Ethical Student Hackers

Windows Security

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

Difference between Windows and Linux

Comparison Table

	Windows	Linux
How are passwords stored?	SAM Hives	/etc/shadow
How are firewalls set?	Windows Defender Firewall	iptables, nftables
How are processes scheduled?	Task Scheduler	systemd
How are file permissions managed?	Explorer	Kernel, chmod, chown, chroot
How are user privileges managed?	UAC, Privileges	Sudo, kernel, su
How are services run?	Service accounts	Systemctl, user accounts
What antivirus is available?	Defender, proprietary	Proprietary

CVE Bingo!

How many vulnerabilities in Windows OS or services can you name?

Windows CVEs

Follina
(CVE-2022-30190)

PrintNightmare
(CVE-2021-34527)

Defender Priv Esc
(CVE-2021-24092)

Exchange Server
Exploit Chain
(CVE-2021-27065,
CVE-2021-26855,
CVE-2021-26857,
CVE-2021-26858)

MSHTML
(CVE-2021-40444)

OMIGOD
(CVE-2021-38647)

EternalBlue
(CVE-2017-0143)

HiveNightmare
(CVE-2021-36934)

PetitPotam
(CVE-2021-36942)

SambaCry
(CVE-2017–7494)

PrintSpoofer
(CVE-2020-1048)

SHEFFIELD ETHICAL STUDENT HACKERS

Windows… Design Flaws

ADCS Abuse

Pass the Hash

Printers running as SYSTEM…

DLL Injection

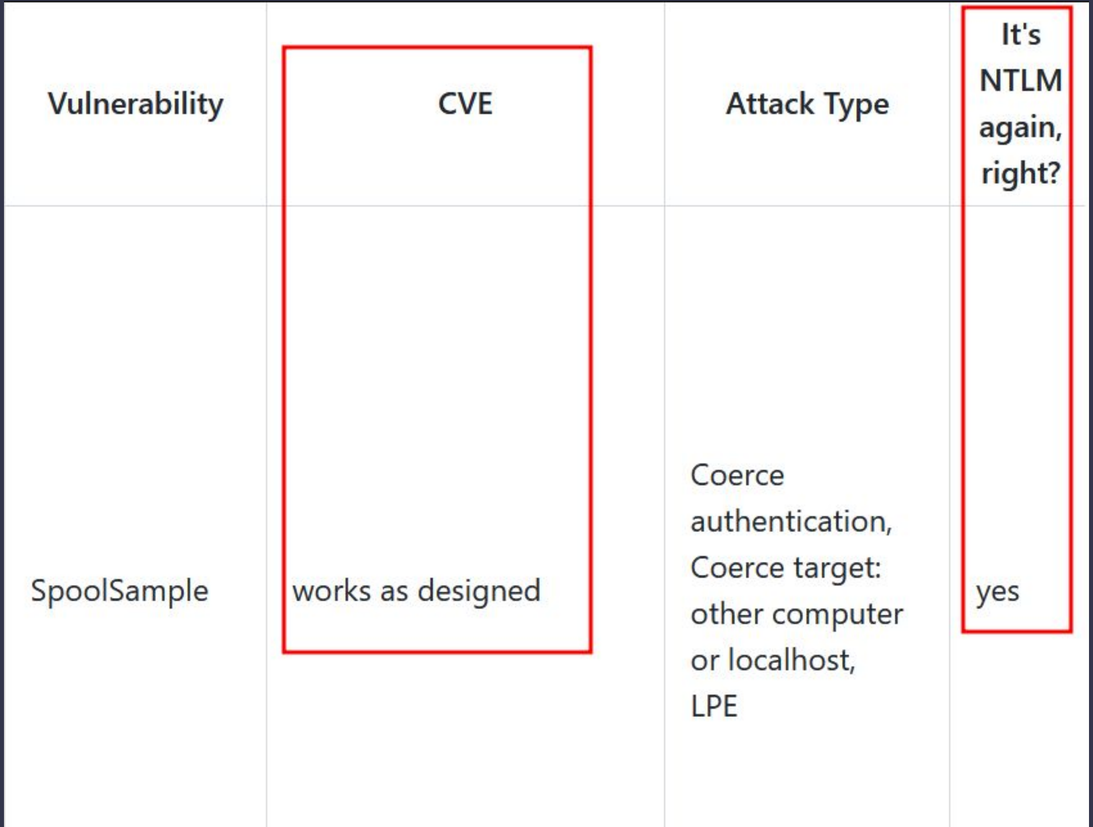
Word using IE to render web content…

Potato Attacks (SeImpersonatePrivilege)

NTLM in general is the source of many issues…

https://github.com/cfalta/MicrosoftWontFixList/blob/main/README.md

Windows… Design Flaws



Vulnerability	CVE	Attack Type	It's NTLM again, right?
SpoolSample	works as designed	Coerce authentication, Coerce target: other computer or localhost, LPE	yes

Windows Services

Here are some of the services you might see when scanning a Windows Machine:

- RPC + RPCBind (port 111 and 135): Lists services, allows remote interaction, enum with rpcclient
- Netbios + SMB (port 139 and 445): File sharing services, checking version numbers is crucial
- LDAP (port 389, 3268): Active Directory querying service
- Kerberos (port 88): Authentication Service
- RDP (port 3389): Remote Desktop Protocol
- WinRM (port 5985): Another remote access protocol

Many of these services make use of NTLM for authentication - SMB is used in Responder, and is the service used by psexec. NT hashes can also be used with tools like evil-winrm

Windows Commands

See users - `**net user**` or in powershell `**Get-WmiObject Win32_UserAccount -filter “LocalAccount=True”**`

See groups - `**net localgroup**` or in powershell `**Get-LocalGroup**`

See domain users - `**net user /domain**`

Check your privileges - `**whoami /priv**`

Look at system information incl. Hostname and build - `**systeminfo**`

Windows Security Features

(a very brief overview)

Users & Groups

- Like in Unix, each User has an account, and Users can be grouped
- Identified by a Security Identifier (SID) - this is included in Access Tokens granted when a user logs on
- Read more: https://www.digitalcitizen.life/simple-questions-what-user-group-windows-what-does-it-do/

Service Accounts

- Services, such as webservers on IIS or MSSQL servers, often run under a separate account
- They can ‘impersonate’ users’ Kerberos tokens (more on this in our AD session) and act as that user
- This enables a whole branch of security issues… more on this later, too
- Read more: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts

NTFS/Share Permissions

- Apply to files and folders (locally) or shared folders
- NTFS: Read, Read and Execute, Write, Modify, List Folder Contents, and Full Control
- Shares: Read, Change, and Full Control
- Read more: https://www.dell.com/support/kbdoc/en-uk/000137238/understanding-file-and-folder-permissions-in-windows

Windows Security Features (cont.)

Privileges

- Give an account the ability to perform a certain action (such as shutdown, impersonation etc)
- Common privilege escalation vector if an account has SeImpersonatePrivilege
- Read more: https://docs.microsoft.com/en-us/windows/win32/secauthz/privileges, https://blog.palantir.com/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e, and https://foxglovesecurity.com/2016/09/26/rotten-potato-privilege-escalation-from-service-accounts-to-system/

User Account Control (UAC)

- Operations that require administrative privileges require prompts for consent
- Processes are assigned ‘integrity’ levels - this indicates the level of trust
- Read more: https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works

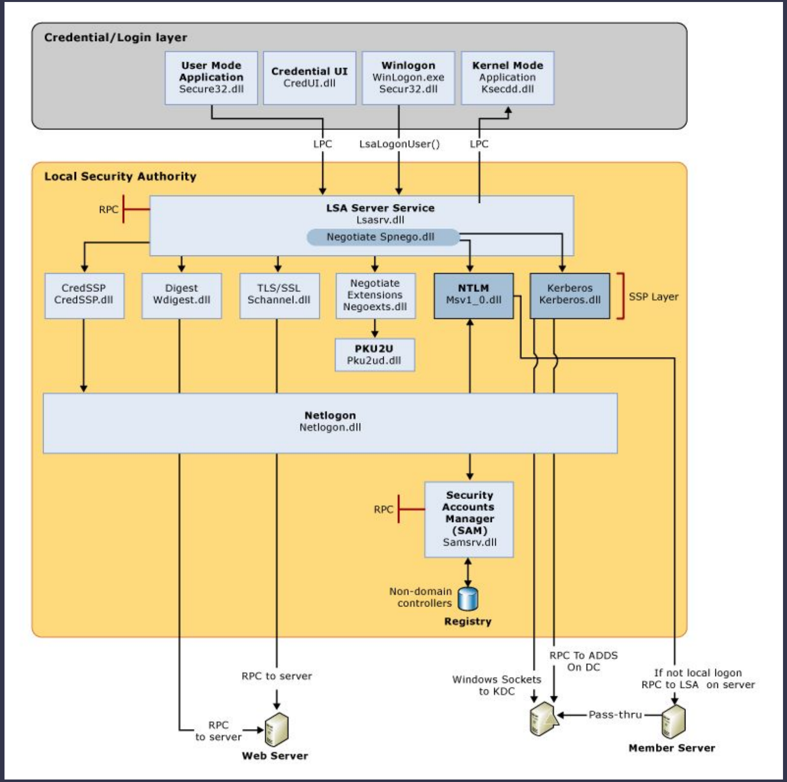
Windows Authentication

Security Accounts Manager (SAM)

- Windows Credential Store Database
- Stores several hashed passwords and Usernames
- SAM ‘hives’ can be extracted with tools like mimikatz and hashes dumped with impacket-secretsdump

NTLM Authentication Protocol

- NT hashes used to identify users
- Kerberos, the authentication protocol used in Active Directory, makes use of this
- Hashes can be used to authenticate on their own in pass-the-hash and NTLM relay attacks



Source: https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication

What's Wrong with Windows?

A core Windows feature ties together a lot of Windows CVEs - NTLM Authentication

Passing the Hash

- Plaintext passwords are rarely used to authenticate in Windows - usually it is the NT Hash
- This means stealing the NT Hash is roughly equivalent to stealing a plaintext password
- Hashes can be extracted from the SAM or NTDS.DIT databases
- Hashes can be stolen by tricking accounts into authenticating - for example, Responder's rogue SMB server
- One compromised machine can lead to multiple if they have the same passwords
- impacket-psexec: psexec.py -hashes [HASH] Administrator@ip
- Read more: https://en.hackndo.com/pass-the-hash/#protocol-ntlm and https://www.securify.nl/en/blog/living-off-the-land-stealing-netntlm-hashes/

NTLM Relays

- NTLM authentication can be Man-in-the-Middled to authenticate against Active Directory
- This is the basis for PetitPotam and several other attacks - read more: https://www.csoonline.com/article/3632090/ntlm-relay-attacks-explained-and-why-petitpotam-is-the-most-dangerous.html

Final note: https://github.com/cfalta/MicrosoftWontFixList/blob/main/README.md

Exploits

Initial Access - Eternal Blue

Brief history of Eternal Blue (i.e. Shadow Brokers): Known by NSA for 5+ years. Had to be patched on all Windows versions from Windows XP.

What causes exploit: Vulnerability in implementation of SMB protocol

How to exploit it: Sending a request with more than expected data to port 445(open by default).

How to mitigate it: Install the patch, limit access to critical functions, disable unused services.

Emergency patches: MS17-010

Activity - Eternal Blue

TryHackMe room - 10 minutes

https://tryhackme.com/room/blue

Initial Access - Follina

A recent exploit (CVE-2022-30190) in MSDT, a service for reporting diagnostics and crashes to Microsoft

Common vector is to send a Word Document with an HTML resource embedded inside it - the HTML resource then uses Javascript to *redirect* to an MSDT resource, triggering the vulnerability

What causes it:

- Word can fetch web content (as specified in an attacker-controlled document)
- Javascript can force computer to make a request to MSDT resource
- If resource is >4096 bits long, causes a buffer overflow and command

Unlike common Macro-based vectors, doesn’t require user to ‘Allow Macros’

Can even be ‘no click’ in some file formats

Initial Access - Follina

How to exploit it

- Host a HTML page that requests an MSDT
- Create a word document that requests this HTML resource + send it to victim
- Pad the MSDT resource after the command to 4096 bits to cause buffer overflow

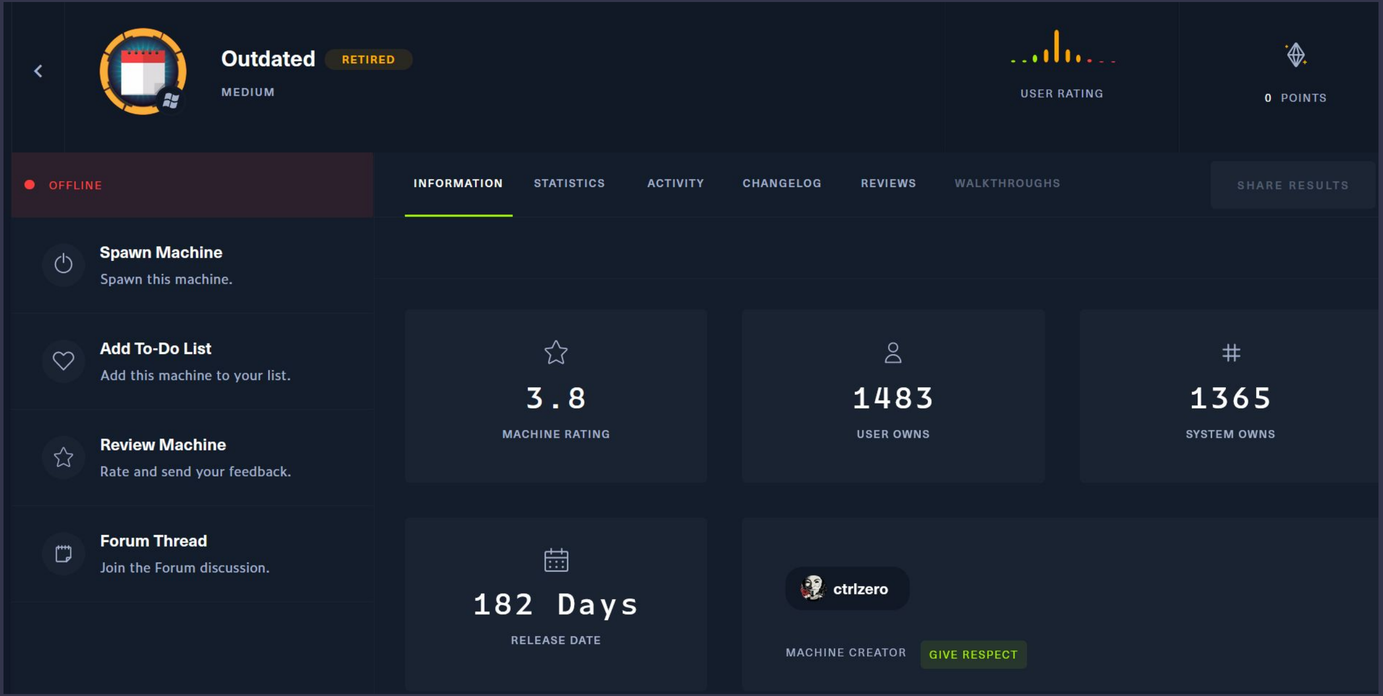
View proof of concept and explanation: https://github.com/JohnHammond/msdt-follina

Read more:

- https://www.blackberry.com/us/en/solutions/endpoint-security/security-vulnerabilities/follina-vulnerability
- https://logrhythm.com/blog/detecting-follina-cve-2022-30190-microsoft-office-zero-day-exploit/
- https://www.beyondtrust.com/blog/entry/mitigating-the-follina-zero-day-vulnerability-cve-2022-30190-with-privilege-management-for-windows

Demo - Follina

https://app.hackthebox.com/machines/490 - Writeup: https://0xdf.gitlab.io/2022/12/10/htb-outdated.html



Outdated RETIRED

MEDIUM

USER RATING

0 POINTS

● OFFLINE

INFORMATION | STATISTICS | ACTIVITY | CHANGELOG | REVIEWS | WALKTHROUGHS | SHARE RESULTS

Spawn Machine
Spawn this machine.

Add To-Do List
Add this machine to your list.

Review Machine
Rate and send your feedback.

Forum Thread
Join the Forum discussion.

3.8
MACHINE RATING

1483
USER OWNS

1365
SYSTEM OWNS

182 Days
RELEASE DATE

ctrlzero
MACHINE CREATOR GIVE RESPECT

Privesc - Windows Exploit Suggester

A key tool when getting started with Windows security to find common exploits

https://github.com/AonCyberLabs/Windows-Exploit-Suggester

First, run systeminfo on the target machine

Then feed the output into a file and run the tool on your local machine e.g. Kali:

```
python2 windows-exploit-suggester.py --database 2021-05-07-mssb.xls --systeminfo /path/to/systeminfo
```

Make sure to run python2 windows-exploit-suggester.py --update regularly

Privesc - WinPEAS

You’ve heard of LinPEAS… now get ready for:
https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

Download from releases page - either exe or bat, try both

It can look for things like

- Missing OS patches
- Exposed credentials
- Readable files
- Dangerous privileges
- Injectable DLLs / Processes to hollow

Lots of info - takes experience to filter through - To do this manually instead:
https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalation

SHEFFIELD ETHICAL STUDENT HACKERS

Privesc - Potato Attacks

This family of attacks is possible in many ways, but they rely on a key privilege - SeImpersonatePrivilege
What is SeImpersonatePrivelege - “Impersonate a client after authentication”1

HOT POTATO:

- Local NSBN Spoofer
- Fake WPAD proxy server
- HTTP to SMB NTLM Relay.

Some write-ups: https://jlajara.gitlab.io/Potatoes_Windows_Privesc, https://foxglovesecurity.com/2016/01/16/hot-potato/. GitHub links: https://github.com/antonioCoco/RemotePotato0

Privesc/Pivoting - Mimikatz

Once you have SYSTEM access on a windows machine, you can gain access to other machines by stealing credentials that might be reused

Upload and run mimikatz.exe (from /usr/share/windows-resources/mimikatz/x64/mimikatz.exe on Kali)

- Essential steps to elevate mimikatz’ capabilities
  - privilege::debug
  - token::elevate
- sekurlsa::logonpasswords to dump all stored passwords
- sekurlsa::tickets to dump tickets (useful for AD - next week!)

https://www.varonis.com/blog/what-is-mimikatz

Activity - SAM Hash Extraction

Download the SAM file zip from here: https://shefesh.com/assets/demos/SAM%20Files.zip

(Short Url: shorturl.at/fs149)

- On Linux: wget https://shefesh.com/assets/demos/SAM%20Files.zip
- Files were extracted with reg.exe save hklm\sam c:\windows\temp\sam.save (etc for hklm\security, hklm\system)

Extract the hashes using impacket-secretsdump

- secretsdump.py -sam SAM -security SECURITY -system SYSTEM LOCAL

Optional: crack the hashes using hashcat

- hashcat -a 0 -m 1000 hashes --wordlist /usr/share/wordlists/rockyou.txt

Bletchley Park Trip

Tickets are OUT today!

This trip is a fantastic price and a great chance to learn about the history of codebreaking

£6.50 covers transport for the day and 4 hours in the museum

There are 13 tickets allocated to SESH members - if you miss out, CompSoc and SWiCS also have tickets

Buy here: https://su.sheffield.ac.uk/events/id/3220-ethical-student-hackers-bletchley-park-ticket

BLETCHLEY PARK TRIP

Sunday 12th March

Tickets £6.50
Avaliable Monday
13th Feb @ 9am

Upcoming Sessions

What’s up next?

www.shefesh.com/sessions

20/02/23 – Active Directory

27/02/23 – Advanced Web Hacking

06/03/23 – Cryptography

12/03/23 – **BLETCHLEY PARK TRIP!**

13/03/23 – Hardware Hacking

Any Questions?

SHEFFIELD ETHICAL STUDENT HACKERS

www.shefesh.com

Thanks for coming!