

Forum:[Hack Forums](#)

Thread: [Hacking highly secured windows-environment](#)

The-hunter22 - March 12, 2018, 8:39 am

Hi. I have been pentesting for 1.5 years now. I have seen the good, the bad and the ugly sysadmin creatures but this job now is nextlevel. I am in the preparation phase and a few seniors will help me but your tips are welcome!

It is a gray box highly secured windows environment. I have 'basic user privs'. Like, you can expect they have the basics and more right. It's a big company -> they told me their soc will be at my desk if I make too much nmap noise xd

Are there any special tools and tricks to use, to get something.

*ps: I dont consider myself a skid or idk, newbie so please don't tell me to 'just look around and find version numbers' -> too basic and too unspecified.

Thank you

CyberStrike - March 12, 2018, 9:01 am

Well enumeration can't be undervalued but high security I usually would think that endpoints would end up with logs, so you will want to stay away from doing things that log. and also after you have escalated privileges on the machine they might be running something like responder (it detects responder) I have not seen it often but never know. Take a bit and look around on the network.

Also within the network consider making full use of machines that are compromised yet their whole job is just to redirect traffic. Generally you want 3 machines redirecting for each one scanning/attacking machine. These redirect machines should have NO tools only thing is just it forwards traffic.

Check if they are using sysmon for logging and forwarding alerts to endpoints .. sysmon is quite robust and if used right it's effective. Let's see bloodhound shouldn't raise flags. Once you got admin get into that guys email and make sure to delete alerts.

Let's see if you don't find responder being used use subdoc injection and responder together to compromise HVT (High Value Targets) you will get their username/hash. Make extensive use of PTH.

Stay away from psexec you have smbexec and wmiexec these are options. pssessions works too

Don't undervalue printers they can be exploited

Make sure you use a code signing cert.. if you get their code signing cert sign with it .

Use rev_https connections. Remember that anything found even in memory is fair game. We can carve out DLLs that are in memory.

You will find various lan segments, those multihomed machines are going to be where you want your sniffing to be, hopefully an admin is silly and they have tcpdump or tshark running.

Nomad.Null - March 13, 2018, 10:47 am

Focus on your OSINT, passive reconnaissance is a godsend and tells you a lot more than you initially think it might. Make extensive use of shodan, dns enumeration, googling, and data mining. Tools like Focka, TheHarvester, and especially recon-ng are very good at performing passive reconnaissance on engagements that you are supposed to stay extremely quiet on. Tools like Nmap are basically out of the question unless you do some very subtle port knocking...ie: you know what ports are open, you just want to grab some fingerprints to find out if any low hanging fruit are on the outside.

In addition to shodan, an awesome tool is dnsdumpster.com, which tells you all of the publicly known DNS records pulled from any domain you feed it. This is awesome when combined with any DNS brute-force tool like Fierce to help you identify what are the most important systems and services on the client's external network. It may not tell you ports, but crucial information like SPF records, txt records that reveal if they're using a mail filtering service like mimecast or spamassassin are incredibly useful in helping you prepare for a certain attack vector I'm not allowed to talk about here because HF mistakenly believes it is the root of all evil ;)

Above all else, use social media to your advantage. People are like sheep, idiots bleating into the dark about their lives and how they feel. People love to brag on LinkedIn, Facebook, Twitter, and many others about their newest position, achievements, and such. You can infer a lot of information about an organization's structure and culture just by reading employees' LinkedIn profiles. Combine LinkedIn with sources like Hunter.io as well, if you need a list of emails and usernames. It is very good at enumerating emails and identifying the schema which can help you both in scenarios where that special-case attack scenario I'm not allowed to talk about here is in scope. It's also mildly useful when you want to password spray against external services as well. VPN portals are a personal favorite, but make sure you have a Windows VM ready to go in case it uses a Windows-only client that tells Linux to kick rocks.

I preach about recon-ng a lot, but I promise it's a good tool when you learn how to use it effectively and combine certain modules to get some juicy info on an org. Run most of the modules twice and you can sometimes catch things you would have otherwise missed. I promise, if you're dilligent about checking public sources, sorting through metadata and documents that have been published/leaked online, you can uncover a LOT of potential paths into the network. Hell, one of my colleagues found a hard-coded domain admin password in a fucking powershell script on github not more than a month ago. You'd be surprised at what kinds of absurd shit you find clients doing. Some shit they do will make you want to head-desk through the fucking table.

Feel free to come back for more info, but yeah, for your engagement, stay stealthy and rely heavily on your public osint. It can really save you.

CyberStrike - March 13, 2018, 11:29 am

^^ Good stuff, also look at job boards pay attention to the language like "Must Fill" interpret that as "If you got a pulse we will hire you", important if say they are missing a Security Engineer or something. "Position Just Opened" means old employee was let go quickly .. their logins may work still. "X number of Positions to be filled" .. they probably let go a few employees or just got a big new contract. All this gives you an idea as to their security posture as well as what the hell is going on inside. Check Glassdoor see what employees are saying they tend to be honest.

Gee4rce - March 13, 2018, 7:39 pm

These are great answers you already have there!

For the scanning, you could limit nmap scans to only scan IANA Top 100 Portlist (think thats default anyways, but not sure atm), this will enumerate most common ports without causing to much traffic. Make sure to skip on options like "consider

host alive" and such, as this would dramatically increase network traffic caused by nmap scans. For simple scans i mostly go like "nmap -sV 1.2.3.4-200" (-sV bannergrabbing the version/service info).

Imo, the above represents the minimum requirement for a proper evaluation of machines and common services, shrinking it down even more would lead to loss of results on potential findings. There are always over-cautious admins, but it is your job to convince them of the need for these tests, and if a service still would go down (even if minimum load was caused) then this just exposes a weak service that should have been taken care of anyways. But this is not easy to communicate, even with the more friendly species of sysadmins.

For the Windows environment, look for LDAP misconfiguration, Sharepoint Servers, Active Directory, Network Shares and such. Check Intranet for Webapplications, try to gain access there. Often Employees have own service applications, like the office guys often work with SAP which they have (mostly) a webmask to login into.

Other than that, regular stuff applies like OS privilege escalation with Powershell scripts or WMI provider,
(carefull, before breaking things you should always check if thats inline with the rules and scope, some
admins don't like to see shellcode being executed on their systems).

This may only represent my personal style, i come from the webapplication hacking sector so my first
and main goal are mostly Webapps to target. This may not apply to everybody and some will have it easier targeting network infrastructure directly. Nevertheless, in a full pentest, both should be tried.

Cheers, Gee.

[BLANK] - March 14, 2018, 7:55 am

I recently wrote a great (well in my opinion) tutorial for attacking active directory...unfortunately it is only available to Superior members, so get in that group and read my write up!

But, as a good Samaritan I want to help you out. So I understand you are a professional penetration tester, you got a year and a half in and probably several years of security experience under your belt. You don't need basic tips etc. So lets examine what you have to work with.

1. You have basic user rights, does this mean you are already on the domain?
2. It sounds as if you are using a company computer, not your own computer but correct me if I am wrong.
3. Port scanning will get flagged as well as probably other obvious attacks.

First thing you will want to do is escalate your privs on the local machine. Since you are a pro I will assume you are already doing that and will move on. But the reason why you want those higher local privileges (for those reading) is because he will want to run powershell scripts and other programs as Administrator. If this company has locked down their host machines then PowerShell may not even be available for use.

Lets assume that you can use PowerShell and bypass any execution policy the company has in place. Our goal will be to utilize domain and system functions to enumerate the network and possibly find a path to domain admin. For this I propose using the following tools:

PowerView
PowerSploit
* BloodHound

I would love to details the steps and commands etc but it would take a lot of space up. That should give you a good start. BUT you may not be on a Windows box right now, maybe you have your own device and you are using Linux. In that case I would start with passive recon, one of my favorite is a simple "nmap -e eth0 --script=broadcast-*" that will give you a good idea of what is broadcasting on the network. I would also utilize Responder with NTLMRelayx as a means of using their broadcast against them. Though if this target is really locked down they may have enabled SMB signing but its always worth a try.

Overall you will want to be stealthy, that means avoid mass port scanning, avoid kernal exploitation and go after the Active Directory directly. It will take a lot of enumeration, user hunting, krbtgt manipulation etc but you can do it without triggering alarms. It really depends if you are on the domain already or if you have to get on the domain.

The-hunter22 - March 19, 2018, 8:31 am

Man you guys are awesome. Learned alot!

Last time I visited HF, it was full of bs and skiddies, who want to hack their gf snapchat. Awesome to see some quality!

<3

developer11 - March 19, 2018, 10:18 am

First and foremost :: take extremely good care of your security - you will need something thats more secure than Tor => your own hardware. Yes, its costly, but its the only way you are 100% hidden.

Buy HPE server and install Windows 2016 Core (without UI -> will not need it).

Buy second HPE machine. This time install Windows 2016 DataCenter.

Connect both to AD making one with Win2016 DC Active Domain Controller.

Switctch to Win2016 DC and do what follows::

Start > Control Panel > Default Programs > uncheck Internet Explorer; go to Server Manager > Extended security > OFF/OFF

Install FreeNET

Run FreeBrowser.

Install WireShark, open it.

fuckall

Now switch to Win2016 core.

Run commands

Get-IpBinds

By default, you will get one Bind (thatys from DomainController to your machine)

Install wirepcap-fetcher

Your server will restart.One up and running, open FreeBrowser, and just have fun. Watch other server for wireshark's data

CyberStrike - March 19, 2018, 12:02 pm

(Mar 19, 2018 08:31 AM)The-hunter22 Wrote: [\[CITE\]](#) Man you guys are awesome. Learned alot!

Last time I visited HF, it was full of bs and skiddies, who want to hack their gf snapchat. Awesome to see some quality!

<3

Don't worry those people are still here who do all that stuff.

Edit:

Quote:First and foremost :: take extremely good care of your security - you will need something thats more secure than Tor => your own hardware. Yes, its costly, but its the only way you are 100% hidden. Buy HPE server and install Windows 2016 Core (without UI -> will not need it).

Buy second HPE machine. This time install Windows 2016 DataCenter.

Connect both to AD making one with Win2016 DC Active Domain Controller.

Switctch to Win2016 DC and do what follows::

Start > Control Panel > Default Programs > uncheck Internet Explorer; go to Server Manager > Extended security > OFF/OFF

Install FreeNET

Run FreeBrowser.

Install WireShark, open it.

fuckall

Now switch to Win2016 core.

Run commands

Get-IpBinds

By default, you will get one Bind (thatys from DomainController to your machine)

Install wirepcap-fetcher

Your server will restart.One up and running, open FreeBrowser, and just have fun. Watch other server for wireshark's data

FreeNET? Yes by all means cache what other people are looking at. Adding machines to the Domain you sure are a stealthy guy do you call them up as well and inform them of your pentest. Server Manager also is not one the default Windows 2016 install sir.. it's all Powershell unless you want to install a gui..

Quote:When you install Windows Server 2016 using the Setup wizard, you can choose between Windows Server 2016 and Windows Server (Server with Desktop Experience). The Server with Desktop Experience option is the Windows Server 2016 equivalent of the Full installation option available in Windows Server 2012 R2 with the Desktop Experience feature installed. If you do not make a choice in the Setup wizard, Windows Server 2016 is installed; this is the Server Core installation option.

<https://docs.microsoft.com/en-us/windows-server/get-started/getting-started-with-server-with-desktop-experience>

Next WireShark.. tcpdump is text based and will capture user authentications just fine.

The-hunter22 - March 21, 2018, 6:17 am

Lawl, talking about...

I will update you guys about this, if I find some juicy thingies

skudZ-0 - March 23, 2018, 12:41 pm

Great Suggestions here! Thanks guys, this is exactly the content ive been looking for on HF.

Although, Im not really sure you can call any Windows environment "highly secure" LOL

The-hunter22 - *March 27, 2018, 7:42 am*

Hmmm. I have seen highly secured windows environments. It is possible and with the right tools and people it isnt that difficult at all. You can even have highly secured win xp environments. It isnt that bad as people think

CyberStrike - *March 27, 2018, 9:46 pm*

(Mar 23, 2018 12:41 PM)skudZ-0 Wrote: [\[CITE\]](#) Great Suggestions here! Thanks guys, this is exactly the content ive been looking for on HF. Although, Im not really sure you can call any Windows environment "highly secure" LOL

Linux/FreeBsd/OSX all have vulnerabilities Windows can be just as secure as Linux, for example if I had a Linux server that had some old and vulnerable service it's Linux but it's vulnerable. Don't fall for that old 1990-2004 myth of Linux invulnerability remember that Linux kernel 2.6.12 in 2005 got ASLR protections and Windows in 2007 with Vista, neither did much for ROP chains it still happens to this day.