administrator credentials, and subsequently take control of the entire environment.*

Limiting workstation-to-workstation communication will severely restrict attackers' freedom of movement via techniques such as PtH. In general, limiting the number and type of communication flows between systems also aids in the detection of potentially malicious network activity. Because there are fewer allowed communication paths, abnormal flows become more apparent to attentive network defenders.

e. ***Perimeter Filtering:*** *Perimeter filtering refers to properly implementing network security devices, such as proxies, firewall, web content filters, and IDS/IPS. The intent is to block malicious traffic from reaching a user's machine and provide protection against data exfiltration and command and control. The default stance should be to deny by default and exceptions should be reassessed regularly.*

f. ***Use Web Domain Name System (DNS) Reputation*** [ix]***:*** *Various commercial services offer feeds rating the trustworthiness of web domains. Enterprises can protect their hosts by*

screening web accesses against such services and redirecting dangerous web requests to a warning page. Inspection can be implemented at either the web proxy or browser level.

g. ***Restrict or Prevent Remote Admin Access:*** *Prior to an intrusion, remote access should be severely restricted and highly monitored. Once an intrusion is detected, all remote administration should be completely disallowed. Not only does this clear up the network traffic coming and going from a network it also allows the network defenders to determine that the remote administration activities are malicious and better track and block them.*

3. ***Implement Host Intrusion Prevention System (HIPS) Rules*** [x]***:*** *Standard signature based host defenses are overwhelmed by exploit kits that continually morph attack components. HIPS technology focuses on threat behaviors and can better scale to entire sets of intrusion activities. For an enterprise with a well configured and managed network, HIPS can be tuned to learn and allow normal network functionality while flagging anomalies characteristic of intrusions.*

4. ***Centralize logging of all events:*** By pulling all of the system logs (such as Windows Event or Error logs, and any logs from security devices, such as SNORT, HIPS or firewall rule hits, as a few examples) into a centralized location that protects it from tampering and enables analytics, the network admin and intrusion response team would be able to more efficiently detect and understand the tools, tactics, and procedures of the adversary. Using this information then increases the responder's ability to effectively corner and expel the adversary. This paper does not detail the entirety of logs that could be aggregated, however, specific recommendations of particular logs that should be targeted for aggregation can be obtained via consultation with the network's Computer Network Defense-Service Provider (CND-SP) or with any of the organizations listed in the introduction to this section.

5. ***Take Advantage of Software Improvement*** [xi]***:*** Apply patches for vulnerabilities as soon as they are released by the vendor. Upgrade as new versions of applications, software and operating systems become available. Delaying or ignoring patches for vulnerabilities considerably increases the chance of systems being exploited, in particular Internet/public facing systems (VPN, web, email servers). Open source research has shown that a working exploit is often available on the same day vulnerabilities are publicly disclosed, making it imperative to patch immediately. Vendors typically perform extensive testing of patches prior to release so misconceptions about negative effects on systems are often overstated. The cost of pre-deployment testing by the enterprise is minisculecompared to the potential costs incurred from a security breach. Application deployment and updating is becoming increasingly automated. Many operating systems and applications provide automatic update features to minimize the human factor.

6. ***Implement Application Whitelisting*** [xii, xiii]***:*** Application whitelisting is the configuring of host system to only execute a specific, known set of code. Basically, if a program or executable code, such as a piece of malware, is not included in the whitelist it's never allowed to run. Location-based directory application whitelisting provides significant security improvement with less ongoing maintenance overhead than most other forms of application whitelisting.

NSA Methodology for Adversary Obstruction

7. ***Install and correctly use EMET*** [xiv]***:*** One of the frequently used tactics by an adversary is to initially infect a host through spear-phishing and drive-by's/water-holing websites. The best way to counter this initial exploitation is through the implementation of an anti-exploitation tool, such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET). These tools can render useless entire classes of malware and malicious TTP instead of eliminating one piece of malware at a time; an enormous boon to a network's security.

8. ***Public Services Utilization:*** Enterprises are embracing the use of public services such as Cloud Storage and Social Networking Sites (SNS) as they offer capabilities not available with traditional software. These services also introduce a new set of vulnerabilities that must be considered. Open source reporting has shown these services to be an increasingly used vector for both malware delivery and data exfiltration. Establish a comprehensive public services policy and framework. Discover and document all the Cloud and Social Networking Services used and establish a policy that includes IT sanctioned sites permitted and prohibited within the enterprise as well as what is considered acceptable use. Integrate traffic logs to/from these sites into your centralized logging environment and implement analytics to detect and alert on potentially suspicious or abnormal traffic that could be indicative of a compromise.

9. ***Use a Standard Baseline*** [xv]***:*** Implementing a uniform image with security already baked in and standardized applications affords the incident response team the ability to look at exploited machines and distinguish what is malicious vs. allowed. It also ensures that each machine on the network is at least at a certain level of security prior to further customization for a user's needs. Within the DoDIN this can be satisfied through the Unified Master Gold Disk, maintained and distributed through DISA.

10. ***Data-at-Rest and Data-in-Transit Encryption:*** Implementing encryption for both data at rest and data in transit ensures that what is meant to be kept private stays private, whether it is stored on a disk or moving across a network. It means that exfiltration and espionage attempts can be thwarted since a threat actor cannot access the information.

11. ***Use Anti-Virus File Reputation Services*** [xvi]***:*** Most of today's host security products augment their product's core host controls with intelligence from cloud-hosted threat databases. In order to gain the most complete threat picture, organizations need to leverage these threat intelligence clouds.

Disclaimer

NSA Methodology for Adversary Obstruction

Contact Information

Industry Inquiries
410-854-6091
bao@nsa.gov

Client Requirements and General Information Assurance Inquiries

IAD Client Contact Center
410-854-4200
email: IAD_CCC

LINKS TO REFERENCES:

[i] Reducing the Effectiveness of Pass-the-Hash at: https://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

[ii] Also see the Microsoft publication on PtH: Mitigating Pass-the-Hash (PtH) and Other Credential Theft Techniques at http://www.microsoft.com/en-us/download/details.aspx?id=36036

[iii] Ensure administrative accounts do not have email accounts or Internet access; see: https://www.nsa.gov/ia/_files/factsheets/Final_49635Noninternalsheet91.pdf

[iv] Hardening Authentication, at https://www.nsa.gov/ia/_files/factsheets/IAD_HardeningAuth_PrintFile.pdf

[v] Spotting the Adversary with Event Log Monitoring: https://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Event_Log_Monitoring.pdf

[vi] Please see IAD's Manageable Network Plan Teaser at: https://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlanTeaser.pdf

[vii] Segregating Networks and Functions at: https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf

[viii] Limit Workstation to Workstation Communications: https://www.nsa.gov/ia/_files/factsheets/I43V_Slicksheets/Slicksheet_LimitingWtWCommunication_Web.pdf

[ix] Web Domain Name System Reputation Services at: https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_WebDomainNameSystemReputation_Web.pdf

[x] Host Intrusion Prevention Systems at: https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_HostIntrusionPreventionSystems.pdf

[xi] Take Advantage of Software Improvements at: https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SoftwareImprovements_Print.pdf

[xii] IAD's Application Whitelisting Slicksheet: https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_ApplicationWhitelisting_Standard.pdf

[xiii] Application Whitelisting Trifold: https://www.nsa.gov/ia/_files/factsheets/Application_Whitelisting_Trifold.pdf

[xiv] IAD's Anti-Exploitation Slicksheet:
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_AntiExploitationFeatures_Web.pdf

[xv] Secure Host Baseline at:
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SecureHostBaseline_Web.pdf

[xvi] Anti-Virus File Reputation Services at:
https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_AntivirusFileReputationServices.pdf