Windows Privilege Escalation Part 2: Domain Admin Privileges

Introduction This is the second part of a two-part series that focuses on Windows privilege escalation. The previous post (Part 1) provided an overview of 10 vectors that could be used to obtain local SYSTEM and administrative privileges from an unprivileged user account. This post focuses on obtaining domain administrative privileges from a local administrator or domain user account.
Escalation Techniques Once the initial steps have been taken to obtain local administrative access on a Windows operating system, the natural next steps are to gain domain user and domain administrative privileges. Many of the methods for gaining domain administrative privileges are the same as or similar to those used to gain local administrative privileges. So, don't forget to try out some of the techniques used in the last post. Using the escalation vectors listed below, penetration testers often gain unauthorized access to all kinds things like applications, systems, and everyone's favorite–domain administrator accounts.

1. ***Crack Local LM Password Hashes***
   A long time ago, in an LAN far away, there lived a strong password stored as an LM Hash. The penetration testers of the LAN tried brute force and dictionary attacks, but it took weeks to crack the single LM password hash. The IT administrators were pleased and felt there was security across the LAN.I think that we've all heard that bedtime story before, and it's less true now than ever. Using tools like Rainbow Tables, LM password hashes can be cracked in a few minutes instead of a few weeks. Tools like these allow penetration testers to quickly crack local, service, and in some cases domain accounts. Service and domain accounts can be especially helpful for the reasons below. Service Accounts Local service accounts are commonly installed using the same passwords across an entire environment. To make matters worse (or better, depending on your perspective), many of them allow interactive login, and in extreme cases are installed on domain controllers with Domain Admin privileges. Service accounts may seem trivial at first glance, but make sure to give them the attention they deserve; it usually pays off in the end. Domain Accounts Domain accounts are nice to have for a number of reasons. First, they typically provide a penetration tester with enough privileges on the domain to look up other user accounts to target in future attacks e.g., domain administrators. Second, they typically provide testers with access to shares that haven't been locked down properly. Finally, they provide a means for logging into other systems such as domain controllers and member servers. To be fair, most small to mid-sized companies are getting better at only allowing the storage NTLM v2 password hashes, but it seems to be something that a lot of large companies are still struggling with. So don't forget to dump and crack those hashes. Although it's not always that easy, sometimes it is.
2. ***Impersonate Users with Pass-The-Hash Toolkit and Incognito***
   Have you ever wanted to be someone else? Well, now you can. With local administrator rights to a system you can impersonate any logged-on user with the Pass-The-Hash Toolkit or Incognito tool. Both of the tools provide the functionality to list logged-on users and impersonate them on the network by manipulating LSA (Local Security Authority) logon sessions. In most cases this means domain user or administrator access. I know it's exciting, but don't forget to keep in mind that anti-virus and anti-malware products typically protect LSA sessions from manipulation, so they must be disabled before the tools can be used. Or for the more ambitious, modify the executable source code and recompile each program to avoid detection

3. ***Install a Keylogger***
   Installing key loggers on systems is a time-honored tradition practiced by hackers for generations. They can be a great vector for gathering passwords to systems, applications, and network devices. Historically, they have been pretty easy to create and conceal. However, I still recommend disabling anti-virus services, or at least creating an anti-virus exception for certain relative files types (for example, *.exe files) before installing a key logger.

   Key loggers are relatively easy to program and obfuscate, but if you're not up to task of making your own, there are plenty of open-source and commercial options available on the Internet. Just keep in mind that most installations require local administrative access.

   Happy logging!

4. ***Install a Sniffer on the Localhost***
   Installing a network traffic sniffer is another vector of attack that has been practiced since the dawn of the Internet. As you might expect, sniffers can also be a great vector for gathering passwords to systems, applications, and network devices. Unfortunately, this is another one that will require local administrative access. It's needed to install the WinPcap driver used to perform promiscuous sniffing of network traffic.Typically, the only traffic sniffed on today's networks is broadcast traffic and traffic flowing to and from the localhost. Apparently, somewhere along the line most companies figured out that using routers and switches was a better idea than daisy-chaining hubs. Even with this limitation, sniffing traffic on the right server can yield great results, especially with the popularity of unencrypted web applications that authenticate to Active Directory. There are number of great open-source and commercial sniffing tools out there. If you don't mind using a GUI interface, then I recommend the full WinPcap install and Wireshark. Wireshark is made for a number of platforms, has lots of great options, and is free. Alternatively, if you prefer a stealthier method of installation, I recommend using WinDump (Windows port of TCPDump) and the WinPcap distribution that comes with the Windows Nmap zip package, because it can all be installed silently without a GUI.
5. ***Sniff from Network Devices***

   A few of the most common vectors of attack overlooked by penetration testers are routers and switches. Typically, both device types can copy network traffic and direct it anywhere on the network for sniffing. In some cases testers can even monitor and view traffic right on the device itself. Oddly enough, many companies don't change the default passwords and SNMP strings that protect the management of such devices. Unfortunately for penetration testers, some companies only allow read access to device configurations, but have no fear. Many of the same devices will accept and reply to SNMP queries for the TFTP image paths. Most TFTP servers don't use authentication, which means the image can be downloaded and the device passwords can be read or cracked to gain full access.

6. ***Perform Man in the Middle (MITM) Attacks***Ok, you caught me, I lied about only being able to sniff network traffic coming to and from the localhost. However, it was for good reason. I wanted to make the distinct point that MITM attacks are typically required to sniff network traffic flowing between remote systems on a LAN. One of the easiest ways to conduct MITM attacks is ARP spoofing. It's a simple attack, there are lots of free tools that support it, and many companies still don't protect against it. Explaining how ARP spoofing works will not be covered in this article, but I strongly suggest reading up on it if you are not familiar.There are a lot of ARP spoofing tools out

there, but I don't think that I'm alone is saying that Cain & Abel is a my favorite. It makes initiating an ARP spoofing attack as easy as using Notepad. In addition, it also gathers passwords for at least 20 different applications and protocols while sniffing. The fun doesn't stop there; it also intercepts HTTPS, RDP, and FTPS communications, making it extremely valuable even against encrypted communications. In some cases MITM attacks can be more effective than all of the other escalation vectors. It can take time to sniff the right password, but on the bright side it can be done while you're conducting other attacks – Hooray for multi-tasking!

7. ***Attack Domain Controllers Directly***

   If domain controllers are in scope for your penetration test, then I recommend starting there. Gaining almost any level of user access on a domain controller typically leads to domain administrator access. If SYSTEM-level access is not immediately obtained via missing patches, weak configuration, or coding issues, then (in most cases) using the other vectors of attacks listed in Parts 1 and 2 of this series should allow you to escalate your privileges.

   Remember, SYSTEM-level access on a domain controller is equivalent to domain administrator access. SYSTEM access can be easily leveraged by penetration testers to create their own domain administrator account.

8. ***Online Resources***
   Never underestimate the power of public information. Public registrars are a great place to find company contacts, business partners, IP Addresses, and company websites. All of which can lead to valuable information such as internal procedures, configuration files, patch levels and passwords. There have been many occasions when I've found internal installation procedures containing passwords on company websites, forums, and blogs.Once passwords have been found, use externally accessible login interfaces to gain access to systems and sensitive information.
9. ***Buy Used Computer Equipment***
   Going once, going twice, sold to the highest bidder. Sensitive information like social security numbers, credit card numbers, and account passwords are being sold every day in a neighborhood near you. Companies sell their used POS terminals, workstations, servers, and network equipment all the time. However, what many of them don't do is take the time to securely wipe the disks. As a result, sensitive data is flying around Ebay, Craigslist, and your local auction house. I've personally seen POS terminals storing thousands of card numbers in clear text. Even worse, I've seen firewalls with configurations that allow the buyer direct VPN access to the corporate network of the company that sold the devices.
10. ***Social Engineering***
    Sometimes the easiest way to gain domain administrative privileges is to never touch a computer. If your part of the security community you already know what social engineering is, and what the common vectors are. However, this may be a new concept for some people, so I'll provide a brief overview. In a nutshell, social engineering is the process of manipulating people into providing information or performing actions. Although there are many types of social engineering attacks, there are three primary vectors: in person, phone-based, and the most common, email phishing. At this point you may still be wondering how this is going to result in domain administrator access. So I've provide an example for each vector below. In Person Who wants to play dress up? One of the easiest ways to gain access to systems and networks is to pose as an IT vendor or internal IT staff member. Showing up unannounced can be tricky, but with a good back-story the IT director will walk you right into the data center. If you're lucky the employees will even bring you coffee. With physical access to the systems, the network is yours for the taking. Have fun

installing key loggers, backdoors, wireless access points, and adding your own accounts for future access. However, keep in mind that there is always a small chance that you'll end up in choke hold or handcuffed by an excitable security guard, so I recommend getting a formal authorization letter before going onsite. Understandably, not everyone is keen on lying to people's faces. If that's the case, I recommend doing it via the phone or email instead. Over the Phone There are a number of proven techniques for conducting social engineering attacks over the phone, but depending on your goal I recommend one of two approaches. If the goal is to get a large volume of passwords and install backdoors, then target employees directly. Even if the company provides security training on an annual basis, most people tend to forget the IT procedures. If the goal is to target specific accounts, then calling the IT Support line is the way to go. Most support teams have some type of identification procedure, but in most cases a sob story and an employee number will get you access to the account. Email Phishing The superstar of the social engineering world is definitely email phishing. It is the most widely used vector for one very good reason—it's easy to do. Attackers can set up a fake company survey on the Internet, and send phishing emails to solicit passwords with very little effort. In my experience phishing attacks have approximately an 80% success rate, and in some cases the passwords can be gathered within minutes of sending the first phishing email. Similar to phone-based attacks, targets can vary from every employee in a company to strategic individuals such as CEOs. Technical vulnerabilities can present a real threat to organizations, but when it comes to getting the best results for your energy, social engineering wins out every time. However, keep in mind that social engineering tests are not a substitute for technical testing and should be done in conjunction with traditional assessments.

Conclusion Obtaining domain administrative privileges doesn't always require super hacker tools, but sometimes they do help. Also, when attacking the beast, go for the heart. Translation: When domain controllers are in scope, attack them first to save a lot of time. Until next time, keep shining light into the dark places. – SPS **Tool and Command References**

- http://www.foofus.net/fizzgig/fgdump/
- http://www.oxid.it/cain.html
- http://rainbowtables.shmoo.com/
- http://www.mcafee.com/us/downloads/free-tools/creddigger.aspx
- http://nmap.org/download.html
- http://www.wireshark.com/
- http://oss.coresecurity.com/projects/pshtoolkit.htm
- http://sourceforge.net/projects/incognito/
- http://labs.mwrinfosecurity.com/publications/white_paper_security_implications_of_windows_access_tokens/
- http://sourceforge.net/projects/ettercap/files/